3 Механизмы обеспечения безопасности

3.1 Введение в механизмы обеспечения безопасности

В этой главе вы сможете узнать о механизмах, ориентированных на обеспечение безопасности S7-400F/FH. Эта информация служит основой при переходе к проектированию системы повышенной безопасности и созданию и тестированию отказобезопасной программы. Описываются только функции, в которых поведение S7-400F отличается от стандартной системы S7. Стандартное поведение описано в руководствах по STEP 7 и аппаратному обеспечению.

Какие механизмы обеспечения безопасности имеют значение для вас?

Механизмами, ориентированными на обеспечение безопасности в CPU (аппаратура и операционная система), являются:

- Защита от доступа для систем повышенной безопасности, что позволяет избежать ошибок
- Самотестирование, что позволяет обнаруживать и идентифицировать неисправности

Ориентированные на обеспечение безопасности функции для обнаружения неисправностей и реагирования на неисправности расположены, главным образом, в F-программе и в сигнальных модулях повышенной безопасности. Эти функции реализуются с помощью соответствующих отказобезопасных блоков и поддерживаются аппаратными средствами и операционной системой CPU.

Функции, ориентированные на обеспечение безопасности отказобезопасных сигнальных модулей, описаны в руководстве /1/.

3.2 Режим обеспечения безопасности

Ориентированные на обеспечение безопасности функции для обнаружения неисправностей и реагирования на неисправности активизируются в режиме обеспечения безопасности

- в сигнальных модулях повышенной безопасности
- в F-программе CPU

Режим обеспечения безопасности сигнальных модулей повышенной безопасности

При проектировании сигнальных модулей повышенной безопасности в HW Config вы можете использовать для установки стандартного режима или режима обеспечения безопасности параметр "Safety Mode [Режим обеспечения безопасности]":

- Для установки стандартного режима не выбирайте параметр "Safety Mode".
- Для установки безопасного режима выберите параметр "Safety Mode".

Дополнительную информацию о стандартном режиме и режиме обеспечения безопасности можно найти в руководстве /1/. Информацию о параметризации сигнальных модулей повышенной безопасности можно найти в системе оперативной помощи и в разделе "Параметризация сигнальных модулей повышенной безопасности (F SM)" в главе "Проектирование".

Режим обеспечения безопасности F-программы

Отказобезопасная программа (F-программа) обычно исполняется на CPU в режиме обеспечения безопасности. Т.е. все механизмы обеспечения безопасности для обнаружения неисправностей и реагирования на неисправности активизированы. Если F-программа находится в режиме обеспечения безопасности, то ее невозможно изменить.

Режим обеспечения безопасности F-программы в CPU может быть выключен и снова включен, чтобы дать возможность изменить F-программу в режиме RUN. Включать и выключать режим обеспечения безопасности для F-программы в CPU можно в SIMATIC Manager выбором команды меню **Options > Customize Safety Program [Дополнительные возможности > Настроить программу обеспечения безопасности]**. Дальнейшую информацию об изменении F-программы в режиме RUN можно найти в разделах "Деактивизация режима обеспечения безопасности " и "Изменение F-программы в режиме RUN" главы "Программирование".

3.3 Реакции на неисправности

Безопасное состояние

Основа концепции безопасности состоит в том, что для всех переменных процесса должно иметься безопасное, нейтральное состояние. В случае двоичных сигнальных модулей это всегда значение "0".

Реакции на неисправности в CPU и операционной системе

Если CPU обнаруживает неисправность аппаратными средствами (контроль времени) или с помощью операционной системы (самотестирование и т.д.), то по умолчанию CPU может быть переведен в состояние STOP.

Реакции на неисправности в F-программе

Все реакции F-программы на неисправности приводят к безопасному состоянию:

- STOP CPU. Это состояние может быть изменено только запуском (холодный пуск или теплый пуск). Информацию о характеристиках запуска и защите от запуска и перезапуска можно найти в разделе 3.4 "Запуск системы повышенной безопасности".
- Устойчивая к отключению питания блокировка операций вывода, связанных с обеспечением безопасности. Ошибки периферии или обмена данными приводят к блокировке соответствующих операций вывода, а не к переходу CPU в STOP. Эти операции могут быть разблокированы после подтверждения пользователя через входной параметр на отказобезопасном драйвере канала.

Как правило, в реакции на обнаружение неисправностей могут быть выполнены функции диагностики, не связанной с обеспечением безопасности, и функции сообщений.

В системе S7-400FH инициируется переключение главный/резервный, если главное устройство переходит в состояние STOP.

Список причин перевода CPU в STOP вы найдете в разделе "Информация об ошибках после перехода CPU в STOP".

3.4 Запуск системы повышенной безопасности

Режимы работы S7-400F/FH

Режимы работы S7-400F отличаются от нормальных режимов только характеристиками запуска и поведением в режиме фиксации (HOLD). В остальном состояния отказоустойчивой системы и режимы работы главного и резервного CPU в системе S7-400FH такие же, как это описано в /4/, глава 4.

Характеристики запуска

Характеристики запуска определяются F-программой следующим образом: После каждого прерывания программы пользователя – посредством выключения питания или перевода CPU в STOP – запуск F-программы возможен только с начальными значениями отказобезопасных блоков.

Если при запуске запрашивается теплый пуск, то такой пуск выполняется только для стандартного раздела программы пользователя. Теплый пуск для раздела программы пользователя, обеспечивающего повышенную безопасность, невозможен; F-программа запускается с начальными значениями отказобезопасных блоков таким же образом, как и после холодного пуска.

При компиляции F-программы в начале исполняемой последовательности в OB 100 автоматически вставляются дополнительные блоки (DB_RES) и вызовы, которые не должны изменяться.

Защита от запуска

Запуск F-программы с начальными значениями может быть также активизирован обработкой ошибки или внутренней ошибкой. Если процесс этого не допускает, то реакция на это должна быть запрограммирована в F-программе. Для сигнализации о запуске F-программы с начальными значениями имеется в распоряжении блок F_START (см. раздел "Программирование характеристик запуска").

Защита от горячего пуска

F-программа после обнаружения проблемы, имеющей значение для безопасности, блокирует все операции вывода, связанные с обеспечением безопасности. Эта блокировка может быть изменена только запуском (холодный или теплый пуск). Запуск может удалить информацию об ошибках, хранящуюся в CPU.

Если горячий пуск процесса после реакции S7-400F на внутреннюю ошибку недопустим, то должно быть запрограммировано ручное разблокирование операций вывода после запуска F-программы с начальными значениями (см. выше).

Режим HOLD

Режим HOLD для систем повышенной безопасности S7-400F/FH не поддерживается. Если исполнение программы пользователя останавливается запросом на HOLD, то это состояние может быть изменено только запуском (холодный или теплый пуск).

3.5 Самотестирование и тестирование команд

Самотестирование

Самотестирование выполняется в системе S7-400F/FH для обнаружения неисправностей. Интервал циклического самотестирования может быть установлен при проектировании (по умолчанию 90 минут).

Замечание

Для S7-400F/FH разрешены установки только до 12 часов.

У S7-400F/FH нельзя изменять самотестирование, имеющее значение для обеспечения безопасности, с помощью SFC 90 "H_CTRL". Если вы это сделаете, то CPU перейдет в STOP самое позднее через 24 часа. Не допускается отключение или включение компонентов тестирования (подрежимы 0 .. 5 режимов 20, 21 и 22).

По той же причине вы не должны на слишком долгое время блокировать актуализацию с помощью SFC 90 "H_CTRL".

Полное выполнение тестирования (исполнение программы, все аппаратные средства, ориентированные на обеспечение безопасности) и его результаты контролируются в F-программе отказобезопасным блоком тестирования (F_TESTC), который автоматически вставляется при компиляции F-программы.

Тестирование команд

Некоторые команды тестируются в самом быстром цикле F-программы. Это тестирование команд реализуется в блоке F_TEST, который автоматически вставляется при компиляции F-программы.

3.6 Логический и временной контроль исполнения программы

Контроль исполнения программы

Ошибки могут исказить правильное выполнение программы. Это может быть обнаружено с помощью логического контроля выполнения программы, контроля ее выполнения по времени и контроля потока данных.

Логический контроль исполнения программы и потока данных

Во время компиляции в схему CFC автоматически вставляются отказобезопасные блоки для логического контроля исполнения программы и потока данных: в каждую исполняемую группу с отказобезопасными блоками вставляется один блок F_PLK и один блок F_PLK_O. F_PLK вызывается перед операциями вывода, а F_PLK_O после них.

Если обнаруживается опасная неисправность, логический контроль выполнения программы требует перевода CPU в STOP вызовом SFC 46 "STP". Затем требуется запуск (холодный или теплый пуск).

Контроль выполнения программы по критерию времени

Контроль выполнения программы по критерию времени осуществляется через:

- активный контроль во время обмена данными, ориентированного на обеспечение безопасности
- контроль времени F-цикла

Активный контроль во время обмена данными, ориентированного на обеспечение безопасности

F-программа циклически обменивается данными с сигнальными модулями повышенной безопасности и с F-программами на других CPU с помощью специальных протоколов обеспечения безопасности. При возникновении проблемы приемники реализуют функцию реагирования на неисправность:

- Модули вывода повышенной безопасности выключают выходы.
- Отказобезопасные блоки F_RCVBO и F_RCVR в F-программах на других CPU выводят параметризуемые заменяющие значения.

После устранения проблемы требуется подтверждение пользователя на отказобезопасном драйверном блоке канала или отказобезопасном блоке F_RCVBO или F_RCVR или запуск (холодный или теплый пуск).

Контроль времени F-цикла

Максимальное время F-цикла (время циклического прерывания для OB с исполняемыми F-группами) назначается в CFC как входной параметр отказобезопасного блока F_CYC_CO. Отказобезопасный блок F_CYC_CO F должен присутствовать в каждом F-цикле (т.е. в каждом OB прерываний с отказобезопасными блоками).

При превышении времени F-цикла CPU переходит в STOP, а все выходы возвращаются в безопасное состояние.

3.7 Отказобезопасные пользовательские времена

Значения времени, генерируемые в F-программе с помощью блоков F_TP, F_TON и F_TOFF, контролируются посредством механизмов обеспечения безопасности CPU. Для этого сравниваются два независимых друг от друга счетчика времени. Пока различие между этими двумя счетчиками меньше 10 мс в течение периода времени 50 с, время считается правильным. Если различие больше, то предполагается неисправность аппаратуры.

Максимальная неточность пользовательских времен может быть рассчитана на основе следующей таблицы:

Пользовательские времена от	**до**	**макс. неточность**
10 мс	50 с	± 5 мс
> 50 с	100 с	± 10 мс
...	...	...
> n* 50 с	(n+1)*50 с	± (n+1)*5 мс

Фактическая неточность значительно меньше этой. Обратите также внимание на неточность времени, возникающую из-за обработки в ходе циклического прерывания.

3.8 Защита паролем для систем повышенной безопасности

Пароль защищает S7-400F/FH от несанкционированного доступа, т.е. от нежелательных загрузок в CPU из системы разработки (ES) или устройства программирования (PG). Кроме стандартного пароля для CPU, требуется также дополнительный пароль для систем повышенной безопасности и отказоустойчивых систем повышенной безопасности для F-программы (F-пароль).

Сравнение

В следующей таблице дается сравнение пароля CPU и пароля для программы обеспечения безопасности.

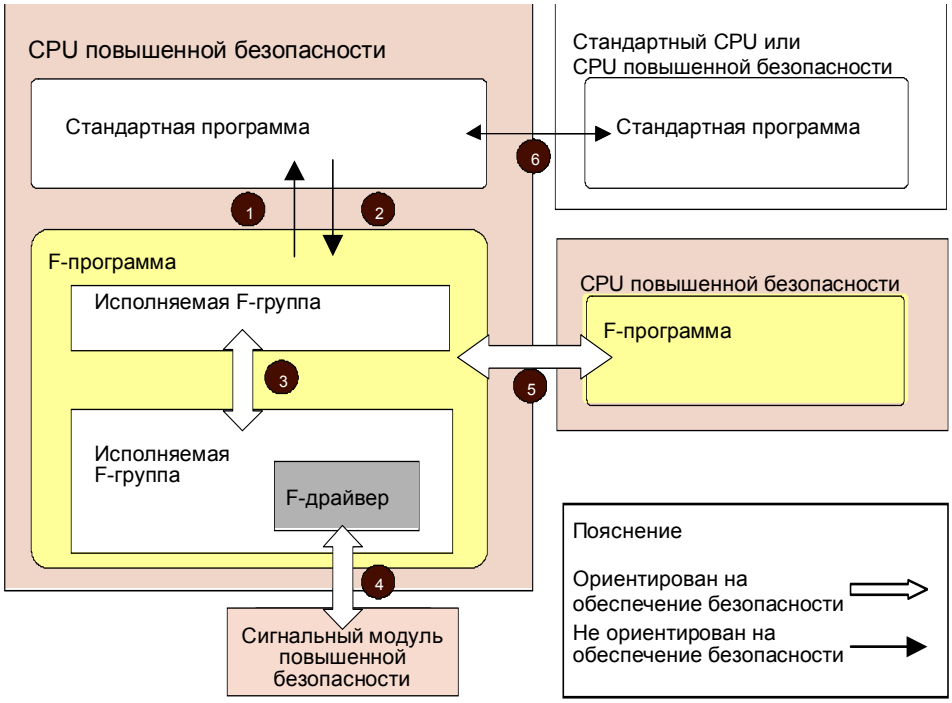
	Пароль CPU	**Пароль для программы обеспечения безопасности**
Ввод	В HW Config при проектировании CPU, закладка "Protection [Защита]" в диалоговом окне "Properties [Свойства]"	В SIMATIC Manager, **Options > Customize Safety Program [Дополнительные возможности > Настроить программу обеспечения безопасности]**
Запрашивается при	• загрузке всей программы из CFC или SIMATIC Manager • загрузке изменений F-программы из CFC • загрузке и удалении отказобезопасных блоков из SIMATIC Manager • загрузке на плату памяти СППЗУ на CPU из SIMATIC Manager • сбросе памяти из CFC или SIMATIC Manager • изменении F-констант в режиме тестирования CFC	• компиляции изменений в F-программе • включении и выключении режима обеспечения безопасности • загрузке изменений данных F-программы, когда режим обеспечения безопасности не активен • изменении F-констант в режиме тестирования CFC
Время действия	Действует неограниченно, пока не будет явно отменен через соответствующую функцию SIMATIC Manager или пока не завершены все приложения STEP 7.	Один час после ввода пароля, или пока права доступа не будут явно отменены.

Вы можете найти дополнительную информацию о защите паролем в главе "Проектирование", раздел "Установка, изменение и отмена прав доступа".

3.9 Обмен данными, ориентированный на обеспечение безопасности

Обзор обмена данными

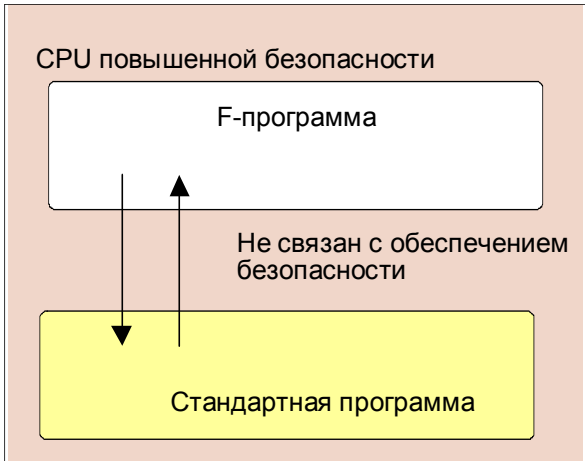
На следующем рисунке показаны возможности обмена данными, имеющимися в распоряжении системы повышенной безопасности:



Номер	Обмен данными между	и	Ориентирован на обеспечение безопасности
1	F-программой в CPU повышенной безопасности	стандартной программой	Нет
2	стандартной программой	F-программой	Нет
3	исполняемой F-группой	исполняемой F-группой	Да
4	F-программой в CPU повышенной безопасности	сигнальным модулем повышенной безопасности	Да
5	F-программой в CPU повышенной безопасности	F-программой в CPU повышенной безопасности	Да
6	стандартной программой в стандартном CPU или CPU повышенной безопасности	стандартной программой в стандартном CPU или CPU повышенной безопасности	Нет

3.9.1 Обмен данными между F-программой и стандартной программой пользователя

Стандартные программы и F-программы используют разные форматы данных. Поэтому для обмена данными должны применяться специальные блоки преобразования.



Из	**в**	**Блок**	**Ориентирован на обеспечение безопасности**
F-программы	стандартную программу	F_F*data type_data type*	Нет
стандартной программы	F-программу	F_*data type*_F*data type*	Нет

В F-программе параметры передаются как F-типы данных, ориентированные на обеспечение безопасности. Если стандартная программа пользователя должна обрабатывать данные из F-программы, например, для целей контроля, то в CFC должен быть вставлен блок для преобразования данных (F_F*data type_data type*), чтобы преобразовывать F-типы данных в стандартные типы данных. Эти блоки можно найти в библиотеке User Blocks [Пользовательские блоки] в разделе Failsafe Blocks [Отказобезопасные блоки].

Блоки F_F*data type_data type* должны вызываться в стандартной программе пользователя (в схеме CFC, в стандартной исполняемой группе).

Если данные из стандартной программы пользователя должны обрабатываться в F-программе, то из стандартных типов данных с помощью блоков для преобразования данных F_*data type*_F*data type* должны быть созданы F-типы данных, ориентированные на обеспечение безопасности, и, если необходимо, затем подвергнуты проверке на достоверность, программируемой с помощью отказобезопасных блоков. Блоки преобразования данных F_*data type*_F*data type* должны использоваться только в F-программе (в схеме CFC, в исполняемой F-группе).

3.9.2 Обмен данными между исполняемыми F-группами

Исполняемые группы, содержащие отказобезопасные блоки, называются **отказобезопасными исполняемыми группами (исполняемыми F-группами)**. Передача данных между исполняемыми F-группами пользовательской программы должна быть ориентирована на обеспечение безопасности. Для ориентированного на обеспечение безопасности обмена данными между исполняемыми F-группами имеются отказобезопасные блоки **F_S_*data type*** и **F_R_*data type***. Это позволяет передавать фиксированное количество параметров одного и того же F-типа данных.

Чтобы обеспечить возможность обмена данными между исполняемыми F-группами в различных OB циклических прерываний, циклическое прерывание с более коротким циклом должно при проектировании получить более высокий приоритет.

Блок F_S_*data type* встраивается в передающую исполняемую F-группу, а его входные F-параметры соединяются с подлежащими передаче параметрами других отказобезопасных блоков. Блок F_R_*data type* вставляется в принимающую исполняемую F-группу, а его выходные F-параметры соединяются с входами других отказобезопасных блоков. Соединение между F_S_*data type* и F_R_*data type* устанавливается с помощью системы взаимных соединений в CFC.

3.9.3 Обмен данными между CPU и сигнальными модулями повышенной безопасности

Ориентированный на обеспечение безопасности обмен данными между CPU и сигнальными модулями повышенной безопасности через ProfiSafe

F-программа обменивается данными с сигнальными модулями повышенной безопасности через **ProfiSafe**, ориентированный на обеспечение безопасности протокол шины PROFIBUS DP/PA. Этот протокол обеспечения безопасности реализуется в F-программе в отказобезопасных драйверных блоках, а также в программах ПЗУ сигнальных модулей повышенной безопасности.

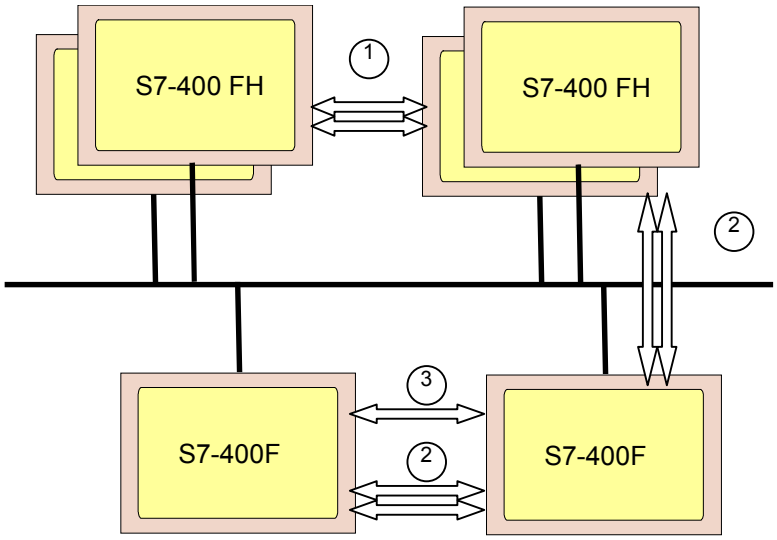
Ориентированный на обеспечение безопасности обмен данными между F-программой и сигнальными модулями повышенной безопасности осуществляется посредством циклической передачи данных пользователя. Важным параметром для этого является время контроля, задаваемое во время проектирования сигнальных модулей повышенной безопасности и автоматически передаваемое отказобезопасным драйверным блокам в качестве входного параметра.

Обмен данными между CPU и сигнальными модулями повышенной безопасности, не связанный с обеспечением безопасности

Для обмена данными между CPU и сигнальными модулями повышенной безопасности, не связанного с обеспечением безопасности, могут использоваться обычные механизмы – прямой доступ, обращение к образу процесса или к записям. Например, диагностическая информация, не имеющая значения для обеспечения безопасности, передается ациклически из сигнальных модулей повышенной безопасности путем передачи записей.

3.9.4 Ориентированный на обеспечение безопасности обмен данными между CPU

Возможности обмена данными



Ориентированный на обеспечение безопасности обмен данными между CPU осуществляется через спроектированные стандартные или отказоустойчивые S7-соединения.

Номер	Передача данных от...	в	Вид соединения	Ориентирован на обеспечение безопасности
1	S7-400FH	S7-400FH	S7-соединение, отказоустойчивое	Да
2	S7-400F/FH	S7-400F	S7-соединение, отказоустойчивое	Да
3	S7-400F	S7-400F	S7-соединение	Да

Для ориентированного на обеспечение безопасности обмена данными между F-программами на различных CPU имеются в распоряжении отказобезопасные блоки F_SEND*data type* и F_RCV*data type*. Это означает, что *фиксированное* количество параметров типов F_*data* может быть передано надежно. Типом F_*data* может быть F_BOOL или F_REAL.

Указание по безопасности

Ориентированный на обеспечение безопасности обмен данными между CPU через сети общего пользования недопустим.

Обмен данными между стандартными CPU

Непосредственный обмен данными между F-программой и стандартным CPU невозможен. Обмен данными может осуществляться в стандартной программе на F-CPU только после преобразования F-типов данных в стандартные типы данных посредством блока преобразования. Обмен данными в стандартной программе использует стандартные коммуникационные функции.