7 Безопасность

7.1 Стандарты, сертификаты и удостоверения о допуске к эксплуатации

Сертификация безопасности

Если вы заказываете лицензию на копирование отказобезопасных блоков (F copy license), то к продукту будет приложена копия сертификата Союза технического надзора (TÜV) для отказобезопасных компонентов системы S7-400F/FH.

Вы можете получить дополнительные копии этого сертификата, сопроводительное сообщение и Приложение 1 к описанию сертификата, озаглавленное
"Safety-Related Programmable Systems
SIMATIC S7-400F and S7-400FH [Программируемые системы повышенной безопасности SIMATIC S7-400F и S7-400FH]"
по запросу от:

Ms. Petra Bleicher
A&D AS E423
Факс: ++49 9621 80 3146

Замечание

Приложение 1 к описанию сертификата содержит допустимые номера версий и контрольные коды отказобезопасных компонентов S7-400F/FH, которые должны проверяться при приемке программы.

Описание сертификата содержит условия, которые в настоящее время должны выполняться при использовании S7-400F/FH.

Стандарты, относящиеся к функциональной безопасности

В следующих таблицах приведены стандарты, учтенные при разработке S7-400F/FH.

Текущие состояния и редакции стандартов и действующих в настоящее время условий можно найти в описании сертификата безопасности.

Стандарт	Название /Описание
DIN V 19250	Фундаментальные аспекты, подлежащие учету, для измерительного и управляющего оборудования
DIN V VDE 0801 Включая изменение A1	Принципы для компьютеров в системах повышенной безопасности
IEC 61508 - 1 … 7	Функциональная безопасность; системы повышенной безопасности
prEN 50159-1	Применение на железных дорогах; требования к отказобезопасному обмену данными в замкнутых системах передачи данных
prEN 50159-2	Применение на железных дорогах; требования к отказобезопасному обмену данными в открытых системах передачи данных

Технология

Стандарт	Название /Описание
DIN V 19251	Технологические процессы и технология управления – Защитное оборудование МС – Требования и мероприятия для безопасного функционирования
VDI / VDE 2180 - 1, 2 и 5	Защита промышленных технологических установок с помощью системы управления процессом
NE 31	Рекомендации NAMUR Обеспечение безопасности оборудования с помощью аппаратуры, используемой в процессе, и технологии управления
ISA S 84.01	Применение систем, оборудованных приборами для обеспечения безопасности, в обрабатывающей промышленности

Отопление

Стандарт	Название /Описание
EN 230 № 7.3	Моноблочные нефтяные топки
EN 298 № 7.3, 8, 9, 10	Автоматические системы управления газовыми горелками для газовых горелок и устройств для сжигания газа с вентиляторами и без вентиляторов
DIN V ENV 1954	Поведение при внутренних и внешних неисправностях электронных элементов повышенной безопасности газовых устройств
DIN VDE 0116 № 8, 9	Электрическое оборудование печей
pr EN 50156-1	Электрическое оборудование печей Часть 1: Правила планирования и конструирования применений

Безопасность машинного оборудования

Стандарт	Название /Описание
EN 60204-1	Безопасность машинного оборудования – Электрическое оборудование машин; часть 1: Общие требования
EN 954-1 кат. 2 – 4	Безопасность машинного оборудования – Отказобезопасные элементы систем управления - часть 1: Общие принципы проектирования

Стандарты и директивы, относящиеся к другим аспектам

Стандарт	Название /Описание
DIN EN 61131-2	Программируемые контроллеры – Требования к оборудованию и тестирование
EN 50178	Электронное оборудование для использования в силовых установках
DIN VDE 0110	Координация изоляции для оборудования внутри низковольтных систем
EN 60068	Тестирование окружающей среды
EN 55011	Пределы и методы измерения характеристик радиопомех промышленного, научного и медицинского высокочастотного оборудования
EN 50081-2	Электромагнитная совместимость (ЭМС); Стандарт общего излучения; часть 2: Промышленная среда
EN 50082-2	Электромагнитная совместимость (ЭМС); Стандарт общей помехоустойчивости; часть 2: Промышленная среда

7.2 Требования к безопасности

Стандартизованные требования к безопасности

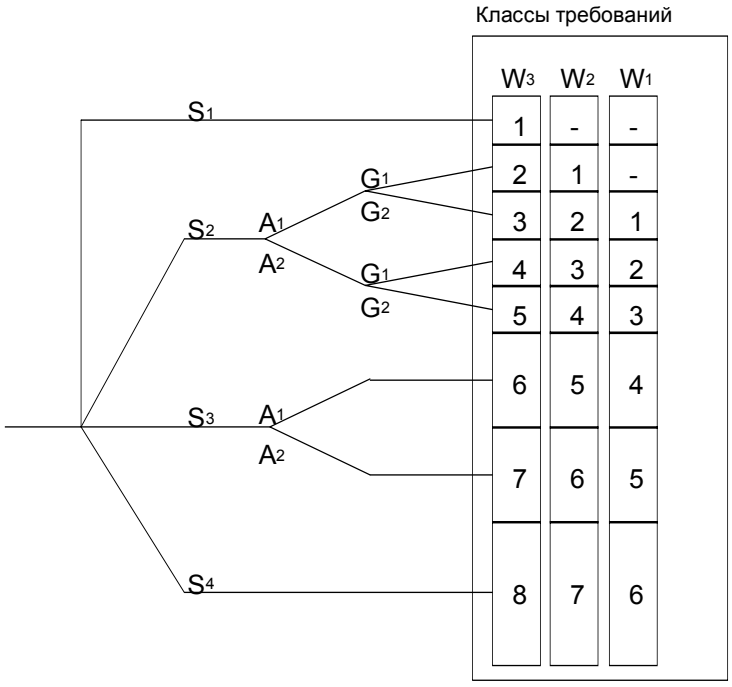
S7-400F/FH удовлетворяет следующим требованиям к безопасности:

- Классы требований AK1 - AK6 в соответствии с DIN V 19250/VDE 0801
- SIL1 - SIL3 (уровень сохранности безопасности) в соответствии с IEC 61508
- Категории 1 – 4 в соответствии с EN 954-1

Граф рисков и классы требований (AK) в соответствии с DIN V 19250

Классы требований (AK), соответствующие отдельным рискам, определены в DIN V 19250. Требования процесса могут быть разработаны с использованием параметров этих рисков. Классы требований (AK), которым должны удовлетворять контроллеры, могут быть установлены с помощью схем рисков.

Эта процедура приводит к классу требований AK для приложений, для которых не разработан производственный стандарт. Затем с помощью DIN V VDE 0801 могут быть установлены основные требования к безопасности. Если для приложения имеется производственный стандарт, то требования к безопасности отмечены в нем.



S_{1-4} Размер ущерба
A_{1-2} Длительность простоя
G_{1-2} Предотвращение опасности
W_{1-3} Вероятность возникновения нежелательных событий

Параметры рисков

Параметры рисков имеют следующие значения в соответствии с DIN V 19250:

Параметры	Значение
Степень повреждения или ущерба	
S1	Небольшие травмы; небольшие вредные воздействия на окружающую среду
S2	Серьезные необратимые телесные повреждения одного или нескольких лиц или гибель человека; Временные, серьезные вредные воздействия на окружающую среду
S3	Несколько смертельных случаев; Длительные, серьезные вредные воздействия на окружающую среду
S4	Катастрофические последствия, большое количество смертельных случаев
Частота и длительность воздействия	
A1	От редких до более частых
A2	От частых до постоянных
Возможность избежания опасности	
G1	Возможность при определенных обстоятельствах
G2	Редкая возможность
Вероятность возникновения нежелательных событий	
W1	Очень низкая
W2	Низкая
W3	Относительно высокая

Уровень сохранности безопасности в соответствии с IEC 61508

Для каждого уровня сохранности безопасности (Safety Integrity Level, SIL) стандарт IEC 61508 определяет в качестве степени достижения цели вероятность отказа функции обеспечения безопасности, поставленной в соответствие системе повышенной безопасности.

Уровень сохранности безопасности	**Работа в режиме редких запросов** (Средняя вероятность отказа выполнения функции при запросе)	**Работа в режиме частых или постоянных запросов** (Вероятность опасного выхода из строя в час)
4	от $\geq 10^{-5}$ до $< 10^{-4}$	от $\geq 10^{-9}$ до $< 10^{-8}$
3	от $\geq 10^{-4}$ до $< 10^{-3}$	от $\geq 10^{-8}$ до $< 10^{-7}$
2	от $\geq 10^{-3}$ до $< 10^{-2}$	от $\geq 10^{-7}$ до $< 10^{-6}$
1	от $\geq 10^{-2}$ до $< 10^{-1}$	от $\geq 10^{-6}$ до $< 10^{-5}$

Исполнительные устройства и датчики обычно вносят наибольший вклад в эти вероятности отказов.

Каждая функция обеспечения безопасности всегда содержит целую цепь от сбора и обработки информации до целенаправленных действий.

Используемое оборудование, такое как программируемый контроллер S7-400F/FH, датчики и исполнительные устройство, должно в целом выполнять AK и SIL, определенные в результате оценки опасности.

Если функции управления и соответствующие функции защиты реализуются вместе в одном и том же S7-400F/FH, то говорят о режиме работы с высокими или постоянными требованиями.

В следующей таблице приведены значения вероятностей выхода из строя отдельных компонентов S7-400F/FH:

	Режим работы с низкими требованиями (Средняя вероятность отказа для выполнения функции проектирования по запросу)	**Режим работы с высокими или постоянными требованиями** (Вероятность опасного выхода из строя в час)	**Интервал проверочных испытаний**
CPU, способный выполнять функции обеспечения безопасности	1,24E-04	1,42E-09	10 лет
SM 326; DO 10 x DC 24V/2A; с диагностическим прерыванием 6ES7 326-2BF00-0AB0	6,97E-06	7,96E-11	10 лет
SM 326; DI 24 x DC 24V; с диагностическим прерыванием 6ES7 326-1BK00-0AB0	1,55E-06 при SIL 2 4,99E-08 при SIL 3	1,77E-11 при SIL 2 5,70E-13 при SIL 3	10 лет
SM 326; DI 8 x NAMUR; с диагностическим прерыванием 6ES7 326-1RF00-0AB0	2,74E-06 при SIL 2 4,83E-08 при SIL 3	3,13E-11 при SIL 2 5,51E-13 при SIL 3	10 лет
SM 336; AI 6 x 13Bit; с диагностическим прерыванием 6ES7 336-1HE00-0AB0	4,96E-08 при SIL 3	5,66E-13 при SIL 3	10 лет
Обмен данными, связанными с обеспечением безопасности	1,00E-05	1,00E-09	

Вы можете получить вклад S7-400F/FH в вероятность отказа функции обеспечения безопасности сложением вероятностей отказа всех используемых CPU и сигнальных модулей повышенной безопасности S7-400F/FH. Резервируемые CPU при расчете учитываются однократно, резервируемые сигнальные модули повышенной безопасности учитываются дважды. Затем должен быть добавлен вклад отказобезопасного обмена данными. В реализацию функции обеспечения безопасности может быть вовлечено несколько систем S7-400F/FH.

Пример:

Функция обеспечения безопасности реализуется системой S7- 400FH. CPU и сигнальные модули повышенной безопасности, вовлеченные в реализацию функции обеспечения безопасности, перечислены в следующей таблице. Эти CPU и сигнальные модули повышенной безопасности используются в резервируемой конфигурации. Их интервал проверочных испытаний составляет 10 лет. Сигнальные модули повышенной безопасности находятся в режиме обеспечения безопасности для SIL 3. Режим работы с высокими требованиями:

CPU, сигнальные модули повышенной безопасности и оборудование для отказобезопасного обмена данными, вовлеченное в реализацию функции обеспечения безопасности.	**Количество**	**Резервирование**	**Вероятность опасного отказа в час**
CPU, способный выполнять функции обеспечения безопасности	1	Да	1,42E-09
SM 326; DO 10 x DC 24V/2A; с диагностическим прерыванием 6ES7 326-2BF00-0AB0	1	Да	1,59E-10
SM 326; DI 24 x DC 24V; с диагностическим прерыванием 6ES7 326-1BK00-0AB0	2	Да	2,28E-12
Отказобезопасный обмен данными			1,00E-09
Всего			**2,58E-09**

7.3 Конфигурация системы

Рамки конфигурации системы S7-400F/FH устанавливаются, главным образом, используемым CPU. Соответствующие значения вы можете найти в технических данных CPU в /3/, глава 5.

Ограничения, относящиеся к S7-400FH, можно найти в /4/ и в readme-файле в дополнительном пакете "S7 H Systems [Отказоустойчивые системы S7]".

В приложении A вы найдете сертифицированные компоненты аппаратуры и программного обеспечения системы повышенной безопасности в виде контрольных списков.

7.4 Времена контроля

7.4.1 Проектирование времен контроля для систем F/FH

Правила для времен контроля

При проектировании времен контроля вы должны принять во внимание как коэффициент готовности, так и безопасность системы F/FH:

- Коэффициент готовности: Чтобы временной контроль не запускался при отсутствии ошибки, выбранные времена контроля должны быть достаточно длинными.
- Безопасность: Чтобы не превысить допустимое время отказа, выбранные времена контроля должны быть достаточно короткими.

Времена контроля системы повышенной безопасности

Вы должны запроектировать следующие времена контроля для системы повышенной безопасности:

- Параметры отказобезопасных блоков:

Контроль	Блок	Параметр
Контроль времени F-цикла OB циклических прерываний, содержащего программу обеспечения безопасности	F_CYC_CO	MAX_CYC
Контроль отказобезопасного обмена данными между исполняемыми F-группами	F_R_R F_R_BO	TIMEOUT
Контроль отказобезопасного обмена данными между CPU	F_RCVR, F_RCVBO F_SENDR, F_SENDBO	TIMEOUT

- Параметры сигнальных модулей повышенной безопасности

Контроль	Параметр
Контроль отказобезопасного обмена данными между F-CPU и сигнальными модулями повышенной безопасности через ProfiSafe	Monitoring time [Время контроля] (диалоговое окно свойств (Properties) в HW Config)

Основная последовательность действий

Для проектирования времен контроля действуйте следующим образом:

1. Спроектируйте стандартную или отказоустойчивую систему. Необходимую информацию вы можете найти в соответствующих руководствах по аппаратным средствам и в системах оперативной помощи.
2. Спроектируйте конкретные времена контроля отказоустойчивой системы с учетом коэффициента готовности: Эти времена должны быть значительно больше минимальных времен контроля. Вы можете найти приближенные формулы в информации о расчете минимальных времен контроля или в таблице Excel STEP7\S7BIN\S7ftimeb.xls.
3. Используйте таблицу Excel STEP7\S7BIN\S7ftimeb.xls для расчета максимального времени реакции и проверьте, не превышено ли максимально допустимое время отказа для процесса.

Указание по безопасности

Чтобы *надежно* обеспечить обнаружение импульсов, время между двумя изменениями сигнала (длительность импульса) должно быть больше, чем соответствующее время контроля.

7.4.2 Расчет минимальных времен контроля

7.4.2.1 Контроль времени F-цикла

Время контроля ставится в соответствие входному параметру MAX_CYC отказобезопасных блоков F_CYC_CO.

Чтобы контроль не запускался при отсутствии неисправности, MAX_CYC должен быть больше, чем максимальное время цикла TCImax соответствующего OB циклических прерываний:

MAX_CYC > TCImax

TCImax должно иметь, по меньшей мере, такую же величину, как и спроектированное время цикла TCI OB циклических прерываний. В системе FH должно быть также принято во внимание максимальное время блокирования для классов приоритета > 15 (TP15) при актуализации. Таким образом, могут быть применены следующие приближенные формулы:

TCImax = TCI	в системе повышенной безопасности
TCImax = MAX (TCI; TP15)	в FH-системе с OB циклических прерываний со специальной обработкой
TCImax = TCI + TP15	в FH-системе с OB циклических прерываний без специальной обработки

Обратите внимание на следующее:

Время	**Описание**	**Где его найти?**
TCI	Спроектированное время цикла OB циклических прерываний	HW Config Свойства CPU, "Cyclic Interrupt [Циклическое прерывание], Execution [Выполнение]"
TP15	Максимальное время блокирования для классов приоритета > 15	HW Config Свойства CPU, "H Parameters [Параметры обеспечения отказоустойчивости]"

"Cyclic Interrupt OB with Special Handling [OB циклических прерываний со специальной обработкой]" – это параметр обеспечения отказоустойчивости CPU в системе S7-400FH. Этот параметр содержит номер OB циклических прерываний, который вызывается отдельно операционной системой, когда актуализируется резерв, после блокирования всех прерываний. Обычно вводится номер OB циклических прерываний с наивысшим приоритетом, которому в CFC поставлены в соответствие отказобезопасные блоки F-программы.

Замечание

Для активизации контроля максимального времени блокирования для классов приоритета > 15 вы должны присвоить этому параметру значение в HW Config (Свойства CPU, закладка "H Parameters" [Параметры обеспечения отказоустойчивости]).

7.4.2.2 Контроль отказобезопасного обмена данными между F-CPU и сигнальными модулями повышенной безопасности

Контроль времени ProfiSafe в сигнальном модуле повышенной безопасности *и* в отказобезопасном драйвере осуществляется с *одной и той же* периодичностью. Значение, введенное и назначенное в HW Config, как время контроля сигнального модуля повышенной безопасности автоматически назначается отказобезопасным драйверам при компиляции (TIMEOUT).
Чтобы контроль не запускался ни в отказобезопасном драйвере, ни в сигнальном модуле повышенной безопасности при отсутствии неисправностей, выбранное время контроля ProfiSafe TPSTO должно быть достаточно большим:

TPSTO > 2* TTR + TF SM, ACK + MAX(TCImax; TCI + TDP_FD) + TDP_SO + TSLAVE_SO

Обратите внимание на следующее:

Время	**Описание**	**Где его найти?**
TCI	Спроектированное время цикла OB циклических прерываний	HW Config Свойства CPU, "Cyclic Interrupt [Циклическое прерывание], Execution [Выполнение]"
TCImax	Максимальное время цикла соответствующего OB циклических прерываний	Раздел "Контроль времени F-цикла"
TTR	Максимальное целевое время повторения для master-системы DP	Свойства master-системы DP, параметры шины в HW Config
TDP_FD	Макс. время обнаружения неисправности DP	Свойства master-системы DP, параметры шины, закладка "H Parameters [Параметры обеспечения отказоустойчивости]" в HW Config
TDP_SO	Макс. время переключения DP	Свойства master-системы DP, параметры шины, закладка "H Parameters [Параметры обеспечения отказоустойчивости]" в HW Config
TSLAVE_SO	Максимальное время переключения для активного канала связи в коммутируемой системе ввода/вывода	В технических данных коммутируемого slave-устройства DP (ET200M)
TF SM, ACK	Максимальное время квитирования сигнального модуля повышенной безопасности в режиме обеспечения безопасности	Это время можно найти в технических данных сигнального модуля повышенной безопасности в главах 9 и 10 руководства по сигнальным модулям повышенной безопасности.

Замечание

Чтобы *проверить во время работы*, не слишком ли малы спроектированные времена контроля ProfiSafe, вы можете вставить в ET 200M с сигнальными модулями повышенной безопасности, находящимися в режиме обеспечения безопасности, *дополнительные* сигнальные модули повышенной безопасности в режиме обеспечения безопасности, в которых запроектированное время контроля ProfiSafe *меньше*. Это особенно рекомендуется в том случае, если запроектированное время контроля ProfiSafe, подлежащее проверке, не слишком превышает минимально возможное время контроля ProfiSafe.

7.4.2.3 Контроль отказобезопасного обмена данными между CPU

Контроль времени в F-блоках F_SENDR и F_RCVR или F_SENDBO и F_RCVBO соответственно происходит с *такой же* периодичностью, которая должна быть установлена при параметризации на *обоих* блоках (TIMEOUT).

Чтобы контроль не запускался в F_SENDR и F_SENDBO или в F_RCVR и F_RCVBO, когда нет ошибок, выбранное время контроля TIMEOUT должно быть достаточно большим:

TIMEOUT > T CI,F_SEND + T CI,F_RCV + MAX(TDelay,F_SEND; TDelay,F_RCV) + 2*TUSEND

Обратите внимание на следующее:

Время	**Описание**	**Где его найти?**
TCI,F_SEND	Спроектированное время цикла OB циклических прерываний с вызовом F_SENDBO или F_SENDR	HW Config Свойства CPU, "Cyclic Interrupt [Циклическое прерывание], Execution [Выполнение]"
TCI,F_RCV	Спроектированное время цикла OB циклических прерываний с вызовом F_RCVBO или F_RCVR	HW Config Свойства CPU, "Cyclic Interrupt [Циклическое прерывание], Execution [Выполнение]"
TDelay,F_SEND	Максимальная задержка обмена данными, когда резерв в FH-системе актуализируется, с вызовом F_SENDBO или F_SENDR	Свойства передающего CPU, "H Parameters [Параметры обеспечения отказоустойчивости]"
TDelay,F_RCV	Максимальная задержка обмена данными, когда резерв в FH-системе актуализируется, с вызовом F_RCVBO или F_RCVR	Свойства принимающего CPU, "H Parameters [Параметры обеспечения отказоустойчивости]"
TUSEND	Максимальное время реакции USEND • с 48 байтами данных пользователя *для F_SENDBO* • с 88 байтами данных пользователя *для F_SENDR*	Информацию можно найти в Интернете (см. ниже)

Поиск TUSEND

Вы можете загрузить инструмент для расчета значения TUSEND из Интернета по адресу:

http://www4.ad.siemens.de:8080/intracs/livelink.exe?func=cslib.csinfo&table=ProductNodes&lang=de&nodeID=2526

ID взноса 1651770

Замечание

Для активизации контроля максимальной задержки обмена данными, когда резерв в FH-системе актуализируется, вы должны присвоить значение этому параметру в HW Config (Свойства CPU, "H Parameters [Параметры обеспечения отказоустойчивости]").

Одновременная актуализация в обоих CPU не допускается.

7.4.2.4 Контроль отказобезопасного обмена данными между исполняемыми F-группами

Контроль времени происходит в FB F_R_BO и F_R_R и назначается там во входном параметре TIMEOUT.

Чтобы контроль не запускался при отсутствии неисправностей, время контроля TIMEOUT должно иметь, по меньшей мере, такую же величину, как и большее из двух максимальных времен цикла циклических прерываний F_S_R и F_S_BO или F_R_R и F_R_BO:

TIMEOUT > MAX(TCimax, F_S; TCImax, F_R)

Обратите внимание на следующее:

Время	**Описание**	**Где его найти?**
TCImax, F_S	Максимальное время цикла OB циклических прерываний с вызовом F_R_BO или F_R_R	Контроль времени F-цикла
TCImax, F_R	Максимальное время цикла OB циклических прерываний с вызовом F_S_BO или F_S_R	Контроль времени F-цикла

7.5 Приемка системы повышенной безопасности

7.5.1 Приемка системы повышенной безопасности

Система повышенной безопасности обычно принимается независимым экспертом.

Во время приемки системы повышенной безопасности вам оказывают поддержку специальные функции в SIMATIC Manager. Они дают вам возможность:

- сравнивать F-программы
- протоколировать F-программы
- печатать F-программы

Информацию об этих темах можно найти в разделе 5.4.

Указание по безопасности

Для архивирования проекта S7-400F/FH должно иметься в распоряжении управление версиями. Кроме того, мы рекомендуем вам архивировать каждый принятый проект в STEP 7, а для изменений создавать новый проект.

При приемке системы должны быть приняты во внимание все требования, которые содержатся в описании сертификата и должны быть проверены.

Вы можете заархивировать все данные, имеющие значение для приемки отказоустойчивой системы, в SIMATIC Manager (**File > Archive [Файл > Архивировать]**) и распечатать их в нужном виде.

Контрольные списки для приемки

Вы можете найти в приложении следующие контрольные списки. Они могут быть использованы при приемке S7-400F/FH:

- Контрольный список для жизненного цикла программируемых контроллеров повышенной безопасности содержит сводку действий за время жизненного цикла системы повышенной безопасности S7-400F/FH, а также ссылки на требования и правила, которые должны быть удовлетворены.
- Контрольный список сертифицированных модулей
- Контрольный список сертифицированных блоков

7.5.2 Начальная приемка F-программы

Основная последовательность действий для начальной приемки F-программы

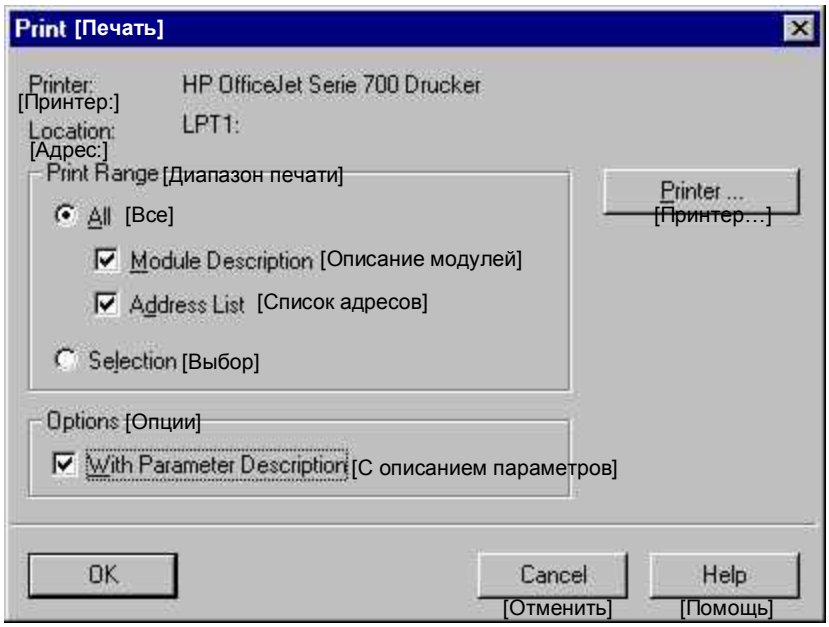
1. По желанию: предварительная приемка проекта сигнальных модулей повышенной безопасности
2. Сохранение программы
3. Проверка распечатки
4. Загрузка программы в CPU
5. Выполнение тестирования всех функций

Необязательная предварительная приемка проекта сигнальных модулей повышенной безопасности

После конфигурирования аппаратуры и параметризации сигнальных модулей повышенной безопасности вы можете выполнить начальную приемку проекта сигнальных модулей повышенной безопасности.

Данные конфигурации аппаратуры должны быть распечатаны, сохранены и заархивированы вместе со всем проектом STEP 7.

Распечатайте F-программу из SIMATIC Manager, используя команду меню **File > Print [Файл > Печатать]**. Для получения полной распечатки выберите диапазон и опции печати, как показано на следующем рисунке:



После проверки параметров сигнального модуля повышенной безопасности, связанных с обеспечением безопасности, CRC параметров на распечатке параметров сигнальных модулей повышенной безопасности достаточно в качестве эталона для последующей приемки. Они следующие:

- CRC параметров (вкл. адрес): 12345
- CRC параметров (без адреса): 54321

Сигнальные модули повышенной безопасности, которые обязаны иметь такие же параметры, связанные с обеспечением безопасности, могут быть

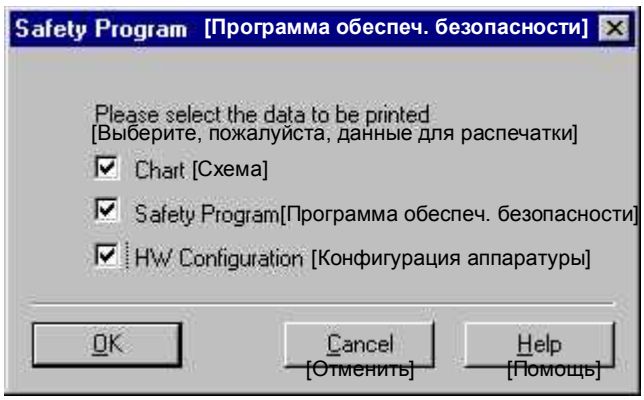
скопированы во время проектирования. Эти их параметры не нужно больше проверять индивидуально: Достаточно сравнить 'Parameter CRC (without address) [CRC параметров (без адреса)]' скопированных сигнальных модулей повышенной безопасности с CRC параметров (без адреса) уже проверенных сигнальных модулей повышенной безопасности и проверить логические начальные адреса.

Сохранение программы

F-программа, подлежащая приемке, должна быть сохранена и заархивирована вместе со всем проектом STEP 7. Все данные проекта (информация о программе, схемы CFC, данные конфигурации аппаратуры и протоколы) должны быть распечатаны и заархивированы вместе с проектом STEP 7. Как сохранять и архивировать проекты S7, можно узнать в основной справочной системе STEP 7.

Проверка распечатки

Распечатайте весь проект, как описано в разделе "Распечатка F-программы".



Распечатка содержит общий контрольный код в качестве эталона. Общий контрольный код появляется в распечатке дважды, один раз в разделе информации о программе как значение папки блоков и один раз в нижнем колонтитуле как значение из источника. Эти значения должны соответствовать друг другу.

В нижнем колонтитуле распечатки появляется номер версии дополнительного пакета "S7 F Systems [Системы повышенной безопасности S7]", он должен быть проверен.

Если общий контрольный код в нижнем колонтитуле не распечатывается, это значит, что изменилась F-программа или конфигурация (HW Config или NetPro). В этом случае F-программа должна быть скомпилирована снова.

Проектирование

- Сигнальные модули повышенной безопасности, у которых должны быть такие же параметры, имеющие значение для обеспечения безопасности, могут быть скопированы во время проектирования. Эти их параметры не нужно больше проверять индивидуально: Достаточно сравнить 'Parameter CRC (without address) [CRC параметров (без адреса)]' скопированных сигнальных модулей повышенной безопасности с CRC параметров (без адреса) уже проверенных сигнальных модулей повышенной безопасности и проверить логические начальные адреса.
- После предварительной приемки проекта сигнального модуля повышенной безопасности достаточно сравнить 'Parameter CRC (incl. address) [CRC параметров (вкл. адрес)]" в новой распечатке с этими данными в принятой распечатке проекта.

Программирование

В распечатке должны быть проверены следующие параметры отказобезопасных блоков:

- В распечатке должны быть проверены все входные параметры, связанные с обеспечением безопасности, которые не назначены автоматически, или в схемах CFC, или в разделе параметров, связанных с обеспечением безопасности. Входные параметры, которые не видны в схемах CFC, распечатываются в разделе параметров, связанных с обеспечением безопасности. Если параметры легче проверять в схеме, чем в разделе параметров, связанных с обеспечением безопасности , то эти параметры не должны быть скрытыми.
- У каждого отказобезопасного драйвера модуля должно быть проверено назначение, сделанное отказобезопасным драйверам каналов на выводах CHADDRxx, с помощью тестирования функций или просмотром распечатки.
- Начальные значения выходных параметров, связанных с обеспечением безопасности, должны быть проверены, если последовательность исполнения не соответствует потоку данных, т.е. если блок вызывается только после того, как выходные параметры были переданы другому блоку. Это происходит, например, при наличии обратной связи. Эти выходные параметры распечатываются в разделе параметров, связанных с обеспечением безопасности, и помечаются символом (*).
- У следующих отказобезопасных блоков должны быть проверены определенные входы/выходы:

Отказобезопасный блок	**Вход/выход**	**Описание**
F_CYC_CO	MAX_CYC	Максимально допустимое время F-цикла
F_SENDBO, F_RCVBO F_SENDR, F_RCVR	TIMEOUT	Время контроля при обмене данными между F-CPU
F_R_R, F_R_BO	TIMEOUT	Время контроля при обмене данными между исполняемыми F-группами
F_M_DI8 F_M_DI24 F_M_DO10 F_M_AI6	TIMEOUT	Время контроля для обмена данными ProfiSafe с сигнальным модулем повышенной безопасности
F_M_DI8 F_M_DI24 F_M_DO10 F_M_AI6	LADDR LADDR_R	Логический адрес модуля (SM1) Логический адрес резервного модуля (SM2)
F_M_AI6	MODE_00 … MODE_05	Кодирование диапазона измерений в случае аналогового модуля ввода
F_CH_DI, F_CH_DO, F_CH_AI	ACK_NEC	Квитирование, необходимое для повторного включения в систему
F_LIM_HL	QH	1: Нарушена верхняя граница
F_LIM_LL	QL	1: Нарушена нижняя граница
F_RS_FF	Q	Выход
F_SR_FF	Q	Выход
F_CTUD	CV	Текущее значение счетчика

Коммутируемые выходные параметры отмечены в распечатке звездочкой (*).

Проверка контрольных кодов

Общий контрольный код: После загрузки программы в CPU (см. разделы "Загрузка всей F-программы" и "Загрузка изменений") вы должны сравнить общий контрольный код программы в CPU с общим контрольным кодом в принятой распечатке. В случае систем S7-400FH вы должны сделать это сравнение для обоих CPU.

Контрольные коды и контрольные коды начальных значений отказобезопасных блоков: Контрольные коды и контрольные коды начальных значений всех отказобезопасных блоков должны совпадать с их величинами в Приложении 1 описания сертификата. Если вы используете вновь созданные типы отказобезопасных блоков, вы должны выполнить это сравнение для всех отказобезопасных блоков, вызываемых в этом типе F-блока.

Вы можете получить общий контрольный код программы и контрольные коды блоков в CPU выбором команды меню **Options > Customize Safety Program [Дополнительные возможности > Настроить программу обеспечения безопасности]**. Когда делается сравнение с программой в режиме online, оно показывает, соответствуют ли друг другу источник, загрузочная и рабочая память (это дает возможность обнаружить недопустимые манипуляции с данными у отказобезопасных входных параметров, не включенных в систему соединений, в рабочей памяти).

Вы можете проверить, действительно ли F-программа в CPU является той принятой программой, которую вы ожидали, выполнив следующие шаги:

1. Выберите в SIMATIC Manager команду меню **Options > Customize Safety Program [Дополнительные возможности > Настроить программу обеспечения безопасности]** и активизируйте "Online" в диалоговом окне. Контрольный код, отображаемый в диалоговом окне, должен совпадать с контрольными кодами в принятой распечатке (в тексте и в нижнем колонтитуле).
2. Для обнаружения недопустимых манипуляций (напр., через режим тестирования в CFC) в рабочей памяти CPU, выберите "Compare... [Сравнить…]" и сравните принятую программу с онлайновой программой в диалоговом окне. Здесь отображаются все параметры, с которыми были выполнены манипуляции. Этот шаг обязателен для приемки.
3. У отказоустойчивых систем S7-400FH вышеприведенные шаги должны быть выполнены для обоих CPU в онлайновом отображении SIMATIC Manager.

Если вы повторяете загрузку или проверку F-программы, выполните эту проверку общего контрольного кода снова.

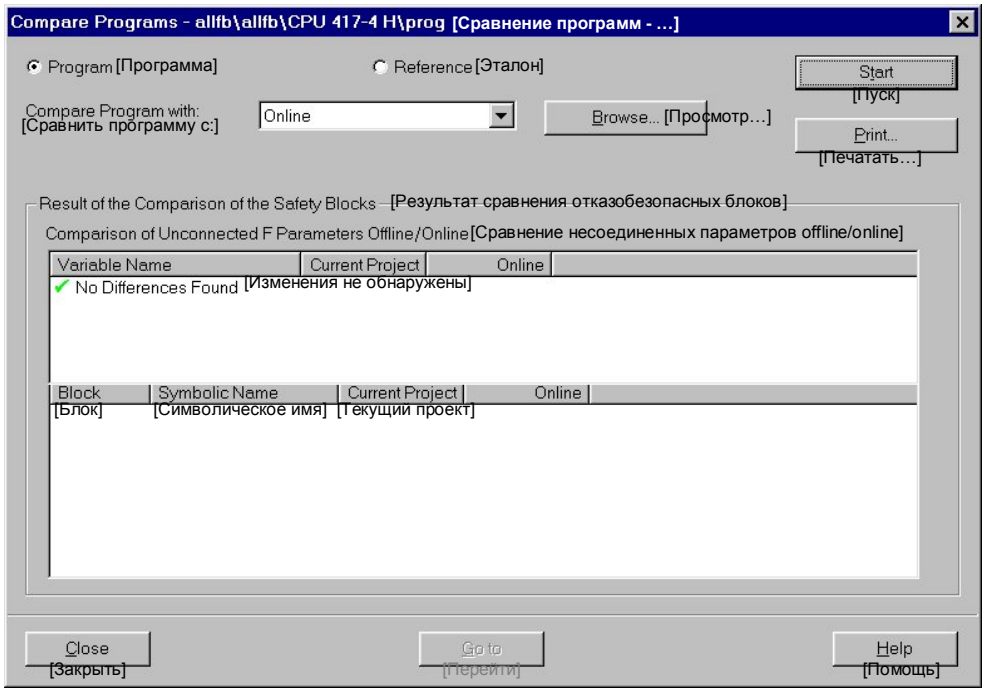
7.5.3 Приемка изменений в F-программе

Для приемки изменений в F-программе действуйте следующим образом:

1. Сохранение программы
2. Сравнение новой программы с принятой (см. раздел "Сравнение F-программ").
3. Проверьте изменения в распечатке
4. Загрузите новую программу в CPU
5. Выполните функциональное тестирование изменений

При проверке распечатки и выполнении функционального тестирования, следует проверять только новые разделы и разделы, содержащие изменения.

Чтобы их выявить, новая программа сравнивается с принятой программой.



Пояснение к рисунку: Variable Name – имя проекта.

Принятая программа должна быть сохранена в другом проекте. Щелкните на "Browse [Посмотреть]" и введите путь для принятой программы.

Изменения проекта сигнальных модулей повышенной безопасности, имеющие значение для обеспечения безопасности, можно распознать по изменению параметров CRC_IMP1 и CRC_IMP2 соответствующего отказобезопасного драйвера модуля (F_M_xx).

Изменения адресов и символических имен сигналов можно распознать по изменению параметра ADDR_CODE соответствующего отказобезопасного драйвера канала (F_CH_xx).

Изменения проекта сети в NetPro можно распознать по изменению параметра CRC_IMP соответствующих отказобезопасных коммуникационных блоков (F_RCVxx и F_SENDxx).

Правила и информацию о том, как нужно действовать в случае изменений в F-программе, вы можете найти в разделе "Эксплуатация и обслуживание, Изменение F-программы".

7.5.4 Приемка типовых F-блоков

Начальная приемка

Вновь созданный типовой F-блок в первый раз принимается так же, как и F-программа. Функциональное тестирование типового F-блока должно производиться в среде тестирования в специальной F-программе.

При приемке новых типовых F-блоков существенны общий контрольный код и контрольный код начальных значений нового типового F-блока. Для этих контрольных кодов должно быть выполнено сравнение с распечаткой приемки. Должны быть также проверены контрольные коды и контрольные коды начальных значений вызываемых отказобезопасных блоков.

Общие контрольные коды в нижних колонтитулах распечаток программы обеспечения безопасности и схемы CFC типового F-блока должны совпадать, или этот типовой блок должен быть снова скомпилирован.

Приемка изменений

Приемка изменений в типовом F-блоке выполняется так же, как для F-программы. Все пункты в тестируемой F-программе, в которых вызывается новый типовой F-блок, также должны быть проверены посредством функционального тестирования. Измененные контрольные коды отказобезопасных блоков отображаются в схемном представлении при сравнении F-программ.

7.5.5 Ответственность и квалификация

Требования к безопасности, относящиеся к специфическому для системы использованию S7-400F/FH, могут быть удовлетворены следующим распределением ответственности:

- Эксперты по процессу и операторы – за концепцию обеспечения безопасности системы, включая определение функций, имеющих значение для обеспечения безопасности и не имеющих значения для обеспечения безопасности.
- Независимый эксперт – за приемочные испытания системы в части обеспечения безопасности.
- Планировщики S7-400F/FH – за реализацию концепции обеспечения безопасности системы в части функционирования, конфигурации и подключения схем, за планирование интерфейсов отказоустойчивой системы, соответствие и реализацию предписаний из описания сертификата и ввод паролей в STEP 7
- Специалисты по монтажу и вводу в эксплуатацию S7-400F/FH – за реализацию и удовлетворение требований, относящихся к окружающей среде, в месте установки, безошибочную реализацию подключения схем, загрузку разрешенной F-программы в CPU и назначение пароля для CPU.
- Специалисты по вводу в эксплуатацию S7-400F/FH – за функциональное тестирование приемки с имитацией критериев отключения в соответствии с концепцией обеспечения безопасности системы и измерение необходимых для обеспечения безопасности времен.