3 Режим обеспечения безопасности

Содержание

Указание по безопасности

Эта глава содержит важную информацию об отказобезопасном использовании сигнальных модулей повышенной безопасности.

Вы должны прочитать эту главу, чтобы использовать сигнальные модули повышенной безопасности в режиме обеспечения безопасности.

3.1 Варианты конфигурации периферийных модулей повышенной безопасности в режиме обеспечения безопасности

Децентрализованное функционирование в ET 200M

В режиме обеспечения безопасности сигнальные модули повышенной безопасности работают децентрализованно в устройстве децентрализованной периферии ET 200M.

Замечание

Сигнальные модули повышенной безопасности **не** должны использоваться и конфигурироваться в режиме обеспечения безопасности на центральных монтажных стойках в качестве централизованных периферийных модулей. В ET 200M возможно только децентрализованное функционирование.

Допустимые IM 153-x

Какие компоненты ET 200M могут использоваться в режиме обеспечения безопасности, зависит от класса безопасности и использования разделительного модуля в конфигурации ET 200M:

- Если вы удовлетворяете требованиям класса SIL 2 или используете разделительный модуль в классе безопасности SIL 3, то вы можете использовать все интерфейсные модули IM 153-x устройства децентрализованной периферии ET 200M (как в стандартном режиме). Устанавливайте разделительный модуль слева от сигнальных модулей повышенной безопасности.
- Если вы не используете разделительный модуль в ET 200M в SIL 3, то вы должны монтировать ветви PROFIBUS-DP в программируемых контроллерах S7-400F и S7-400FH с использованием **волоконно-оптических кабелей**. Тогда используйте следующий интерфейсный модуль ET 200M:

  ET 200M с IM 153-2 FO (начиная с номера для заказа 6ES7 153-2AB01-0XB0)

Совместное использование периферийных модулей повышенной безопасности со стандартными модулями S7-300

Если вы используете в ET 200M разделительный модуль, то вы можете применять в ET 200M сигнальные модули повышенной безопасности со стандартными сигнальными модулями S7-300 в режиме обеспечения безопасности **в** SIL 3.

Разделительный модуль защищает сигнальные модули повышенной безопасности от возможных перенапряжений в случае неисправности ("безопасное функциональное низкое напряжение", см. раздел 8.2). Для этого сигнальные модули повышенной безопасности должны быть вставлены в конфигурацию ET 200M справа от разделительного модуля, а все стандартные сигнальные модули должны быть вставлены слева от разделительного модуля (см. главу 11).

Совместное использование периферийных модулей повышенной безопасности в стандартном режиме и в режиме повышенной безопасности

Указание по безопасности

В **одном** ET 200M можно **вместе** эксплуатировать сигнальные модули повышенной безопасности, работающие в разных режимах (т.е. в стандартном режиме и в режиме обеспечения безопасности). При этом нет необходимости разделять сигнальные модули повышенной безопасности в зависимости от режима, в котором они работают (т.е. устанавливать их в различных ET 200M или использовать разделительный модуль).

Варианты конфигурации в режиме обеспечения безопасности

Компоненты децентрализованной периферии могут присоединяться к сигнальным модулям повышенной безопасности следующими тремя способами:

В системе	Вариант конфигурации	Готовность
S7-400F	• Одноканальная односторонняя периферия	Стандартная готовность
S7-400FH	• Одноканальная коммутируемая периферия	Повышенная готовность
	• Резервируемая коммутируемая периферия	Максимальная готовность

Следующие страницы содержат примеры типичных конфигураций. Коэффициент готовности сигналов процесса зависит от используемого варианта конфигурации.

Дополнительная информация

Подробную информацию о разделительном модуле вы найдете в главе 11.

Вы можете найти подробное описание конфигурации ET 200M в руководстве *Устройство децентрализованной периферии ET 200M*.

Если вы хотите использовать сигнальные модули повышенной безопасности в качестве резервируемых периферийных модулей в системе FH, обратитесь к руководству *Система автоматизации S7-400H, Отказоустойчивые системы*.

3.1.1 Одноканальная односторонняя периферия

Что такое одноканальная односторонняя периферия?

В случае одноканальной односторонней периферии сигнальные модули повышенной безопасности не дублируются; каждый из них имеется только в одном экземпляре. Обращение к сигнальным модулям повышенной безопасности производится из одного CPU.

- Конфигурация для S7-400F
- При монтаже PROFIBUS-DP **с использованием медного кабеля** вам потребуется следующее:
  - один CPU, способный выполнять отказобезопасные (F) программы (напр., CPU 417-4 H)
  - одна линия PROFIBUS-DP
  - один ET 200M: IM 153-x
  - разделительный модуль (монтаж слева от отказобезопасной периферии)
  - два шинных штекера для присоединения модуля CPU и IM 153-x к PROFIBUS-DP
- При монтаже PROFIBUS-DP **с использованием волоконно-оптического кабеля** вам потребуется следующее:
  - один CPU, способный выполнять отказобезопасные (F) программы (например, CPU 417-4 H)
  - одна линия PROFIBUS-DP
  - один ET 200M: IM 153-2 FO
  - компонент для присоединения модуля CPU к волоконно-оптическому кабелю (напр., OLM/OBT)
- по одному сигнальному модулю повышенной безопасности (без резервирования)

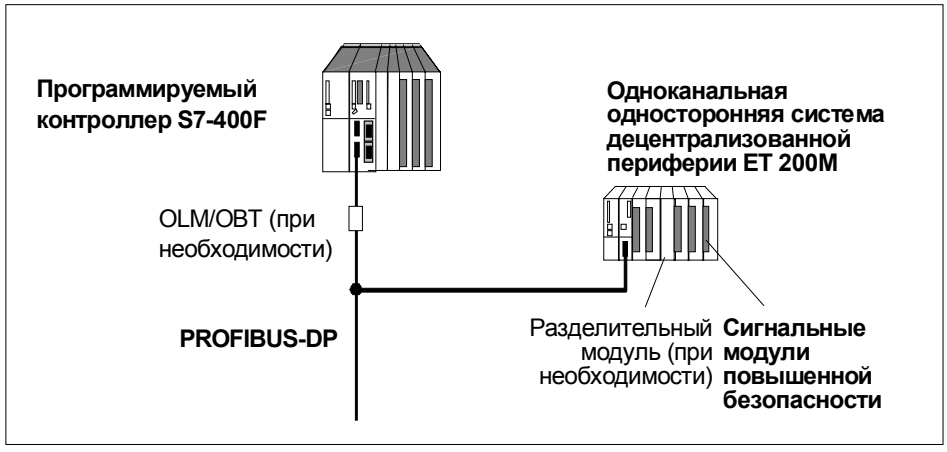


Рис. 3-1. Конфигурация с одноканальной односторонней периферией

Возможности доступа

В случае неисправности периферия становится недоступной. Сигнальные модули повышенной безопасности пассивируются (см. раздел 3.4).

Возможные причины:

- отказ сигнального модуля повышенной безопасности
- отказ IM 153-x/IM 153-2 FO
- отказ всего ET 200M
- отказ линии PROFIBUS-DP
- отказ CPU

3.1.2 Одноканальная коммутируемая периферия

Что такое одноканальная коммутируемая периферия?

В случае одноканальной коммутируемой периферии сигнальные модули повышенной безопасности не дублируются; каждый из них имеется только в одном экземпляре. Обращение к сигнальным модулям повышенной безопасности производится из двух CPU. ET 200M имеет интерфейс slave-устройства DP с каждой из двух резервируемых линий PROFIBUS-DP и, таким образом, имеет физическое соединение с каждым из двух CPU.

- Конфигурация для S7-400FH
- При монтаже PROFIBUS-DP **с использованием медного кабеля** вам потребуется следующее:
  - два CPU, способных выполнять отказобезопасные (F) программы (напр., CPU 417-4 H)
  - две линии PROFIBUS-DP
  - один ET 200M с двумя (резервируемыми) интерфейсными модулями IM 153-x, каждый с интерфейсом PROFIBUS-DP
  - разделительный модуль (монтаж слева от отказобезопасной периферии)
  - четыре шинных штекера для присоединения обоих модулей CPU и обоих IM 153-x к PROFIBUS-DP
- При монтаже PROFIBUS-DP **с использованием волоконно-оптического кабеля** вам потребуется следующее:
  - два CPU, способных выполнять отказобезопасные (F) программы (напр., CPU 417-4 H)
  - две линии PROFIBUS-DP
  - один ET 200M с двумя (резервируемыми) интерфейсными модулями IM 153-2 FO, каждый с интерфейсом PROFIBUS-DP
  - два компонента для присоединения модулей CPU к волоконно-оптическим кабелям (напр., OLM/OBT)
- по одному сигнальному модулю повышенной безопасности (без резервирования)

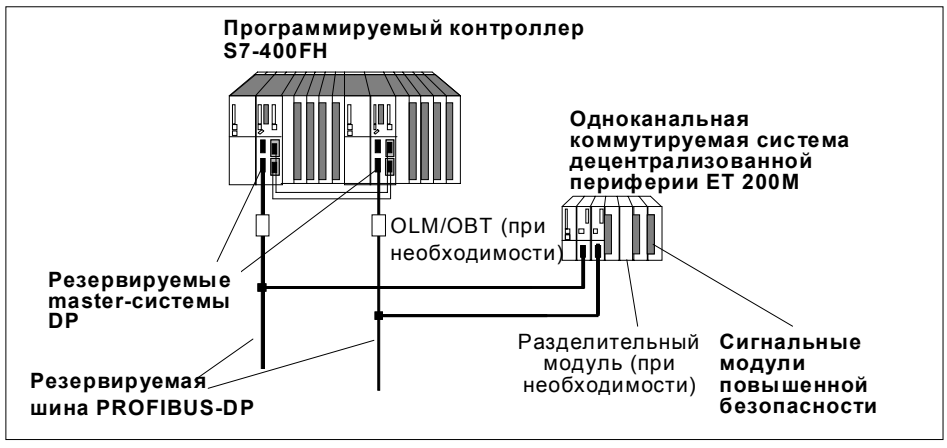


Рис. 3-2. Конфигурация с одноканальной коммутируемой периферией

Возможности доступа

В случае неисправности сигнального модуля повышенной безопасности периферия становится недоступной. Соответствующий сигнальный модуль повышенной безопасности пассивируется (см. раздел 3.4). Коммутируемая периферия остается доступной процессу в следующих случаях:

- отказ одного IM 153-x/2 FO
- отказ одной линии PROFIBUS-DP
- отказ одного CPU

Коммутируемая периферия становится недоступной процессу в следующих случаях:

- отказ сигнального модуля повышенной безопасности
- отказ всего ET 200M

Дальнейшее повышение готовности достигается резервированием сигнальных модулей внутри ET 200M. Коммутируемая периферия остается в этом случае доступной процессу даже после выхода из строя одного сигнального модуля повышенной безопасности. Только при выходе из строя всего ET 200M коммутируемая периферия становится недоступной процессу.

3.1.3 Резервируемая коммутируемая периферия

Что такое резервируемая коммутируемая периферия?

В случае резервируемой коммутируемой периферии сигнальные модули повышенной безопасности дублируются (резервируются). Два сигнальных модуля повышенной безопасности находятся или в отдельных устройствах ET 200M, или в одном и том же. В следующем примере два резервируемых сигнальных модуля находятся в разных устройствах ET 200M.

- Конфигурация для S7-400FH
- При монтаже PROFIBUS-DP **с использованием медного кабеля** вам потребуется следующее:
  - два CPU, способных выполнять отказобезопасные (F) программы (напр., CPU 417-4 H)
  - две линии PROFIBUS-DP
  - два устройства ET 200M: каждый с двумя модулями IM 153-x
  - два разделительных модуля (монтаж слева от отказобезопасной периферии)
  - шесть шинных штекеров для присоединения обоих модулей CPU и четырех IM 153-x к PROFIBUS-DP
- При монтаже PROFIBUS-DP **с использованием волоконно-оптического кабеля** вам потребуется следующее:
  - два CPU, способных выполнять отказобезопасные (F) программы (напр., CPU 417-4 H)
  - две линии PROFIBUS-DP
  - два устройства ET 200M: каждый с двумя модулями IM 153-2 FO
  - два компонента для присоединения модулей CPU к волоконно-оптическим кабелям (напр., OLM/OBT)
- Дублированные (резервируемые) сигнальные модули повышенной безопасности

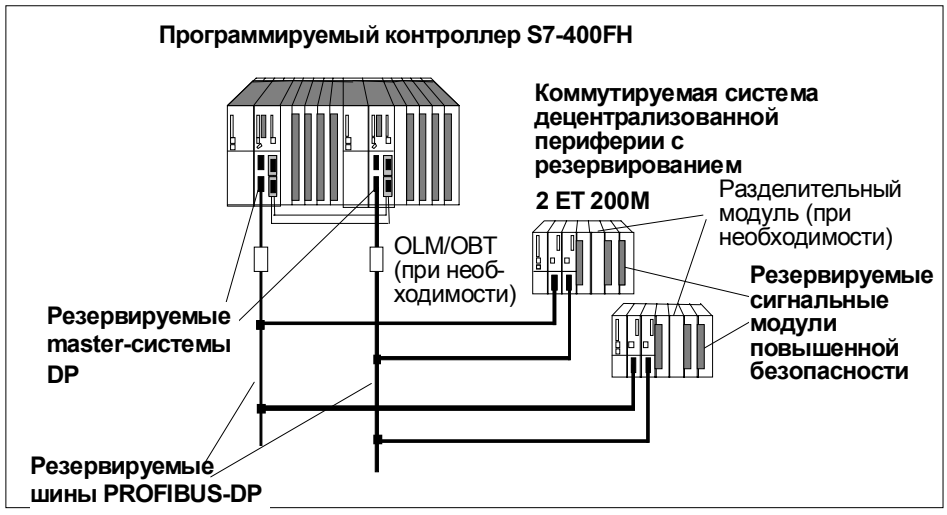


Рис. 3-3. Конфигурация с резервируемой коммутируемой периферией

Готовность

Периферия остается доступной процессу в следующих случаях:

- отказ одного резервируемого сигнального модуля повышенной безопасности
- отказ одного IM 153-x/-2 FO в каждом из двух устройств ET 200M
- полный отказ одного ET 200M
- отказ одной линии PROFIBUS-DP
- отказ одного CPU

3.2 Функции обеспечения безопасности

Указание по безопасности

Информация, содержащаяся в этом разделе, позволит вам правильно подключать и параметризовать отказобезопасные сигнальные модули в режиме обеспечения безопасности для достижения определенного уровня безопасности.

3.2.1 Функции обеспечения безопасности, необходимые для достижения определенных уровней безопасности в случае отказобезопасных модулей ввода

Анализ датчиков в случае модулей ввода повышенной безопасности

В случае отказобезопасных **цифровых модулей ввода** требуемый уровень безопасности достигается путем использования подходящего способа анализа датчиков.

Уровень безопасности			Требуемый вид анализа датчиков
по IEC 61508	**по DIN V 19250**	**по EN 954-1**	
SIL 2	Уровень безопасности AK 4	Категория 3	Анализ 1-из-1
SIL 3	AK 5, 6	Категория 4	Анализ 1-из-2

В случае отказобезопасных **аналоговых модулей ввода** в режиме обеспечения безопасности всегда выполняется анализ датчиков типа "1-из-2".

Уровень безопасности			Требуемый вид анализа датчиков
по IEC 61508	**по DIN V 19250**	**по EN 954-1**	
SIL 2	Уровень безопасности AK 4	Категория 3	Анализ 1-из-1, одноканальные датчики
SIL 3	AK 5, 6	Категория 4	Анализ 1-из-2, резервируемые датчики

Анализ типа "1-из-1"

При использовании анализа типа "1-из-1" имеется один датчик, который подключается к модулю через один канал.

Анализ типа "1-из-2" у цифровых модулей

При анализе типа "1-из-2" сигнальные состояния входов сравниваются внутренне на совпадение или несовпадение.

Для сигнала процесса датчики могут быть присоединены к двум расположенным друг против друга входам сигнального модуля следующим образом:

- Сигнал датчика разветвляется на два входа (не у NAMUR).
  Для достижения при таком присоединении уровня SIL 3 (уровень безопасности AK 6, категория 4) требуется соответствующим образом сертифицированный датчик.
- К двум входам подключаются два несовпадающих сигнала датчика, выдающего два противоположных сигнала (не у NAMUR).
- Два одинаковых датчика для одного и того же параметра процесса (напр., "уровень воды достигнут") подключаются каждый к одному из двух входов.

Обратите внимание, что при анализе типа "1-из-2" имеется в распоряжении только половина входов модуля.

Анализ типа "1-из-2" у аналоговых модулей ввода

У аналогового модуля ввода в режиме обеспечения безопасности на каждый сигнал процесса к двум **противоположным входам** аналогового модуля подключается один датчик (SIL 2 / AK 4) или два резервируемых датчика (SIL 3 / AK 5, 6).

Что нужно сделать?

- Датчики на модуле ввода повышенной безопасности следует подключить в соответствии с желаемым видом анализа датчиков.
- Вид анализа датчиков необходимо параметризовать с помощью дополнительного пакета *S7 F Systems* [*Системы повышенной безопасности S7*] для *STEP 7*.

Проверка рассогласования в случае модулей ввода повышенной безопасности

Проверка рассогласования начинается, если у двух связанных друг с другом входных сигналов обнаруживаются разные уровни. По истечении конфигурируемого интервала времени (время рассогласования) контролируется, исчезло ли рассогласование. Если нет, то имеет место ошибка рассогласования.

У модулей ввода повышенной безопасности имеется два вида проверки рассогласования:

- при анализе датчиков типа "1-из-2"
- у резервируемых модулей (только цифровых)

Проверка рассогласования при анализе типа "1-из-2"

Проверка рассогласования выполняется в модуле ввода повышенной безопасности между обоими входными сигналами, анализируемыми по методу "1-из-2".

У цифровых модулей: если входные сигналы по истечении параметризованного времени рассогласования не совпадают, напр., из-за обрыва провода в линии от датчика, то входной сигнал, подаваемый в CPU, устанавливается в "0". Это соответствует логическому сопряжению входных сигналов в соответствии с функцией И. Кроме того, в диагностическом буфере модуля генерируется диагностическое сообщение "discrepancy error [ошибка рассогласования]" с указанием на соответствующий канал.

Замечание

В течение времени рассогласования модуля в CPU передается **старое значение** соответствующего входного канала. Из этого следует, что время рассогласования двухканальных датчиков для быстрых реакций должно быть рассчитано на малые времена реакции.

Например, не имеет смысла активизировать критическое к времени отключение с помощью двухканальных датчиков с временем рассогласования 500 мс. В наихудшем случае время реакции датчика или исполнительного устройства увеличивается примерно на время рассогласования:

- Поэтому датчики в процессе следует располагать со столь **малым рассогласованием**, насколько это возможно.
- Затем вы должны выбрать **по возможности малое** время рассогласования, которое, с другой стороны, обладает достаточным резервом от ошибочного запуска ошибок рассогласования.

Проверка рассогласования у аналоговых модулей

Если вы запроектировали режим обеспечения безопасности в соответствии с SIL 3 / AK 5, 6, то вы можете запроектировать для аналогового модуля ввода на каждый вход время рассогласования и абсолютный допустимый диапазон в % относительно диапазона измерения от 4 до 20 мА. Кроме того, запроектируйте унифицированное значение (MIN = меньшее / MAX= большее), которое должно быть принято и далее передано в CPU.

Если разность между двумя измеренными значениями находится вне допустимого диапазона дольше запроектированного времени рассогласования, то выдается сообщение об ошибке и принимается унифицированное значение.

Проверка рассогласования у резервируемых цифровых модулей ввода

Проверка рассогласования выполняется между обоими входными сигналами резервируемых модулей ввода с помощью отказобезопасных драйверных блоков.

Если входные сигналы по истечении параметризованного времени рассогласования не совпадают, то выходной сигнал драйвера устанавливается в "1". Это соответствует логическому сопряжению сигналов в драйвере в соответствии с функцией ИЛИ.

Так как сигналы обоих модулей могут рассматриваться как безопасные, то можно доверять значению "1" одного из сигнальных модулей и передать этот сигнал на выход драйвера без риска для безопасности. Это также гарантирует требуемую степень готовности системы.

При ошибках рассогласования на выходах DIAG_1/2 отказобезопасного драйвера модуля дополнительно выводится диагностическая информация (см. главу 8 руководства *Программируемые контроллеры S7-400F и S7-400FH*).

Параметры для проверки рассогласования

Для обоих видов проверки рассогласования выполните параметризацию времени рассогласования с помощью дополнительного пакета *S7 F Systems* [*Системы повышенной безопасности S7*] для *STEP 7*.

Где это описано?

Как подключение, так и параметризация модулей ввода повышенной безопасности зависят от модуля. Применения различных модулей подробно описаны в главах 9 и 10.

3.2.2 Функции обеспечения безопасности, необходимые для достижения определенных уровней безопасности в случае отказобезопасных модулей вывода

Подключение тестовых сигналов у отказобезопасных модулей вывода

У отказобезопасных модулей вывода требуемый уровень безопасности может быть достигнут подключением тестовых сигналов.

Уровень безопасности			… достигается подключением тестовых сигналов
по IEC 61508	**по DIN V 19250**	**по EN 954-1**	
SIL 2	Уровень безопасности AK 4	Категория 3	• "темный" период (< 1 мс)
SIL 3	Уровень безопасности AK 6	Категория 4	• "светлый" период (< 1 мс) и • "темный" период (< 1 мс)

Темный период

"Темные" периоды возникают при тестировании выключения и при полном тестировании двоичных кодов. При этом на активный выход отказобезопасным модулем вывода подаются обусловленные тестированием нулевые сигналы. После этого выход кратковременно ("темный" период) отключается. Достаточно инерционное исполнительное устройство на это не реагирует и остается включенным.

Светлый период (Light period)

"Светлые" периоды возникают при полном тестировании двоичных кодов. При этом на неактивный выход (выходной сигнал "0") отказобезопасным модулем вывода подаются обусловленные тестированием единичные сигналы. После этого выход кратковременно ("светлый" период) включается. Достаточно инерционное исполнительное устройство на это не реагирует и остается выключенным.

Если сигнал изменяется ежедневно или чаще

Если сигнал изменяется ежедневно или чаще, то SIL 3 (уровень безопасности AK 6, категория 4) может эксплуатироваться без "светлого" периода.

Что нужно сделать?

С помощью дополнительного пакета *S7 F Systems* [*Системы повышенной безопасности S7*] для *STEP 7* необходимо параметризовать:

- Вид подключения тестового сигнала
- Сигнал изменяется ежедневно или чаще

Где это описано?

Применения и параметризация модулей вывода повышенной безопасности подробно описаны в главах 9 и 10.

3.2.3 Дополнительные функции обеспечения безопасности

Указание по безопасности

Информация, содержащаяся в этом разделе, позволит вам правильно интерпретировать диагностические сообщения сигнальных модулей повышенной безопасности, имеющие значение для обеспечения безопасности. Они не зависят от достигаемого уровня безопасности.

Кадр для обеспечения безопасности

В режиме обеспечения безопасности данные между CPU и сигнальным модулем повышенной безопасности передаются в кадре, предназначенном для обеспечения безопасности, имеющем длину до 16 байтов. Кадр для обеспечения безопасности состоит из:

- значений процесса (данные пользователя)
- байта состояния и байта управления (координирующие данные для режима обеспечения безопасности)
- тестового значения CRC
- символа активности (или текущего номера)

Контрольная сумма CRC (Cyclic Redundancy Check [контроль с использованием циклического избыточного кода])

Действительность значений процесса, содержащихся в кадре обеспечения безопасности, правильность связей между назначенными адресами и параметры, имеющие значение для обеспечения безопасности, защищены с помощью контрольной суммы CRC, содержащейся в кадре обеспечения безопасности.

Если при обмене данными между CPU и модулем происходит ошибка контрольной суммы, например, из-за возникающих время от времени высоких электромагнитных помех, то появляется диагностическое сообщение, указывающее на ошибку контрольной суммы (CRC). У модулей вывода повышенной безопасности выходы выключаются немедленно.

Время контроля и текущий номер

Временной контроль обновления кадра в протоколе ProfiSafe осуществляется благодаря тому, что CPU задает текущий номер сигнальному модулю повышенной безопасности.

Действительный текущий кадр должен прибыть на CPU с действительным текущим номером в течение назначаемого при параметризации времени контроля.

Если действительный текущий номер не обнаружен в течение времени контроля, то появляется диагностическое сообщение, указывающее, что превышено время контроля для программы обеспечения безопасности. У модулей вывода повышенной безопасности выходы выключаются. У цифровых модулей ввода повышенной безопасности входы для CPU устанавливаются в "0". У аналоговых модулей ввода повышенной безопасности входы для CPU устанавливаются на запроектированные заменяющие значения.

Время контроля параметризуется для каждого сигнального модуля повышенной безопасности в *STEP 7* с помощью дополнительного пакета *S7 F Systems*.

3.3 Адресация в режиме обеспечения безопасности

Адреса

В режиме обеспечения безопасности отказобезопасных сигнальных модулей следует делать различие между:

- логическим адресом модуля
- номером канала

3.3.1 Логический адрес модуля

Настройка

Логический адрес сигнальных модулей повышенной безопасности:

- проектируется как входной параметр отказобезопасных драйверных блоков **и**
- устанавливается на сигнальном модуле повышенной безопасности с помощью переключателя адресов (DIL-переключатель) (см. главу 4, "Монтаж").

Допустимая адресная область

Сигнальные модули повышенной безопасности занимают до 16 байтов в области входов и выходов. Поэтому могут использоваться только следующие адреса:

Допустимая адресная область: от 8 до 8191 шагами по восемь

Правила задания адресов

Указание по безопасности

- Адрес, установленный с помощью переключателя адресов сигнальных модулей повышенной безопасности должен совпадать с адресом, заданным в *HWConfig* в *STEP 7*.
- Чтобы обеспечить уникальность логического адреса модуля в системе шин PROFIBUS-DP, сигнальный модуль повышенной безопасности может адресоваться только одним CPU.

  Исключение: Коммутируемая периферия в S7-400FH (обращение к сигнальному модулю производится всегда по одному и тому же адресу одним из двух CPU, текущим устройством управления передачей данных по шине DP)
- Логические адреса сигнальных модулей повышенной безопасности во всех CPU, находящихся в одной ветви PROFIBUS-DP, должны быть различными (они не должны перекрываться).
- CPU в системе S7-400FH при коммутируемой периферии должны обращаться к одним и тем же сигнальным модулям повышенной безопасности.

Защита

Включение логического адреса модуля в контрольную сумму CRC кадра для обеспечения безопасности защищает присвоение адресов сигнальных модулей повышенной безопасности.

Если адреса не согласованы, например, если на модуле и в отказобезопасном драйверном блоке установлены разные адреса, то при обмене данными между CPU и модулем возникает ошибка контрольной суммы. Появляется диагностическое сообщение, указывающее на ошибку в циклическом контроле избыточности (CRC). -> Происходит переход в безопасное состояние.

3.3.2 Номер канала

Определение

Внутри функций обеспечения безопасности входы и выходы адресуются через номера каналов. Номер канала – это порядковый номер, начинающийся с "0".

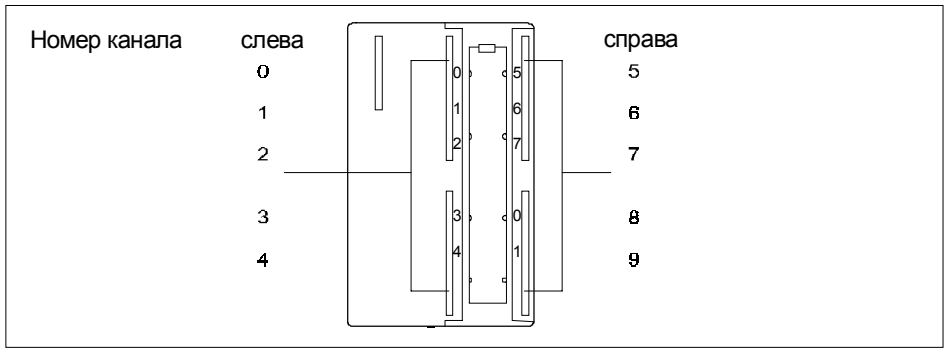
Применение

Номер канала сигнальных модулей повышенной безопасности:

- Проектируется как входной или выходной параметр отказобезопасных драйверных блоков
- На него делается ссылка в диагностических сообщениях, относящихся к каналам

Пример номеров каналов

На следующем рисунке показано соответствие номеров каналов входам и выходам на примере SM 326; DO 10 ✕ 24 V DC/2A; с диагностическим прерыванием:



Деление пополам при анализе типа "1-из-2" у цифровых модулей ввода

При анализе типа "1-из-2" на цифровых модулях ввода датчики подключаются к противоположным клеммам модуля через два канала: количество каналов (номера каналов) при этом уменьшается вдвое.

3.4 Реакции на неисправности в периферийных модулях повышенной безопасности

Безопасное состояние (концепция безопасности)

Основой концепции безопасности является то, что для всех переменных процесса имеется безопасное нейтральное состояние. У цифровых сигнальных модулей это всегда значение "0"; у аналоговых модулей ввода это проектируемое заменяющее значение.

Реакции на неисправности

Если сигнальный модуль повышенной безопасности распознает неисправность, то он переключает затронутый канал или все каналы в безопасное состояние (т.е. каналы этого модуля пассивируются). Сигнальный модуль повышенной безопасности сообщает об обнаруженной ошибке отказобезопасному драйверному блоку.

Пассивация может быть инициирована сигнальным модулем повышенной безопасности, отказобезопасным драйвером модуля или F отказобезопасным драйвером канала или пользователем в программе обеспечения безопасности.

Что такое пассивация?

Пассивация означает, что в случае неисправности один или несколько каналов сигнального модуля повышенной безопасности переключаются в безопасное состояние.

- **Пассивация каналов вывода** означает, что выходы обесточиваются. Отказобезопасный драйвер пассивированного цифрового канала вывода выводит заменяющее значение с кодом качества (QUALITY) 16#48, а выход QBAD устанавливается в 1.
- **Пассивация каналов ввода** означает, что в программу обеспечения безопасности независимо от текущего сигнала процесса передаются заменяющие значения. Отказобезопасный драйвер пассивированного цифрового канала ввода выводит заменяющее значение 0 с кодом качества (QUALITY) 16#48, а выход QBAD устанавливается в 1. В зависимости от параметризации на входе SUBS_ON отказобезопасный драйвер канала аналогового ввода выводит заменяющее значение с кодом качества (QUALITY) 16#48 или последнее допустимое значение с кодом качества (QUALITY) 16#44. Кроме того, выход QBAD устанавливается в 1, и, если выводится заменяющее значение, выход QSUBS тоже устанавливается в 1.

Ошибка канала или модуля?

Если происходит ошибка канала (напр., неисправен датчик), то пассивируется только **затронутый** канал. В случае неисправности или ошибки модуля (напр., коммуникационная ошибка), пассивируются все каналы сигнального модуля повышенной безопасности.

В главах 9 и 10 рассказывается, о каких ошибках канала или модуля сообщается для каждого модуля.

Указание по безопасности

При параметризации сигнальных модулей повышенной безопасности не забудьте включить групповую диагностику для каждого канала в качестве реакции на ошибки канала.

Повторное включение в систему после устранения неисправности или ошибки

Повторное включение в систему означает:

- На выходных каналах модулей вывода повышенной безопасности снова выводятся действительные значения процесса.
- Отказобезопасные драйверы каналов модулей ввода повышенной безопасности снова передают в программу обеспечения безопасности действительные значения процесса.

Программирование отказобезопасных драйверных блоков относительно пассивации и реинтеграции подробно объясняется в руководстве *Системы повышенной безопасности*.

Особенность SM 326; DO 10 x 24 V DC/2A

У SM 326; DO 10 x 24 V DC/2A следующие неисправности каналов

- короткое замыкание на L+
- неисправность выходного драйвера

приводят к срабатыванию **электронной** защиты, и половина каналов соответствующего модуля (0...4 или 5...9) пассивируется. Например, если происходит короткое замыкание на L+ в канале 1, то пассивируются каналы 0...4.

Если короткие замыкания происходят повторно, то модуль немедленно выключается со сбоем программы.

Поведение при выключенной групповой диагностике

Групповая диагностика **может** быть выключена на неиспользуемых входных или выходных каналах с целью повышения коэффициента готовности. Это приводит к следующему поведению:

Модули ввода повышенной безопасности:

Если групповая диагностика входных каналов выключена, то в случае неисправности в CPU тоже передаются безопасные значения "0", но в CPU 417-4H сообщения об ошибках не передаются.

Модули вывода повышенной безопасности:

В случае неисправностей каналов на выходах с выключенной групповой диагностикой происходит следующее:

- При неисправностях с отключением отдельных каналов, затронутые каналы модуля **не** выключаются.
- При неисправностях с отключением затронутой половины модуля (DO0...DO4 или DO5...DO9) соответствующая половина модуля **выключается**.
- CPU **не** получает диагностического сообщения, а выходы **не** пассивируются, в зависимости от настройки отказобезопасного драйвера канала.

Указание по безопасности

У модулей ввода и вывода повышенной безопасности в режиме обеспечения безопасности групповая диагностика должна быть установлена для всех подключенных каналов.

Пожалуйста, проверьте, действительно ли отключение групповой диагностики выполнено только у неиспользуемых входных и выходных каналов.

Пассивация модулей вывода повышенной безопасности в течение длительного времени

Указание по безопасности

Если модуль вывода повышенной безопасности пассивирован в течение длительного интервала времени (> 24 часов) без устранения неисправности, то не исключено, что модуль будет непреднамеренно активизирован второй неисправностью, приведя, таким образом, систему в опасное состояние.

Хотя вероятность возникновения таких аппаратных неисправностей очень мала, такая нежелательная активизация пассивированных модулей вывода повышенной безопасности должна быть предотвращена с помощью коммутационных или организационных мероприятий. Одной из возможностей является отключение питания пассивированного модуля на некоторый период времени (напр., 24 часа).

У установок, для которых имеются производственные стандарты, требуемые мероприятия стандартизованы. У всех остальных установок эксперт, принимающий систему, должен одобрить концепцию необходимых мероприятий, предлагаемую оператором установки.

Вывод заменяющих значений

В режиме обеспечения безопасности у модулей вывода **нет** возможности подключения заменяющих значений (0 или 1).

Индикация неисправностей/ошибок

Общую информацию о диагностических возможностях и диагностических светодиодах можно найти в главе 7 "Диагностика".

Диагностические сообщения, относящиеся к модулям, приведены в главах 9 и 10.

3.5 Требования к датчикам и исполнительным устройствам

Общие требования к датчикам и исполнительным устройствам

Указание по безопасности

Использование датчиков и исполнительных устройств находится вне сферы нашего влияния. Мы оснастили наши электронные компоненты таким образом, что 85 % вероятности остающихся ошибок могут быть возложены на датчики и исполнительные устройства (что соответствует рекомендуемому распределению нагрузки между датчиками, исполнительными устройствами и электронными схемами для ввода, обработки и вывода в системах обеспечения безопасности).

Поэтому обратите внимание на то, что оснащение датчиками и исполнительными устройствами несет на себе значительную долю **ответственности за безопасность**. Помните, что датчики и исполнительные устройства, как правило, не выдерживают 10-летнего интервала профилактического обслуживания, предписанного стандартом IEC 61508, без существенного снижения безопасности.

Дополнительное требование к датчикам и датчикам NAMUR

Указание по безопасности

У модулей ввода повышенной безопасности при обнаружении неисправности в CPU посылается значение "0" (через отказобезопасные драйверные блоки). Поэтому вы должны обеспечить такую реализацию датчиков, чтобы программа пользователя безопасно реагировала на их нулевое состояние.

Пример: В программе пользователя датчик аварийного останова должен выключать соответствующее исполнительное устройство, когда состояние датчика равно "0" (кнопка аварийного останова нажата).

Дополнительное требование к датчикам

Указание по безопасности

Обеспечьте, чтобы сигналы датчиков имели минимальную длительность 50 мс, чтобы они могли быть правильно зарегистрированы.

Дополнительное требование к датчикам NAMUR

Указание по безопасности

Обеспечьте, чтобы сигналы датчиков NAMUR имели минимальную длительность 100 мс, чтобы они могли быть правильно зарегистрированы.

Требования к аналоговым датчикам

Как правило, имеет силу следующее: для удовлетворения требований SIL 2 достаточно одноканального датчика; для удовлетворения требований SIL 3 должно быть два канала. Однако для удовлетворения требований SIL 2 с одноканальным датчиком этот датчик сам должен обладать свойствами SIL 2; в противном случае этот уровень безопасности может быть достигнут только с помощью двухканальных датчиков.

Дополнительное требование к исполнительным устройствам

Модули вывода повышенной безопасности тестируют выходы через регулярные интервалы времени. Для этого модуль кратковременно выключает активные выходы и, если необходимо, кратковременно включает выходы, которые были выключены. Эти тестовые импульсы имеют следующие длительности:

- "Темный" период < 1 мс
- "Светлый" период < 1 мс

Исполнительные устройства с быстрой реакцией во время тестирования могут быть кратковременно деактивизированы или активизированы. Если ваш процесс не может этого допустить, используйте достаточно инерционные исполнительные устройства (> 1 мс).

Указание по безопасности

Если исполнительные устройства эксплуатируются с напряжениями, большими 24 В пост. тока (напр., при 230 В пост. тока) или если исполнительные устройства коммутируют большие напряжения, то выходы модуля вывода повышенной безопасности должны иметь надежную потенциальную развязку с частями установки, несущими повышенное напряжение.

Обычно это имеет место у реле и контакторов. На это нужно обращать особое внимание при использовании полупроводникового коммутационного оборудования.

Исключение "темных" периодов в режиме обеспечения безопасности

Указание по безопасности

При использовании исполнительных устройств, которые реагируют слишком быстро (т.е. < 1 мс) только при подаче тестового сигнала "темный период", то вы можете все же использовать внутреннюю координацию тестирования путем параллельного включения двух противоположных выходов (с последовательным диодом). При параллельном включении "темные" периоды подавляются (см. с. 9-46).

Технические данные датчиков и исполнительных устройств

Информацию о технических данных датчиков и исполнительных устройств вы можете также получить в главах 9 и 10.

3.6 Замена модулей в режиме обеспечения безопасности

Снятие/установка

Если ET 200M сконструирован с **активными шинными модулями**, то сигнальные модули повышенной безопасности могут вставляться и извлекаться во время работы.

Система S7-400F

У системы S7-400F модули могут заменяться во время работы. При этом могут срабатывать функции обеспечения безопасности, затронутые заменой модуля.

Система S7-400FH

У системы S7-400FH резервируемые модули могут заменяться во время работы. При замене модулей ни одна из функций обеспечения безопасности не активизируется.

Предпосылка для замены модулей

При замене модуля обратите внимание на то, чтобы переключатель адресов (DIL-переключатель) на задней стороне нового модуля был установлен так же, как и на старом.

Дополнительная информация

Подробную информацию о замене модулей в ET 200M и о функции "Замена модулей во время работы" можно найти в руководстве *Устройство децентрализованной периферии ET 200M*.