

# 1 Обзор продукта

## 1.1 Обзор

### Системы SIMATIC S7-400 повышенной безопасности

Программируемые контроллеры S7-400F/FH повышенной безопасности (F-системы, отказобезопасные системы) используются в системах с повышенными требованиями к обеспечению безопасности. Целью S7-400F/FH является управление процессами, которые могут быть немедленно возвращены в безопасное состояние. Иначе говоря, если эти процессы внезапно останавливаются, то это не представляет опасности для людей и окружающей среды.

#### Требования к безопасности

S7-400F/FH удовлетворяет следующим требованиям к безопасности:

- классы требований от AK1 до AK6 в соответствии с DIN V 19250/ DIN V VDE 0801
- от SIL1 до SIL3 (**S**afety **I**ntegrity **L**evel – уровень сохранности безопасности) в соответствии с IEC 61508
- категории с 1 по 4 в соответствии с EN 954-1

#### Принципы, лежащие в основе функций обеспечения безопасности

Безопасное поведение в случае отказа достигается с помощью функций обеспечения безопасности, в первую очередь, в программном обеспечении. Функции обеспечения безопасности выполняются программируемым контроллером S7-400F, чтобы вернуть систему в безопасное состояние или сохранить ее в безопасном состоянии при возникновении опасных ситуаций.

Безопасность для процесса может обеспечиваться посредством пользовательской функции обеспечения безопасности или с помощью функции реагирования на неисправность. Если система повышенной безопасности не может больше выполнять свою текущую пользовательскую функцию обеспечения безопасности в случае неисправности, она выполняет функцию реагирования на неисправность: например, соответствующие выходы выключаются, а CPU, если необходимо, переходит в состояние STOP.

**Например:** Система повышенной безопасности должна открыть клапан, если возникает избыточное давление (пользовательская функция обеспечения безопасности). При возникновении опасной неисправности в CPU все выходы выключаются (функция реагирования на неисправность), открывая, таким образом, клапан и возвращая остальные исполнительные устройства в безопасное состояние. Если бы система повышенной безопасности не была повреждена, то только открылся бы этот клапан.

Функции обеспечения безопасности встраиваются в первую очередь в следующие компоненты:

- в ориентированную на обеспечение безопасности программу пользователя в центральном процессоре
- в модули ввода-вывода повышенной безопасности

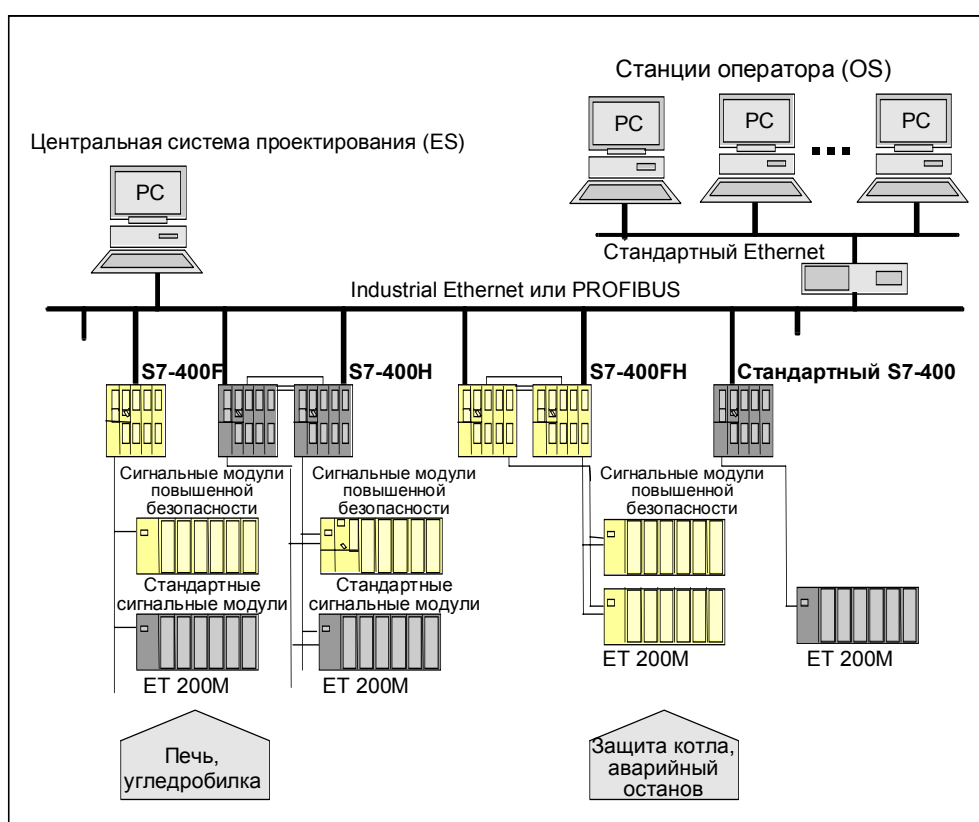
## Безопасность и коэффициент готовности

Чтобы увеличить коэффициент готовности системы автоматизации и, таким образом, избежать простоев в результате неисправностей в системе повышенной безопасности, такие системы могут быть, при желании, спроектированы для получения высокого коэффициента готовности (отказоустойчивости). Этот повышенный коэффициент готовности может быть достигнут с помощью резервируемых компонентов (блока питания, центрального процессора и систем связи и ввода-вывода).

Отказоустойчивые системы повышенной безопасности S7-400FH позволяют продолжать производство, не нанося вреда людям и окружающей среде.

## Использование в проектировании процессов

На следующем рисунке показаны возможности встраивания систем S7-400F и S7-400FH в систему автоматизации процессов с помощью PCS7.



## 1.2 Основные варианты конфигурации

В этом разделе описаны два основных варианта конфигурации систем повышенной безопасности:

- система повышенной безопасности S7-400F
- отказоустойчивая система повышенной безопасности S7-400FH

### Система повышенной безопасности S7-400F

**S7-400F** – это система автоматизации повышенной безопасности, состоящая, по крайней мере, из следующих компонентов:

- Модуль CPU, способный выполнять отказобезопасные программы пользователя (F-программы), например, CPU 417-4 H
- Один или несколько сигнальных модулей повышенной безопасности (F-SM) в устройстве децентрализованной периферии ET 200M (с возможностью резервирования)

На следующем рисунке показаны компоненты аппаратного и программного обеспечения системы повышенной безопасности. Вы можете расширить эту конфигурацию с помощью стандартных модулей S7-400 и S7-300.

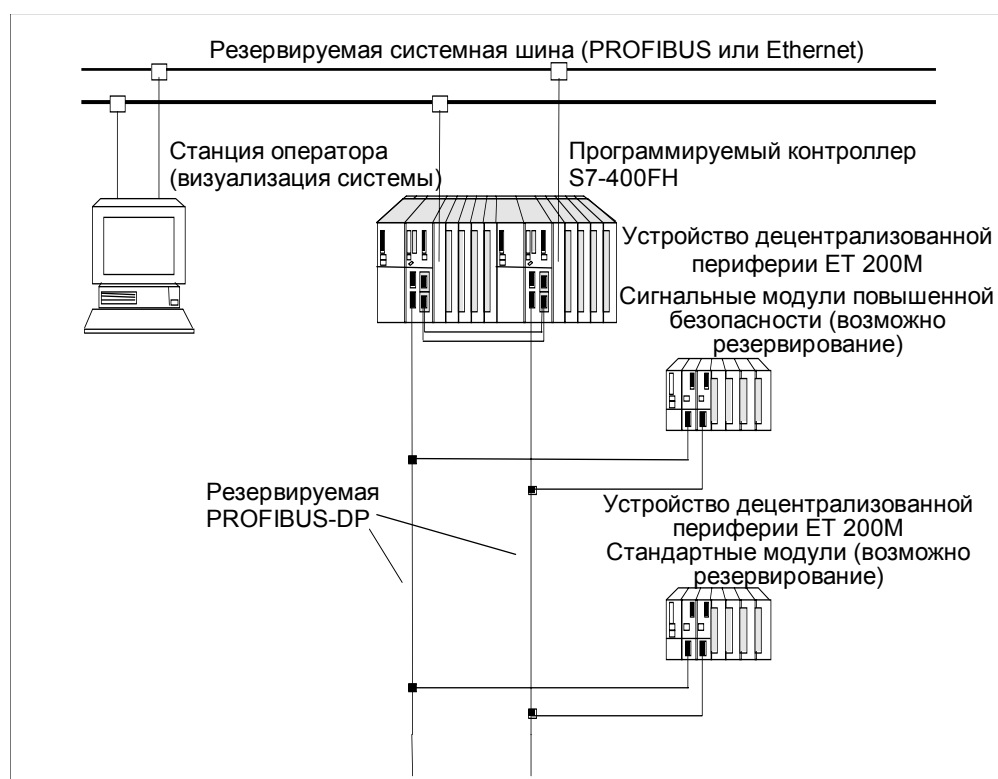


## Отказоустойчивая система повышенной безопасности S7-400FH

**S7-400FH** – это отказоустойчивая система автоматизации повышенной безопасности, состоящая, по крайней мере, из следующих компонентов:

- Отказоустойчивая система S7-400H (главная и резервная), исполняющая отказобезопасную программу пользователя (F-программу)
- Один или несколько сигнальных модулей повышенной безопасности (F-SM) в устройстве децентрализованной периферии ET 200M в качестве системы коммутируемой периферии (дополнительное резервирование)

На следующем рисунке показан пример конфигурации S7-400FH с резервируемым CPU, совместно используемыми, коммутируемыми децентрализованными периферийными модулями, подключенными через резервируемую системную шину.



## Комбинация стандартных, отказоустойчивых и отказобезопасных компонентов

Стандартные, отказоустойчивые (Н) и отказобезопасные (F) компоненты и системы могут использоваться совместно следующим образом:

- Стандартные системы, Н-системы, F-системы и FH-системы могут использоваться вместе в одной **системе**.
- Стандартные модули и сигнальные модули повышенной безопасности могут использоваться совместно в одной **системе автоматизации**. Стандартные модули и сигнальные модули повышенной безопасности в режиме обеспечения безопасности должны, однако, использоваться в отдельных устройствах децентрализованной периферии ET 200M.
- Программа пользователя, ориентированная на обеспечение безопасности, может выполняться вместе со стандартной программой пользователя, не относящейся к обеспечению безопасности, в системе повышенной безопасности (F) или в отказоустойчивой системе повышенной безопасности (FH).

Тот факт, что отказобезопасные (F), отказоустойчивые (Н) и стандартные компоненты могут комбинироваться, имеет следующие преимущества:

- Вы можете создать полностью интегрированную систему автоматизации, в которой можно использовать новинки стандартных CPU с компонентами повышенной безопасности независимо от наличия стандартных компонентов, например, FM или CP. Всю систему можно проектировать и программировать с помощью таких стандартных инструментальных средств, как HW Config и CFC.
- Тот факт, что вы можете комбинировать в одном CPU стандартные части программы и части программы, ориентированные на повышение безопасности, сокращает расходы на приемку, так как объектом процедур приемки являются только части программы, обеспечивающие повышение безопасности. Расходы на эксплуатацию также могут быть сокращены путем размещения максимально возможного количества функций в стандартном разделе, который может быть изменен во время работы.

### 1.3 Компоненты системы S7-400F

На следующем рисунке показаны компоненты аппаратного и программного обеспечения, необходимые для проектирования и эксплуатации S7-400F.



#### Взаимодействие компонентов

S7-400F состоит из аппаратных и программных компонентов, которые должны быть скомбинированы друг с другом для конфигурирования системы повышенной безопасности S7-400F.

##### Подключение сигнальных модулей повышенной безопасности

Сигнальные модули повышенной безопасности должны соединяться с датчиками и исполнительными устройствами таким образом, чтобы гарантировать достижение желаемого уровня безопасности.

##### Проектирование аппаратуры

Проектирование с помощью HW Config должно соответствовать конфигурации аппаратуры; это значит, что схема соединений периферийной системы должна быть отражена в настройке параметров. Должен быть запроектирован CPU, способный выполнять отказобезопасные программы пользователя (F-программы).

##### Создание F-программы пользователя

F-программа пользователя создается в CFC с использованием блоков из библиотеки "Failsafe Blocks [Отказобезопасные блоки]". Для соединения с сигнальными модулями повышенной безопасности используются отказобезопасные драйверные блоки, которым должны быть назначены параметры. Некоторые из этих параметров назначаются автоматически как результат конфигурирования аппаратуры сигнальных модулей повышенной безопасности.

При генерировании исполняемой F-программы автоматически выполняются тесты на безопасность и встраиваются дополнительные функции обнаружения неисправностей.

## 1.4 Аппаратные компоненты

Система повышенной безопасности состоит, с одной стороны, из аппаратных компонентов, удовлетворяющих требованиям безопасности, таких как:

- CPU, например, CPU 417-4H с лицензией на копирование отказобезопасных блоков (F copy license)
- Сигнальные модули повышенной безопасности (F-SM)

Систему повышенной безопасности можно также расширять с помощью стандартных компонентов S7-300 и S7-400.

### F-CPU

Для систем повышенной безопасности S7-400F и S7-400FH центральный процессор (напр., CPU 417-4H, начиная с версии V2.0) с лицензией на копирование отказобезопасных блоков (F copy license) используется или индивидуально, или как отказоустойчивая, главная или резервная, система. Лицензия на копирование отказобезопасных блоков позволяет использовать CPU как **F-CPU** (т.е. для исполнения на нем отказобезопасной программы пользователя).

F-CPU – это CPU, который разрешено использовать в S7-400F/FH. Он становится **F-CPU** только в том случае, если на нем исполняется F-программа пользователя. В ином случае на этом CPU исполняется стандартная программа S7. Возможна комбинация стандартной программы пользователя и F-программы, так как данные F-программы пользователя, ориентированные на обеспечение безопасности, защищены от влияния данных, не связанных с обеспечением безопасности. В этом случае CPU также должен быть спроектирован как F-CPU.

Разделы программы пользователя, имеющие значение для обеспечения безопасности, должны быть защищены паролем на CPU и в системе разработки или в устройстве программирования от несанкционированного доступа. Кроме того, в CPU выполняется полное самотестирование. Это обеспечивает большую вероятность обнаружения ошибок.

### Сигнальные модули повышенной безопасности

Имеются в распоряжении следующие сигнальные модули повышенной безопасности (F-SM):

- Цифровые модули ввода повышенной безопасности:
  - SM 326; DI 8 x NAMUR
  - SM 326; DI 24 x DC 24V
- Цифровые модули вывода повышенной безопасности SM 326; DO 10 x DC 24V/2A
- Аналоговые модули ввода повышенной безопасности SM 336; AI 6 x 13Bit; с диагностическим прерыванием.

Эти модули могут использоваться только в устройстве децентрализованной периферии ET 200M. Они могут использоваться также со стандартными CPU в приложениях, не имеющих отношения к обеспечению безопасности.

F-SM могут использоваться в одноканальной или резервируемой конфигурации:

- В отдельном устройстве децентрализованной периферии
- В двух или более устройствах децентрализованной периферии

## Стандартные компоненты

Ограничения для отказоустойчивых систем (руководство /4/) относятся к использованию стандартных компонентов.

Ограничения для стандартных компонентов в режиме обеспечения безопасности сигнальных модулей повышенной безопасности вы найдете в информации об обеспечении безопасности в главе 3 руководства /1/ "S7-300 Programmable Controller, Fail-Safe Signal Modules [Программируемый контроллер S7-300, Сигнальные модули повышенной безопасности]".

## Дополнительная информация

Подробные описания аппаратных компонентов для S7-400F и S7-400FH можно найти в следующих руководствах:

- *S7-400, M7-400 Programmable Controllers, Installation and Module Data*  
[Программируемые контроллеры S7-400, M7-400, Монтаж и Данные модулей]
- *Система автоматизации S7-400 H, Отказоустойчивые системы*
- *S7-300 Programmable Controller, Fail-Safe Signal Modules*  
[Программируемый контроллер S7-300, Сигнальные модули повышенной безопасности]



## 1.5 Программные компоненты

S7-400F имеет следующие программные компоненты:

- дополнительный пакет S7 F Systems [Системы S7 повышенной безопасности] на устройстве программирования для проектирования и программирования системы повышенной безопасности
- отказобезопасная программа пользователя (F-программа пользователя) на CPU

### Дополнительный пакет S7 F Systems

Дополнительный пакет S7 F Systems необходим для проектирования и программирования S7-400-F. Он дает:

- поддержку для проектирования сигнальных модулей повышенной безопасности с помощью HW Config
- библиотеку "Failsafe Blocks [Отказобезопасные блоки]" для создания F-программ пользователя
- поддержку для обработки F-программы пользователя и для встраивания функций обнаружения неисправностей в такой программе.

### Отказобезопасная программа пользователя

Ниже отказобезопасная программа пользователя называется просто **F-программой** или **программой обеспечения безопасности**.

F-программы создаются с помощью CFC с использованием отказобезопасных блоков, содержащихся в библиотеке, поставляемой вместе с дополнительным пакетом S7 F Systems. Отказобезопасные блоки содержат функции обнаружения неисправностей и реакций на неисправности, а также возможности для программирования функций обеспечения безопасности. Это значит, что они обеспечивают обнаружение отказов и неисправностей и инициирование надлежащей реакции, которая сохраняет систему повышенной безопасности в безопасном состоянии или возвращает ее в безопасное состояние.

Программа пользователя на CPU может состоять из разделов, не имеющих отношения к обеспечению безопасности (стандартная программа), и разделов, ориентированных на обеспечение безопасности (F-программа). F-программа записывается в отдельных схемах CFC. Комбинация отказобезопасных и стандартных блоков в одной схеме недопустима и обнаруживается при компиляции. Передачи данных между стандартной программой и F-программой выполняются через блоки преобразования.

Во время компиляции определенные функции обнаружения неисправностей и реакций на неисправности автоматически добавляются к F-программе. Дополнительный пакет S7 F Systems предоставляет также в распоряжение функции для сравнения F-программ и поддержки приема F-программ.

### Дополнительная информация

Подробную информацию можно найти в следующих разделах

- Проектирование
- Программирование
- Отказобезопасные блоки

и в контекстно-зависимой помощи.

## 1.6 Установка дополнительного пакета S7 F Systems

### Требования к программному обеспечению

На ПК или устройстве программирования должны быть установлены следующие пакеты программ:

- STEP 7, начиная с версии V5.0, + Service Pack 3
- CFC V5.2
- драйверные блоки PCS 7, начиная с версии V5.0, с пакетом Service pack 3
- системы S7 H, начиная с версии V5.1 (дополнительный, для S7-400FH)



#### Указание по безопасности

Недопустимо использование дополнительного пакета S7 F Systems с предыдущими версиями этих пакетов программ.

Для архивирования проекта S7-400F/FH должно иметься управление версиями.

---

Для установки дополнительного пакета S7 F Systems на Windows NT вам нужны права администратора.

### Установка дополнительного пакета

1. Запустите ПК или устройство программирования, на котором установлен базовый пакет программ STEP 7, и обратите внимание на то, чтобы не были открыты никакие приложения STEP 7.
2. Вставьте CD с дополнительным пакетом.
3. Вызовите на CD программу SETUP.EXE.
4. Выполняйте команды программы установки.

### Чтение Readme-файла

Readme-файл содержит важную новейшую информацию о программном обеспечении. Вы можете вывести этот файл на экран по завершении программы установки или открыть его позднее с помощью команды меню **Start > Simatic > Product Notes > English [Пуск > Simatic > Замечания о продукте > Английский язык]**. Он расположен в каталоге **S7ftl STEP 7**.

### Запуск дополнительного пакета

Дополнительный пакет не содержит приложений, которые должны запускаться явно. Поддержка проектирования и программирования систем повышенной безопасности встроена в SIMATIC Manager, HW Config и CFC.

## Отображение встроенной системы помощи

Для диалоговых окон дополнительного пакета имеется в распоряжении контекстно-зависимая справочная информация, которую вы можете вызвать в любое время при проектировании или программировании нажатием F1 или щелчком на кнопке **Help [Помощь]**. Дополнительную справочную информацию можно получить, выбрав команду меню **Help > Contents > Calling Help on Optional Packages > Working with F Systems [Помощь > Содержание > Вызов помощи для дополнительных пакетов > Работа с системами повышенной безопасности]**.

## Авторизация

Для дополнительного пакета S7 F Systems необходима авторизация. Авторизация для дополнительных пакетов может быть установлена так же, как и для STEP 7. Информацию о том, как устанавливать и работать с авторизационным компонентом, можно найти в readme-файле и в главной справочной системе STEP 7.

## 1.7 Работа с системами повышенной безопасности

В этом разделе описаны основные процедуры для работы с системами повышенной безопасности. Включены только те шаги, которые имеют значение для F-систем и отличаются от стандартной процедуры.

### Планирование системы

Задачи планирования, зависящие от процесса, такие как, например, определение схемы трубопроводов и оснащения средствами контроля, создание блок-схемы, создание списка точек измерения, определение структуры и т.д., здесь не описываются.

При планировании системы необходимые функции обеспечения безопасности определяются с помощью соответствующих уровней сохранности безопасности (Safety Integrity Levels, SIL). Из них выводятся требования к компонентам, необходимые для реализации функций обеспечения безопасности (ПЛК, датчикам, исполнительным устройствам). Эти решения влияют на другие задачи, например, монтаж аппаратуры, проектирование и программирование.



#### Указание по безопасности

При планировании важно строго разделять стандартные функции (не имеющие отношения к обеспечению безопасности) и функции, ориентированные на обеспечение безопасности.

---

## Основная процедура

Смонтируйте аппаратные средства S7-400F/FH
Установите адреса на сигнальных модулях повышенной безопасности с помощью DIP-переключателей Подключите модули в соответствии со схемой соединений
Спроектируйте установку
Выполните параметризацию CPU для программы обеспечения безопасности. Выполните параметризацию отказобезопасных сигнальных модулей в соответствии классом обеспечения безопасности и схемой соединений.
Создайте отказобезопасную программу
Разместите, соедините друг с другом и выполните параметризацию отказобезопасных функциональных блоков Сгенерируйте исполняемый код и загрузите его в CPU S7-400F/FH.
Введите систему в действие
Дайте эксперту возможность принять разделы, относящиеся к обеспечению безопасности, до включения режима обеспечения безопасности.
Обслуживание системы
Замена компонентов аппаратуры Изменение отказобезопасной программы Обновление операционной системы

