4 Проектирование

4.1 Обзор

В этом разделе показаны основные различия между проектированием системы повышенной безопасности и стандартной системы S7. В нем также рассматриваются специальные свойства функций устройства программирования, на которые необходимо обращать особое внимание при работе с отказоустойчивой системой.

4.2 Конфигурирование и параметризация аппаратуры

Основная последовательность действий при проектировании системы повышенной безопасности не отличается от последовательности действий для стандартной системы S7, т.е. она состоит из следующих шагов:

- Создание проектов и станций
- Конфигурирование аппаратуры и сети
- Загрузка системных данных в ПЛК

Отдельные шаги, необходимые для конфигурирования, также в значительной степени идентичны шагам при конфигурировании S7-400. Для изменения значений параметров отказоустойчивой системы всегда необходима авторизация.

Правила для систем повышенной безопасности

В дополнение к правилам, которые обычно применяются для размещения модулей в S7-400, в случае системы повышенной безопасности должны выполняться следующие условия:

- ET 200M может содержать только сигнальные модули повышенной безопасности или стандартные сигнальные модули и сигнальные модули повышенной безопасности в стандартном режиме.
  Исключение: Стандартный модуль S7-300 SM 331; AI 2 x 12Bit (номер для заказа 6ES7 331-7TB00-0AB0) может использоваться вместе с сигнальными модулями повышенной безопасности в режиме обеспечения безопасности в ET 200M.
- В режиме обеспечения безопасности сигнальные модули повышенной безопасности могут использоваться в ET 200M только с IM 153-2 FO.
- Отказобезопасная работа сигнальных модулей повышенной безопасности возможна только в адресной области от 8 до 8191. Используемые адреса должны быть установлены на сигнальном модуле повышенной безопасности с помощью переключателей и должны соответствовать сконфигурированным адресам.
- Для запуска CPU с F-программой пользователя для CPU должна быть активизирована соответствующая опция и запроектирован пароль.

- Если конфигурация сигнального модуля повышенной безопасности или CPU (времена циклов OB циклических прерываний) изменена, то F-программа должна быть снова скомпилирована и закружена в CPU.
- Перед загрузкой F-программы вы должны загрузить в CPU конфигурацию.

Указание по безопасности

Безопасная работа невозможна, если эти правила не выполняются.

4.3 Параметризация CPU

Правила проектирования CPU в качестве F-CPU

Указание по безопасности

Для CPU, содержащего F-программу пользователя, должны выполняться следующие правила.

- Должна быть выделена опция "CPU Contains Safety Program [CPU содержит программу обеспечения безопасности]".
- **Всегда** должен быть назначен пароль.

Эти настройки вы должны сделать через свойства объекта (object properties) в HW Config.

Последовательность действий

1. Выберите желаемый CPU в HW Config, а затем выберите команду меню **Edit > Object Properties [Редактировать > Свойства объекта]**.
2. выберите уровень защиты, который вы хотите установить для CPU, а затем введите пароль в предоставленном текстовом поле.
3. Выделите опцию "CPU Contains Safety Program [CPU содержит программу обеспечения безопасности]" в закладке "Protection [Защита]".

Важные параметры для CPU в системе S7-400FH

Чтобы воспрепятствовать контролю времени во время переключения главный / резервный, вы должны запроектировать OB3x, предоставляемый для F-программ с приоритетом > 15, в закладке "Cyclic Interrupts [Циклические прерывания]".

OB циклических прерываний F-программы должен быть запроектирован как "Cyclic Interrupt OB with Special Handling [OB циклических прерываний со специальной обработкой]". Только тогда это циклическое прерывание будет вызываться во время актуализации резерва для классов приоритета > 15 непосредственно перед началом блокировки времени. Для этого перейдите в закладку "H Parameters [Параметры отказоустойчивости]" в свойствах CPU, а затем введите в текстовом окне "Cyclic Interrupt OB with Special Handling [OB циклических прерываний со специальной обработкой]" номер OB циклических прерываний с наивысшим приоритетом, которому в CFC назначены блоки раздела F-программы.

4.4 Параметризация сигнальных модулей повышенной безопасности

Для параметризации сигнальных модулей повышенной безопасности имеются дополнительные опции, недоступные при параметризации сопоставимых стандартных модулей:

- Вы можете выбирать между режимом обеспечения безопасности (различные уровни) и стандартным режимом.
- Вы можете эксплуатировать сигнальные модули повышенной безопасности в режиме обеспечения безопасности с резервированием для увеличения коэффициента готовности (отказоустойчивости). Резервные модули для повышения коэффициента готовности могут быть вставлены в том же или в другом ET 200M или в той же или другой монтажной стойке.

К сигнальному модулю повышенной безопасности в режиме обеспечения безопасности нельзя обратиться непосредственно. К нему можно обращаться только через отказобезопасные драйверные блоки.

Динамическая параметризация посредством вызовов SFC возможна только в стандартном режиме. Этим способом нельзя перейти в режим обеспечения безопасности.

Дополнительную информацию о параметризации сигнальных модулей повышенной безопасности можно найти в руководстве /1/ и в контекстно-зависимой справочной информации в HW Config.

Символические имена

Замечание

Введите символическое имя для каждого входного или выходного канала спроектированных сигнальных модулей повышенной безопасности.

В случае сигнальных модулей повышенной безопасности, находящихся в режиме обеспечения безопасности, вы должны в CFC присвоить выводу VALUE каждого отказобезопасного драйверного блока канала символическое имя соответствующего канала.

Это обеспечивает автоматическое соответствие между параметрами модуля, сконфигурированными в HW Config (адреса, времена контроля и т.д.), и входами/выходами соответствующих отказобезопасных драйверных блоков каналов в CFC.

Если вы проектируете для цифровых модулей ввода анализ датчиков типа "1-из-2", то мы рекомендуем, чтобы вы пометили в таблице символов недоступные каналы (с 4 по 7 в SM 326; DI 8 x NAMUR и с 12 по 23 в SM 326; DI 24 x DC 24 V) как резервные.

Ввод имен модулей

Имя модуля повышенной безопасности можно ввести в HW Config. Это имя принимается за эталон для соответствующего отказобезопасного драйвера модуля (F_*Name*_x), если этот драйвер размещается автоматически. Это облегчает просмотр и контроль связи между отказобезопасным драйвером модуля и соответствующим сигнальным модулем повышенной безопасности.

Вводимое имя может иметь не более 12 символов, если соответствующие эталонные имена отказобезопасных драйверов модулей должны быть уникальными.

Для этого действуйте следующим образом:

1. Выберите желаемый сигнальный модуль повышенной безопасности в HW Config, а затем выберите команду меню **Edit > Object Properties [Редактировать > Свойства объекта]**.
2. Под **Name [Имя]** введите имя для сигнального модуля повышенной безопасности, используя не более 12 символов.

Если эталонное имя отказобезопасного драйвера модуля не уникально, то затем вы сможете проверить связь между этим драйвером и соответствующим сигнальным модулем повышенной безопасности только через логический адрес.

Групповая диагностика

Параметр "Group Diagnosis [Групповая диагностика]" включает и выключает передачу диагностических сообщений, относящихся к каналам (напр., обрыв провода, короткое замыкание) сигнальных модулей повышенной безопасности в CPU. Групповая диагностика **может быть выключена** на неиспользуемых входных или выходных каналах в интересах повышения коэффициента готовности. Это имеет следствием следующее поведение:

Модули ввода повышенной безопасности:

Если групповая диагностика каналов ввода выключена, то в случае неисправности безопасные нулевые значения также посылаются в CPU, но сообщения об ошибках в CPU не посылаются.

Модули вывода повышенной безопасности:

Если имеются неисправности каналов на выходах с выключенной групповой диагностикой, то происходит следующее:

- В случае неисправностей с выключением отдельных каналов, затронутые каналы модуля **не** выключаются.
- В случае неисправностей, при которых затронутая половина модуля (DO0...DO4 или DO5...DO9) выключена, эта половина модуля **выключается**.
- CPU **не** получает диагностического сообщения, а выходы **не** пассивируются, в зависимости от настройки на отказобезопасном драйверном блоке.

Указание по безопасности

В случае модулей ввода и вывода повышенной безопасности, находящихся в режиме обеспечения безопасности, групповая диагностика должна быть установлена для всех подключенных каналов.

Пожалуйста, проверьте, чтобы выключение групповой диагностики было фактически установлено только для неиспользуемых входных и выходных каналов.

4.5 Проектирование резервируемых сигнальных модулей повышенной безопасности

Замечание

В случае модулей, сконфигурированных с резервированием, вы должны обеспечить следующее:

- Чтобы оба модуля были одного типа и имели одинаковую параметризацию
- Чтобы на обоих модулях при параметризации было установлено одинаковое время контроля
- Чтобы в закладке "Inputs [Входы]" была выбрана опция "Safety Mode [Режим обеспечения безопасности]".

Например, для проектирования двух модулей ввода повышенной безопасности с резервированием действуйте следующим образом:

1. В HW Config вставьте в устройство (-а) ET 200M два сигнальных модуля повышенной безопасности.
2. Назначьте параметры первому модулю: В закладке "Inputs [Входы]" выберите опцию "Safety Mode [Режим обеспечения безопасности]" и установите любые дополнительные параметры.
3. Назначьте параметры второму модулю: В закладке «Inputs [Входы]» выберите опцию "Safety Mode [Режим обеспечения безопасности]" и установите **такие же** параметры, как для первого модуля.
4. Для второго модуля в закладке "Redundancy [Резервирование]" установите опцию "Redundancy 2x".
5. В диалоговом окне "Find Redundant Module [Поиск резервного модуля]" выберите желаемый модуль.
6. Если необходимо, вы можете установить длительность несоответствия для резервируемых цифровых модулей ввода.

4.6 Проектирование сетей и соединений

Проектирование сетей и соединений в системе повышенной безопасности отличается от аналогичных операций в стандартной системе S7 только в одном отношении:

Для ориентированного на обеспечение безопасности обмена данными между CPU требуются отказобезопасные функциональные блоки. Поэтому он возможен только между F-программами на F-CPU.

4.7 Функции устройства программирования в STEP 7

Для работы с системой повышенной безопасности в STEP 7 предоставляются в распоряжение те же функции, что и для стандартной системы S7.

Функции устройства программирования, имеющие значение для обеспечения безопасности

Функции устройства программирования, имеющие значение для обеспечения безопасности, исполняются только в том случае, если вы установили для себя права доступа. Следующие функции устройства программирования имеют значение для обеспечения безопасности и могут выполняться только после получения авторизации паролем для CPU, независимо от установленного уровня защиты:

- Загрузка всей программы из CFC или SIMATIC Manager
- Загрузка изменений F-программы из CFC
- Загрузка и удаление отказобезопасных блоков из SIMATIC Manager
- Загрузка в плату памяти СППЗУ на CPU
- Сброс памяти из CFC или SIMATIC Manager

Указание по безопасности

Вы не можете изменять переменные и значения на входах и выходах отказобезопасного блока в режиме online, используя, например, команду меню **PLC > Monitor/Modify Variables [ПЛК > Наблюдение/изменение переменных]**. Если такое изменение в отказобезопасном функциональном блоке обнаружено, то CPU, как правило, переходит в STOP.

Установка точек останова

Замечание

После запроса режима HOLD [фиксация] требуется запуск (холодный или теплый пуск).

4.8 Установка, изменение и отмена прав доступа

4.8.1 Установка прав доступа для CPU

Для установки прав доступа для CPU действуйте следующим образом:

1. Выделите CPU или его программу S7 в SIMATIC Manager.
2. Выберите команду меню **PLC > Access Rights > Setup [ПЛК > Права доступа > Установка]**, а затем введите в появившемся диалоговом окне пароль, назначенный при параметризации CPU в закладке "Protection [Защита]".

Права доступа имеют силу, пока они не отменены (**PLC > Access Rights > Cancel [ПЛК > Права доступа > Отменить]**) или пока не завершится последнее приложение S7.

Указание по безопасности

Если доступ к системе разработки (ES) или устройству программирования не ограничен только лицами, уполномоченными на изменение F-программ, то на ES или устройстве программирования должна быть обеспечена эффективность парольной защиты с помощью следующих организационных мероприятий:

- Пароль должен быть известен только лицам, имеющим полномочия.
- Лица, имеющие полномочия, должны явно отменять авторизацию при выходе из ES или устройства программирования. Если этого правила строго не придерживаются, то должен быть также использован хранитель экрана с паролем, известным только уполномоченным лицам.

Если в режиме обеспечения безопасности изменяется стандартная программа, то не следует получать права доступа, используя пароль для CPU, так как в противном случае может быть изменена и F-программа. Вместо этого соответствующим образом должен быть установлен уровень защиты.

После отмены прав доступа проверьте, если режим обеспечения безопасности активен, идентичны ли общий контрольный код F-программы в режиме online и общий контрольный код принятой F-программы. Если нет, снова загрузите правильную F-программу в CPU (см. разделы "Загрузка изменений" и "Сравнение F-программ").

Указание по безопасности

После небуферизованного холодного пуска текущий пароль удаляется из загрузочной памяти ОЗУ, и снова становится действительным старый пароль из платы памяти флэш-ППЗУ. Чтобы этот старый пароль на плате памяти флэш-ППЗУ не стал известен слишком многим людям, следует принять организационные меры.

Изменение пароля

Пароль можно изменить, только изменив конфигурацию.

Чтобы сделать это для S7-400F, вы должны перевести CPU в STOP.

Для S7-400FH пароль (конфигурацию) можно изменить, не прерывая процесса (в режиме RUN).

4.8.2 Ввод/изменение пароля для программы обеспечения безопасности

Чтобы ввести или изменить пароль для программы обеспечения безопасности, действуйте следующим образом:

1. Выделите CPU или его программу S7 в SIMATIC Manager.
2. Выберите команду меню **Options > Customize Safety Program [Дополнительные возможности > Настроить программу обеспечения безопасности]**
3. Выберите кнопку "Password...[Пароль…]" в появившемся диалоговом окне и введите пароль для программы обеспечения безопасности.

Указание по безопасности

Для улучшения защиты от доступа мы рекомендуем использовать разные пароли для CPU и для программы обеспечения безопасности.

Если вы еще не ввели пароль, то вы получите запрос на его ввод при первой компиляции F-программы (см. ниже "Запрос пароля для программы обеспечения безопасности").

Вы можете изменить пароль так же, как это делается под Windows 95/98/NT, однократным вводом старого пароля и двукратным вводом нового.

Пароль для программы обеспечения безопасности хранится автономно в ES или устройстве программирования вместе с программой обеспечения безопасности.

Запрос пароля для программы обеспечения безопасности

Диалоговое окно для запроса пароля для программы обеспечения безопасности отображается в следующих случаях:

- Компиляция изменений в F-программе
- Включение и выключение режима обеспечения безопасности
- Загрузка изменений в данные F-программы при выключенном режиме обеспечения безопасности
- Изменение F-констант в режиме тестирования CFC

4.8.3 Отмена прав доступа для программы обеспечения безопасности

Действительность пароля для программы обеспечения безопасности

После ввода пароля для программы обеспечения безопасности (после запроса или изменения) он действителен в течение часа. Во время сеанса редактирования F-программы (модификация, компиляция, деактивизация режима обеспечения безопасности, загрузка изменений) вам нужно ввести его только один раз. Через час вы должны ввести его снова.

Вы должны также снова ввести пароль, если последнее из указанных действий во время сеанса было выполнено более часа назад.

Указание по безопасности

Если доступ к системе разработки (ES) или устройству программирования не ограничен доступом только для лиц, уполномоченных на изменение F-программ, то на ES или устройстве программирования должна быть обеспечена эффективность парольной защиты с помощью следующих организационных мероприятий:

- Пароль должен быть известен только лицам, имеющим полномочия.
- Лица, имеющие полномочия, должны явно отменять авторизацию при выходе из ES или устройства программирования. Если этого правила строго не придерживаются, то должен быть также использован хранитель экрана с паролем, известным только уполномоченным лицам.

Отмена прав доступа

Вы можете в любой момент времени отменить права доступа с помощью пароля для программы обеспечения безопасности. Для этого действуйте следующим образом:

1. Выделите CPU или его программу S7 в SIMATIC Manager.
2. Выберите команду меню **Options > Customize Safety Program [Дополнительные возможности > Настроить программу обеспечения безопасности]**
3. Щелкните на кнопке «Password... [Пароль...]» в появившемся диалоговом окне.
4. В появившемся диалоговом окне "Password [Пароль]" щелкните на кнопке "Cancel Access Rights [Отменить права доступа]".