# HIMatrix

## Безопасная система управления

# Руководство по безопасности HIMatrix

## (HIMatrix Safety Manual)


HIMA Paul Hildebrandt GmbH

Системы автоматизации производства

(1538)

HI 800 393 RU

Все названные в данном руководстве HIMA изделия защищены товарным знаком. То же самое распространяется, если не указано другое, на прочих упоминаемых изготовителей и их продукцию.

Все технические характеристики и указания, представленные в данном руководстве, разработаны с особой тщательностью и с использованием эффективных мер проверки и контроля. При возникновении вопросов обращайтесь непосредственно в компанию HIMA. Компания HIMA будет благодарна за отзывы и пожелания, например, в отношении информации, которая должна быть дополнительно включена в руководство.

Право на внесение технических изменений сохраняется. Компания HIMA оставляет за собой также право обновлять письменные материалы без предварительного уведомления.

Более подробная информация представлена в документации на диске DVD HIMA и на наших веб-сайтах http://www.hima.de и http://www.hima.com.



## Контакты

Адрес компании HIMA:

HIMA Paul Hildebrandt GmbH

Postfach 1261

D-68777 Brühl

Тел.: +49-6202-709-0

Факс: +49-6202-709-107

Эл. почта: info@hima.com

| Оригинал на немецком языке | Описание |
|---|---|
| HI 800 022 D, Rev. 2.02 (1329) | Перевод  на русский язык с немецкого оригинала |

# Содержание


1 Руководство по безопасности 7
1.1 Структура и использование документации 7
1.2 Целевая аудитория 8
1.3 Оформление текста 9
1.3.1 Указания по безопасности 9
1.3.2 Указания по применению 10
2 Указания по использованию 11
2.1 Применение по назначению 11
2.1.1 Область применения 11
2.1.2 Ненадлежащее использование 11
2.2 Условия окружающей среды 12
2.3 Задачи изготовителей машин и установок, а также эксплуатирующей стороны 12
2.3.1 Подключение партнеров по связи 12
2.3.2 Использование безопасной коммуникации 12
2.4 Меры по защите от электростатического разряда 12
2.5 Дополнительная документация по системе 13
3 Концепция безопасности для применения ПЭС 14
3.1 Безопасность и готовность 14
3.1.1 Расчеты PFD и PFH 14
3.1.2 Самодиагностика и диагностика ошибок 14
3.1.3 PADT 15
3.1.4 Конструкция системы безопасности по принципу рабочего тока 15
3.2 Время, важное для безопасности 16
3.2.1 Время отказоустойчивости (FTT, см. DIN VDE 0801, приложение A1 2.5.3) 16
3.2.2 Безопасное время ПЭС 16
3.2.3 Безопасное время прикладной программы 16
3.2.4 Время реакции 16
3.2.5 Время сторожевого устройства процессорной системы 17
3.2.6 Время сторожевого устройства прикладной программы для F*03. 17
3.3 Повторная проверка 17
3.3.1 Выполнение повторной проверки 18
3.3.2 Частота повторных проверок 18
3.4 Требования безопасности 18
3.4.1 Проектирование аппаратного обеспечения 18
3.4.2 Программирование 19
3.4.3 Коммуникация 19
3.4.4 Работы по техобслуживанию 20
3.5 Сертификация 21
3.5.1 Сертификат TÜV 21
3.5.2 EC Type Approval 21
3.5.3 Действующие стандарты 22
3.5.4 Условия испытаний 22
4 Основные функции 25
4.1 Блоки питания 25

**4.2 Функциональное описание процессорной системы 25**
**4.3 Самодиагностика 26**
4.3.1 Тестирование микропроцессора 26
4.3.2 Тест областей памяти 26
4.3.3 Зафиксированные области памяти 26
4.3.4 Тест ОЗУ 26
4.3.5 Тестирование сторожевого устройства 27
4.3.6 Тестирование шины ввода/вывода внутри системы управления 27
4.3.7 Реакции на ошибки в процессорной системе 27
**4.4 Диагностика ошибок 27**
**5 Входы 28**
**5.1 Общие положения 28**
**5.2 Безопасность датчиков, декодеров и трансмиттеров 28**
**5.3 Безопасные цифровые входы 29**
5.3.1 Общие положения 29
5.3.2 Тестовые программы 29
5.3.3 Реакция при обнаружении ошибки 29
5.3.4 Перенапряжение на цифровых входах 29
5.3.5 Параметрируемые цифровые входы 30
5.3.6 Управление линией 30
**5.4 Безопасные аналоговые входы (F35, F3 AIO 8/4 01 и F60) 31**
5.4.1 Тестовые программы 33
5.4.2 Реакция при обнаружении ошибки 33
**5.5 Безопасные счетчики (F35 и F60) 34**
5.5.1 Общие положения 34
5.5.2 Реакция при обнаружении ошибки 34
**5.6 Контрольный перечень для безопасных входов 34**
**6 Выходы 35**
**6.1 Общие положения 35**
**6.2 Безопасность исполнительных элементов 36**
**6.3 Безопасные цифровые выходы 36**
6.3.1 Тестовые программы для цифровых выходов 36
6.3.2 Реакция при обнаружении ошибки 36
6.3.3 Поведение при коротком замыкании или перегрузке 36
6.3.4 Управление линией 36
**6.4 Безопасные 2-полюсные цифровые выходы 37**
6.4.1 Реакция при обнаружении ошибки 38
6.4.2 Поведение при коротком замыкании или перегрузке 38
**6.5 Релейные выходы 38**
6.5.1 Тестовые программы для релейных выходов 38
6.5.2 Реакция при обнаружении ошибки 38
**6.6 Безопасные аналоговые выходы (F60) 39**
6.6.1 Тестовые программы 39
6.6.2 Реакция при обнаружении ошибки 39
**6.7 Аналоговые выходы с безопасным отключением (F3 AIO 8/4 01) 40**
6.7.1 Тестовые программы 40
6.7.2 Реакция при обнаружении ошибки 40

**6.8 Контрольный перечень для безопасных выходов 40**

**7 Программное обеспечение для систем HIMatrix 41**

**7.1 Аспекты безопасности для операционной системы 41**

**7.2 Принцип работы и функции операционной системы 41**

**7.3 Аспекты безопасности для программирования 41**

7.3.1 Концепция безопасности инструмента программирования 41
7.3.2 Проверка конфигурации и прикладной программы 42
7.3.3 Архивирование проекта 42
7.3.4 Возможность идентификации программы и конфигурации 43

**7.4 Параметры ресурса 44**

7.4.1 Системные параметры для версий выше CPU OS V7 44
7.4.2 Системные параметры для версий ниже CPU OS V7 49

**7.5 Защита от манипуляций 49**

**7.6 Контрольный перечень по созданию прикладной программы 50**

**8 Аспекты безопасности для прикладной программы 51**

**8.1 Рамки безопасного применения 51**

8.1.1 Основы программирования 51
8.1.2 Функции прикладной программы 52
8.1.3 Описание переменных и сигналов 52
8.1.4 Приемка органом, выдающим разрешение 53

**8.2 Порядок действий 53**

8.2.1 Назначение переменных входам/выходам 53
8.2.2 Блокировка и деблокировка системы управления 54
8.2.3 Генерирование кода 55
8.2.4 Загрузка и запуск прикладной программы 56
8.2.5 Перезагрузка для устройств F*03 56
8.2.6 Инициализация 57
8.2.7 Изменение системных параметров в режиме онлайн для версий от CPU OS V7 и выше 57
8.2.8 Документация программы для безопасных случаев применения 58
8.2.9 Многозадачность для устройств F*03 59
8.2.10 Приемка органом, выдающим разрешение 60

**9 Конфигурацию связи 61**

**9.1 Стандартные протоколы 61**

**9.2 Безопасный протокол (safeethernet) 61**

9.2.1 Время ожидания приема (Receive Timeout) 61
9.2.2 Время ответа (Response Time) 62
9.2.3 Максимальное время цикла системы управления HIMatrix 63
9.2.4 Расчет максимального времени реакции 63
9.2.5 Расчет макс. времени реакции с двумя устройствами удаленного ввода/вывода 64
9.2.6 Расчет максимального времени реакции двух HIMatrix и одной системы управления HIMax 64
9.2.7 Понятия 65
9.2.8 Присвоение адресов safe**ethernet** 65

**10 Использование в приемно-контрольных приборах пожарной сигнализации 66**

11 Использование в качестве предохранительного, контрольного и регулирующего приспособления с сигнализатором газоопасности 68

Приложение 71

Повышение уровня совокупной безопасности датчиков и исполнительных элементов 71

Глоссарий 72

Перечень изображений 73

Перечень таблиц 74

Индекс 75

# 1 Руководство по безопасности

Данное руководство содержит информацию по использованию безопасных устройств автоматизации HIMatrix по назначению.

Чтобы обеспечить безопасность установки, ввода в эксплуатацию, использования и технического обслуживания автоматизированных систем HIMatrix, необходимо соблюдать следующие условия:

- Знание требований инструкций.
- Безупречная техническая реализация приведенных в данном руководстве указаний по безопасности, выполненная квалифицированным персоналом.

Неисправности или нарушения функций безопасности могут нанести тяжелый ущерб здоровью людей либо значительный материальный или экологический ущерб, за причинение которого компания HIMA не несет ответственности в следующих случаях:

- В случае доступа к устройству неквалифицированных сотрудников.
- При отключении функций безопасности или при их обходе (функция «байпас»).
- При несоблюдении указаний данного руководства.

Компания HIMA разрабатывает, производит и проверяет автоматизированные системы HIMatrix с учетом соответствующих стандартов безопасности. Использование устройства допускается только при выполнении всех следующих условий:

- Устройства используются только согласно настоящему руководству.
- Условия окружающей среды соответствуют указанным в руководстве.
- Устройства используются в сочетании со сторонним оборудованием, только если оно было допущено.

Из соображений наглядности данное руководство не содержит полной информации по всем вариантам исполнения устройств автоматизации HIMatrix. Более подробная информация изложена в соответствующих руководствах.

## 1.1 Структура и использование документации

Данное руководство по безопасности разделено на следующие главы:

- Применение по назначению
- Концепция безопасности
- Основные функции
- Входы
- Выходы
- Software, программное обеспечение
- Аспекты безопасности для прикладной программы
- Конфигурацию связи
- Использование в приемно-контрольных приборах пожарной сигнализации
- Приложение:
  - Повышение уровня совокупной безопасности датчиков и исполнительных элементов
  - Глоссарий
  - Списки/указатель

i В настоящем документе компактные системы управления и устройства удаленного ввода/вывода обозначаются как *устройство*, а сменные платы модульной системы управления – как *модуль*.
Термин *модуль* (*Module*) используется в этом значении также и в SILworX.

Перечисленные ниже устройства HIMatrix имеют дополнительные функции:

- F60 CPU 03
- F35 03
- F31 03
- F30 03
- F10 PCI 03

Для данных устройств в настоящем документе используется общее обозначение **F*03**. Данные устройства отличаются от стандартных устройств наличием следующих функций:

- Повышенная производительность
- Возможность регистрации последовательности событий
- Возможность многозадачности
- Возможность перезагрузки
- Два IP-адреса

Руководство различает следующие варианты системы HIMatrix:

| Инструмент программирования | Аппаратное обеспечение | Операционная система процессора | Система управления коммуникациями |
|---|---|---|---|
| SILworX | F*03 | Для версии CPU OS V8 и выше | Для версии COM OS V13 и выше |
| SILworX | Стандартное | Для версии CPU OS V7 и выше | Для версии COM OS V12 и выше |
| ELOP II Factory | Стандартное | Для версий ниже CPU OS V7 | Для версий ниже COM OS V12 |

Таблица 1: Варианты системы HIMatrix

В руководстве используются следующие способы различения между вариантами:

- В отдельных подразделах
- Таблицы, учитывающие различия версий, например для версии CPU OS V7 и выше; для версий ниже CPU OS V7

i **Проекты, созданные с помощью ELOP II Factory, не могут обрабатываться в SILworX, и наоборот!**

## 1.2 Целевая аудитория

Данный документ предназначен для планировщиков, проектировщиков и программистов автоматических установок, а также для лиц, допущенных к вводу в эксплуатацию, эксплуатации и техническому обслуживанию приборов и систем. Требуется наличие специальных знаний в области автоматизированных систем обеспечения безопасности.

## 1.3 Оформление текста

В целях удобочитаемости и наглядности в данном документе используются следующие способы выделения и написания текста:

| | |
|---|---|
| **Полужирный шрифт** | Выделение важных частей текста.<br>Обозначения тех кнопок, опций меню и вкладок в интерфейсе инструмента программирования, которые можно выбрать мышью |
| *Курсив* | Параметры и системные переменные |
| `Шрифт Courier` | Текст, вводимый пользователем |
| RUN | Обозначения режимов работы заглавными буквами |
| Гл. 1.2.3 | Сноски оформлены как гиперссылки, хотя могут и не иметь особой маркировки. При наведении на них указателя мыши его форма меняется. При щелчке по ссылке происходит переход к соответствующему месту в документе. |

Указания по безопасности и применению выделены особым образом.

### 1.3.1 Указания по безопасности

Указания по безопасности представлены в документе следующим образом.
В целях максимального уменьшения риска требуется их неукоснительное соблюдение.
Они имеют следующую структуру

- Сигнальное слово: предупреждение/осторожно/указание
- Вид и источник риска
- Последствия несоблюдения указаний
- Избежание риска

**⚠ СИГНАЛЬНОЕ СЛОВО**

**Вид и источник риска!**

**Последствия несоблюдения указаний**

**Избежание риска**

---

Значение сигнальных слов

- Предупреждение: несоблюдение указаний по безопасности может привести к тяжким телесным повреждениям вплоть до летального исхода
- Осторожно: несоблюдение указаний по безопасности может привести к легким телесным повреждениям
- Указание: несоблюдение указаний по безопасности может привести к материальному ущербу

**ПРИМЕЧАНИЯ**

**Вид и источник ущерба!**

**Избежание ущерба**

---

### 1.3.2 Указания по применению

Дополнительная информация представлена следующим образом:

i В этом месте приводится дополнительная информация.

Полезные советы и рекомендации представлены в следующей форме:

**РЕКОМЕНДАЦИЯ** В этом месте расположен текст рекомендации.

# 2 Указания по использованию

Следует обязательно прочесть изложенную в настоящем руководстве информацию по безопасности и сопутствующие указания и инструкции. Использовать продукт только при соблюдении всех правил, в том числе правил техники безопасности.

## 2.1 Применение по назначению

В данной главе описываются условия использования систем HIMatrix.

### 2.1.1 Область применения

Безопасные системы управления HIMatrix можно применять до уровня совокупной безопасности 3 согласно IEC 61508.

Системы HIMatrix имеют соответствующие сертификаты для систем управления процессом, систем защиты, систем управления горелками и систем контрольных механизмов.

#### 2.1.1.1 Применение в соответствии с принципом тока покоя

Устройства автоматизации созданы для применения по принципу тока покоя.

Система, работающая по принципу тока покоя, в случае аварийного отключения переходит в обесточенное состояние или в состояние не под напряжением (de-energize-to-trip).

#### 2.1.1.2 Применение в соответствии с принципом рабочего тока

Системы управления HIMatrix могут использоваться приложениями, функционирующими по принципу рабочего тока.

Система, работающая по принципу рабочего тока, может запускать исполнительное устройство, чтобы выполнять функции обеспечения безопасности (energize-to-trip).

В концепции системы управления необходимо соблюдать требования стандартов использования, например, может потребоваться диагностика линий вводов и выводов или ответное сообщение от сработавшей системы обеспечения безопасности.

#### 2.1.1.3 Использование в приемно-контрольных приборах пожарной сигнализации

Оснащенные устройством распознавания обрыва и замыкания линии системы HIMatrix прошли проверку для использования в установках пожарной сигнализации и имеют сертификаты согласно DIN EN 54-2 и NFPA 72. В этих системах требуется, чтобы по требованию для устранения опасности принималось активное состояние.

Следует соблюдать условия использования!

### 2.1.2 Ненадлежащее использование

Передача релевантных для безопасности данных через открытые сети (например, Интернет) допускается только с принятием дополнительных мер для повышения уровня безопасности (например, туннель VPN, сетевое устройство защиты и т. д.).

## 2.2 Условия окружающей среды

| Условия | Диапазон значений [1] |
|---|---|
| Класс защиты | Класс защиты III в соответствии с IEC/EN 61131-2 |
| Температура окружающей среды | 0...+60 °C |
| Температура хранения | -40...+85 °C |
| Степень загрязнения | Степень загрязнения II в соответствии с IEC/EN 61131-2 |
| Высота установки | < 2000 м |
| Корпус | Стандарт: IP20 |
| Питающее напряжение | 24 В пост. тока |
| [1] Значения технических характеристик имеют критическое значение для устройств, эксплуатируемых в особых условиях окружающей среды. | |

Таблица 2: Условия окружающей среды

При эксплуатации системы HIMatrix необходимо учитывать требования к окружающей среде, приведенные в данном руководстве.

## 2.3 Задачи изготовителей машин и установок, а также эксплуатирующей стороны

Изготовители машин и установок, а также эксплуатирующая сторона несут ответственность за то, чтобы обеспечивалось безопасное использование систем HIMatrix в автоматических установках и комплексах.

Правильное программирование систем HIMatrix должно быть соответствующим образом утверждено изготовителями машин и установок.

### 2.3.1 Подключение партнеров по связи

К коммуникационным интерфейсам можно подключать только те устройства, которые обеспечивают безопасное электрическое разделение.

### 2.3.2 Использование безопасной коммуникации

При использовании безопасной коммуникации между различными устройствами необходимо следить за тем, чтобы общее время реакции системы не превышало время отказоустойчивости. Следует использовать основы расчета, приведенные в настоящей главе.

## 2.4 Меры по защите от электростатического разряда

Изменение и расширение системы или замена модуля может выполняться только персоналом, ознакомленным с защитными мерами от воздействия электростатического разряда.

**ПРИМЕЧАНИЯ**

**Электростатические разряды могут повредить встроенные в системы HIMatrix электронные детали!**

- **Работы следует производить на рабочем месте с антистатической защитой и носить ленточный заземлитель.**
- **При неиспользовании следует хранить модули с обеспечением электростатической защиты, например в упаковке.**

## 2.5 Дополнительная документация по системе

Для проектирования систем HIMatrix кроме прочего предоставляется следующая документация:

| Название | Применимо | Содержание | Номер документа | Номер по каталогу Формат |
|---|---|---|---|---|
| HIMatrix System Manual Compact Systems | Все версии | Описания компактных систем с техническими характеристиками | HI 800 394 RU | Файл pdf |
| HIMatrix System Manual Modular System | Все версии | Описание модульной системы F60 с техническими характеристиками | HI 800 391 RU | Файл pdf |
| Отчет об испытаниях к сертификату [1)] | Все версии | Основы испытаний, требования безопасности, результаты | | 96 9000104 |
| Communication Manual (Конфигурация в SILworX) | Для версии CPU OS V7 и выше | Описание протоколов передачи данных, ComUserTask и их проектирование в SILworX | HI 801 062 RU | Файл pdf |
| HIMatrix PROFIBUS DP Master/Slave Manual | Для версий ниже CPU OS V7 | Описание протокола PROFIBUS и его проектирование в ELOP II Factory | HI 801 009 E | Файл pdf |
| HIMatrix Modbus Master/Slave Manual | Для версий ниже CPU OS V7 | Описание протокола Modbus и его проектирование в ELOP II Factory | HI 800 003 E | Файл pdf |
| HIMatrix TCP S/R Manual | Для версий ниже CPU OS V7 | Описание протокола TCP S/R и его проектирование в ELOP II Factory | HI 800 117 E | Файл pdf |
| HIMatrix ComUserTask (CUT) Manual | Для версий ниже CPU OS V7 | Описание ComUserTask и его проектирование в ELOP II Factory | HI 800 329 E | Файл pdf |
| SILworX Online Help | Для версии CPU OS V7 и выше | Управление SILworX | - | Файл chm |
| ELOP II Factory Online Help | Для версий ниже CPU OS V7 | Управление ELOP II Factory, протокол Ethernet IP, протокол INTERBUS | - | Файл chm |
| SILworX First Steps Manual | Для версии CPU OS V7 и выше | Введение в SILworX | HI 801 103 E | Файл pdf |
| ELOP II Factory First Steps Manual | Для версий ниже CPU OS V7 | Введение в ELOP II Factory | HI 800 006 E | 96 9000013 Файл pdf |
| [1)] Поставка только вместе с системой HIMatrix. | | | | |

Таблица 3: Документация по системе HIMatrix

Более подробную информацию по устройствам и модулям см. в соответствующих руководствах.

# 3 Концепция безопасности для применения ПЭС

В данной главе рассматриваются важные общие вопросы по функциональной безопасности систем HIMatrix:

- Безопасность и готовность
- Время, важное для безопасности
- Повторная проверка
- Требования безопасности
- Сертификация

## 3.1 Безопасность и готовность

Системы HIMatrix имеют соответствующие сертификаты для систем управления процессом, систем защиты, систем управления горелками и машинами.

Системы HIMatrix не являются источником непосредственной опасности.

**⚠ ОПАСНОСТЬ**

**Травмы персонала из-за неправильно подключенных или неверно запрограммированных безопасных автоматизированных систем!**

**Проверить подключения перед вводом в эксплуатацию и испытать установку в целом!**

### 3.1.1 Расчеты PFD и PFH

Для систем HIMatrix согласно IEC 61508 были выполнены расчеты PFD и PFH.

IEC 61508-1 устанавливает для 3-го уровня совокупной безопасности параметр PFD $10^{-4}$…$10^{-3}$ и PFH $10^{-8}$…$10^{-7}$ в час.

Для системы управления (ПЭС) принимаются 15% предельного значения от стандарта для PFD и PFH. Отсюда получаются как предельные значения для доли системы управления
PFD = 1,5 * $10^{-4}$ и PFH = 1,5 * $10^{-8}$ в час.

Интервал повторной проверки для систем HIMatrix составляет 10 лет, для устройств удаленного ввода/вывода и модулей с релейными выходами — 3 года (proof test, проверочный тест в режиме офлайн, см. IEC 61508-4, абз. 3.8.5).

### 3.1.2 Самодиагностика и диагностика ошибок

При запуске и во время работы операционная система систем управления выполняет обширную самодиагностику. При этом, прежде всего, проверяются:

- Процессоры
- Зоны памяти (ОЗУ, энергонезависимая память)
- Сторожевое устройство
- Отдельные входные/выходные каналы

Если данные тесты обнаруживают ошибку, операционная система отключает неисправный модуль или устройство удаленного ввода/вывода либо неисправный канал ввода/вывода.

В системе без избыточности это означает, что может произойти отключение подфункций или всей ПЭС.

Все устройства и модули HIMatrix соответственно оснащены собственными светодиодами для индикации обнаруженных ошибок. Это обеспечивает в случае сбоя быструю

диагностику ошибок устройства, с которого поступил сигнал об ошибке, или внешнего подключения.

Кроме того, прикладная программа может анализировать различные системные переменные или системные сигналы, которые отображают состояние устройств и модулей.

Обширная диагностическая запись поведения системы и распознанных ошибок сохраняется в памяти диагностики систем управления. Запись можно считать после системного сбоя через PADT.

Детали анализа диагностических сообщений также см. в руководстве по компактной системе (HIMatrix System Manual Compact Systems HI 800 394 RU) или руководстве по модульным системам (HIMatrix System Manual Modular System HI 800 391 RU).

Если отказов элементов настолько мало, что они не влияют на безопасность, то диагностическая информация не генерируется системой HIMatrix.

### 3.1.3 PADT

С помощью PADT пользователь составляет программу и конфигурирует систему управления. Концепция безопасности PADT поддерживает пользователя при корректной реализации задач управления. PADT выполняет многочисленные меры по проверке полученной информации.

PADT — персональный компьютер, на котором установлен инструмент проектирования.

Для системы HIMatrix доступны два инструмента проектирования, в зависимости от версии операционной системы, используемой системой управления:

- С операционной системой процессора V7 и выше следует использовать SILworX.
- С операционной системой процессора ниже V7 следует использовать ELOP II Factory.

### 3.1.4 Конструкция системы безопасности по принципу рабочего тока

Системы безопасности, работающие по принципу рабочего тока (energize-to-trip), имеют следующую функцию:

1. Безопасным состоянием устройства является обесточенное состояние. Переход в это состояние происходит, например, при внутренней ошибке устройства.
2. По требованию система управления может активировать функции безопасности, включив исполнительное устройство.

#### 3.1.4.1 Диагностирование неисправных компонентов

Процесс автоматической диагностики позволяет системе безопасности распознавать неисправное состояние устройств.

#### 3.1.4.2 Обеспечение безопасности при работе по принципу рабочего тока

Для реализации функции обеспечения безопасности система безопасности включает один исполнительный элемент или более (energize), чтобы система достигла безопасного состояния.

Пользователь должен запланировать следующие действия:

- Контроль короткого замыкания и обрыва в цепи для устройств ввода/вывода. Их необходимо параметрировать.
- Обеспечить контроль функций исполнительных элементов можно с использованием позиционной обратной связи.

## 3.2 Время, важное для безопасности

Это:

- Fault tolerance time, время допустимой погрешности
- Время сторожевого устройства
- Безопасное время
- Время реакции

### 3.2.1 Время отказоустойчивости (FTT, см. DIN VDE 0801, приложение A1 2.5.3)

Время отказоустойчивости является характеристикой процесса и описывает промежуток, за который процесс может нагружаться ошибочными сигналами, не входя в опасное состояние.

### 3.2.2 Безопасное время ПЭС

Безопасное время — это время, в течение которого ПЭС, находящаяся в состоянии RUN, должна среагировать после возникновения внутренней ошибки.

Если смотреть с точки зрения процесса, то безопасное время представляет собой максимальное время, в течение которого система безопасности должна среагировать при изменении входных сигналов на выходах (время реакции).

| Версия операционной системы | Безопасное время в диапазоне |
|---|---|
| Для версии CPU OS V7 и выше | 20...22 500 мс |
| Для версий ниже CPU OS V7 | 20...50 000 мс |

Таблица 4: Диапазон значений безопасного времени

### 3.2.3 Безопасное время прикладной программы

Безопасное время прикладной программы не задается непосредственно. Безопасное время прикладной программы рассчитывается HIMatrix на основе параметра ресурса *Safety Time* и параметра *Maximum Number of Cycles*. Подробнее см. в главе 8.2.9.

### 3.2.4 Время реакции

Время реакции циклически работающих систем управления HIMatrix представляет собой двойное время цикла этих систем, если задержка происходит не из-за параметрирования или логической схемы прикладной программы.

Время цикла системы управления состоит из следующих существенных этапов:

- Считывание входов
- Обработка прикладной программы или прикладных программ
- Запись выходов
- Обмен данными процесса
- Выполнение тестовых программ

Для устройств или модулей F*03 цикл прикладной программы может охватывать несколько циклов процессорной системы. Для таких прикладных программ время реакции увеличивается соответствующим образом, см. ниже.

Дополнительно при рассмотрении худшего случая всей системы необходимо принимать во внимание время переключения входов и выходов.

Время реакции $t_{Response}$ складывается следующим образом:

$t_{Response} = t_{Input} + t_{In\text{-}communication} + 2 * t_{WDT} + t_{\text{-}Out\text{-}communication} + t_{Output}$

| | |
|---|---|
| $t_{Input}$ | Время переключения/преобразования ввода |
| $t_{In\text{-}Communication}$ | Для устройства удаленного ввода/вывода: время передачи между вводом в устройстве удаленного ввода/вывода и системой управления |
| $t_{WDT}$ | Зависит от типа устройства:<br>▪ Для стандартных устройств/модулей оно является временем сторожевого устройства ресурса<br>▪ Для устройств/модулей F*03 оно является временем сторожевого устройства прикладной программы и может во много раз превышать время сторожевого устройства процессорной системы |
| $t_{Out\text{-}Communication}$ | Для устройства удаленного ввода/вывода: время передачи между системой управления и выводом в устройстве удаленного ввода/вывода |
| $t_{Output}$ | Время переключения/преобразования вывода |

### 3.2.5 Время сторожевого устройства процессорной системы

Время сторожевого устройства задается в меню настройки свойств ПЭС. Это максимально допустимая продолжительность цикла RUN (время цикла). Если время цикла превышает заданное время сторожевого устройства, то система отключается. Затем система запускается заново, если настроен автозапуск. Если автозапуск не настроен, система переходит в состояние STOP/VALID CONFIGURATION.

Время сторожевого устройства процессорной системы следует устанавливать ≤ ½ ∗ безопасное время PES.

| Версия операционной системы | Аппаратное обеспечение | Диапазон значений времени сторожевого устройства | Значение по умолчанию систем управления | Значение по умолчанию устройств удаленного ввода/вывода |
|---|---|---|---|---|
| Для версии CPU OS V8 и выше | F*03 | 4...5 000 мс | 200 мс | 100 мс |
| Для версии CPU OS V7 и выше | Стандартное | 8...5 000 мс | 200 мс | 100 мс |
| Для версий ниже CPU OS V7 | Стандартное | 2...5 000 мс | 50 мс | 10 мс |

Таблица 5: Диапазон значений времени сторожевого устройства

### 3.2.6 Время сторожевого устройства прикладной программы для F*03.

Каждая прикладная программа имеет собственное время сторожевого устройства.

Время сторожевого устройства прикладной программы не задается непосредственно. Устройства/модули HIMatrix F*03 вычисляют время сторожевого устройства прикладной программы, используя параметры *Max. Watchdog Time* ресурса и *Maximum Number of Cycles*.

Обратите внимание на то, что вычисленное время сторожевого устройства максимально равно времени реакции, которое требуется для части процесса, обрабатываемой с помощью прикладной программы.

## 3.3 Повторная проверка

Повторная проверка направлена на обнаружение скрытых ошибок в безопасной системе, то есть при необходимости система может вернуться в состояние, в котором она выполняет свою запланированную функцию.

Системы безопасности HIMA должны подвергаться проверке каждые 10 лет. Интервал этот нередко можно и продлить, если анализировать реализованные цепи безопасности на основе расчетов.

Для устройств удаленного ввода/вывода и модулей с релейными выходами необходимо осуществлять повторную проверку реле через интервалы времени, определенные для установки.

### 3.3.1 Выполнение повторной проверки

Выполнение повторной проверки зависит от того, какую конфигурацию имеет установка (EUC = equipment under control), какой она имеет потенциал опасности, какие из стандартов используются для эксплуатации установки и какие стандарты были применены полномочным отделом контроля как основание для разрешения.

Согласно стандартам IEC 61508 1-7, IEC 61511 1-3, IEC 62061 и VDI/VDE 2180, лист 1-4, эксплуатирующая сторона должна обеспечить повторные проверки безопасных систем.

### 3.3.2 Частота повторных проверок

Система управления HIMatrix может подвергаться повторной проверке в рамках проверки всей цепи безопасности.

На практике для полевых устройств ввода и вывода требуется более короткий интервал повторения проверки (напр., каждые 6 или 12 месяцев), чем для системы управления HIMatrix. Если пользователь проверяет всю цепь безопасности из-за полевого устройства, то система управления HIMatrix автоматически включается в эту проверку. В этом случае для системы управления HIMatrix не требуется никаких дополнительных повторных проверок.

Если повторная проверка полевых устройств не охватывает систему управления HIMatrix, то для обеспечения уровня совокупной безопасности SIL 3 ее следует проверять не реже одного раза в 10 лет. Этого можно добиться, перезапустив систему управления HIMatrix.

Если для специальных устройств установлены дополнительные требования, касающиеся проведения повторной проверки, то необходимо следовать указаниям руководства соответствующего устройства.

## 3.4 Требования безопасности

При использовании безопасной ПЭС системы HIMatrix действуют следующие требования безопасности:

### 3.4.1 Проектирование аппаратного обеспечения

Лица, занимающиеся проектированием аппаратного обеспечения HIMatrix, должны соблюдать следующие требования безопасности.

#### 3.4.1.1 Требования, не зависящие от изделия

- В целях безопасной эксплуатации разрешается использовать только допущенное аппаратное и программное обеспечение. Допустимое аппаратное и программное обеспечение перечислено в списке *Version List of Devices and Firmware of HIMatrix Systems of HIMA Paul Hildebrandt GmbH, Certificate-No. 968/EZ 128.19/09*. Соответственно текущие номера версий содержатся в списке версий, составляемом совместно с отделом контроля.
- Необходимо соблюдать указанные условия использования (см. главу 2.2) в отношении ЭМС, а также механических, химических и климатических воздействий.
- Небезопасное, но не имеющее обратного воздействия на источник аппаратное и программное обеспечение может использоваться для обработки нерелевантных для безопасности сигналов, однако оно не должно использоваться для обработки задач, связанных с безопасностью.
- При подключении к системе любых внешних цепей безопасности следует соблюдать принцип тока покоя.

#### 3.4.1.2 Требования, зависящие от изделия

- К системе должны подключаться только те устройства, которые имеют безопасное отделение от сети.
- Безопасное электрическое разделение электроснабжения должно осуществляться при подаче 24 В для системы. Разрешается использовать только блоки питания в исполнениях для ЗСНН или БСНН.

### 3.4.2 Программирование

Лица, составляющие прикладные программы, должны соблюдать следующие требования безопасности.

#### 3.4.2.1 Требования, не зависящие от изделия

- В безопасных приложениях необходимо следить за правильным параметрированием релевантных для безопасности системных величин.
- Особое внимание следует уделить определению конфигурации системы, максимального времени цикла и безопасного времени.

#### 3.4.2.2 Требования, зависящие от изделия: CPU OS V7 и выше

Требования к использованию инструмента программирования

- Для программирования следует использовать инструмент **SILworX**.
- После создания приложения путем двукратной компиляции и сравнения CRC конфигурации следует удостовериться, что компиляция произведена корректно.
- **Необходимо валидировать и верифицировать правильность преобразования спецификации приложения. Следует провести полную проверку логической схемы путем отладки.**
- Реакция системы на ошибки в безопасных модулях ввода, модулях вывода и устройствах удаленного ввода/вывода должна быть задана прикладной программой в соответствии с условиями сохранения функции безопасности для конкретной установки.

#### 3.4.2.3 Требования, зависящие от изделия: ниже CPU OS V7

Требования к использованию инструмента программирования

- Для программирования следует использовать инструмент **ELOP II Factory**.
- После создания приложения путем ручной двукратной компиляции и сравнения CRC конфигурации следует удостовериться, что компиляция произведена корректно.
- **Необходимо валидировать и верифицировать правильность преобразования спецификации приложения. Следует провести полную проверку логической схемы путем отладки.**
- Реакция системы на ошибки в безопасных модулях ввода, модулях вывода и устройствах удаленного ввода/вывода должна быть задана прикладной программой в соответствии с условиями сохранения функции безопасности для конкретной установки.

### 3.4.3 Коммуникация

- При использовании безопасной связи между различными устройствами необходимо следить за тем, чтобы общее время реакции системы не превышало время отказоустойчивости. Расчеты должны проводиться на основе принципов, приведенных в главе .
- Передача данных, релевантных для безопасности, через открытые сети (например, Интернет) не разрешена без дополнительных мер безопасности, таких как использование VPN-канала.
- Если передача данных осуществляется по внутренним сетям организации/предприятия, то при помощи административных или технических мер следует обеспечить достаточный уровень защиты от манипулирования (например,

отделение части сети, релевантной для безопасности, от других сетей посредством межсетевого экрана).

- Не разрешается использовать стандартные протоколы для передачи данных, связанных с безопасностью.
- Ко коммуникационным интерфейсам можно подключать только те устройства, которые обеспечивают безопасное электрическое разделение.

### 3.4.4 Работы по техобслуживанию

- Работы по техобслуживанию входят в сферу ответственности эксплуатирующей стороны. Эксплуатирующая сторона обязана принимать надлежащие меры, чтобы обеспечить безопасность эксплуатации в ходе технического обслуживания.
- В случае необходимости эксплуатирующее предприятие по согласованию с приемочным органом, ответственным за применение, должно определить административные меры для защиты системы от доступа.

## 3.5 Сертификация

Функциональная безопасность безопасных устройств автоматизации HIMA (программируемые электронные системы, ПЭС) системы HIMatrix проверена в соответствии с перечисленными стандартами, подтверждена сертификатом TÜV, а также соответствует CE:

Дополнительно к приведенным здесь стандартам могут сертифицироваться отдельные устройства для следующих областей применения. Более подробную информацию вы найдете в руководствах к устройствам.

### 3.5.1 Сертификат TÜV

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie
Am Grauen Stein
51105 Köln

**Сертификат и отчет об испытаниях 968/EZ 128.25/12**
**Безопасные устройства автоматизации**
**HIMatrix F10, F20, F30, F31, F35, F60, RIO-NC**

### 3.5.2 EC Type Approval

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie
Am Grauen Stein
51105 Köln

**EC Type Approval Certificate No. 01/205/0644/09**
**ПЛК безопасности (PES), серия систем**
**HIMatrix F10, F20, F30, F31, F35, F60, RIO-NC**

### 3.5.3 Действующие стандарты

| | |
|---|---|
| Международные стандарты: | |
| EN / IEC 61508, Parts 1-7: 2000 | SIL 3 |
| EN / IEC 61511: 2004 | SIL 3 |
| EN ISO 13849-1: 2008 + AC: 2009 | Performance Level e |
| EN 62061: 2005 | SIL CL 3 |
| EN 50156-1: 2004 | SIL 3 |
| EN 12067-2: 2004 | |
| EN 298: 2003 | |
| EN 230: 2005 | |
| NFPA 85: 2011 | |
| NFPA 86: 2011 | |
| EN 61131-2: 2007 | |
| EN 61326-3-1: 2008 | |
| EN 61000-6-2: 2005 | (директива по ЭМС, согласно декларации изготовителя) |
| EN 61000-6-4: 2007 | |
| EN 54-2: 1997 + AC:1999 + A1:2006 + A1:2007 | |
| EN 50130-4: 1989 + A1: 1989 +A2: 2003 + Corr. 2003 | Стандарт на метод испытания для EN 54-2 |
| NFPA 72: 2010 | |
| EC Directives | см. соответствующие декларации о соответствии |

Глава 3.5.4 содержит подробный список всех проведенных испытаний на воздействие внешних условий и проверок электромагнитной совместимости.

Все устройства имеют знак технического контроля CE.

### 3.5.4 Условия испытаний

Системы HIMatrix были проверены на соответствие следующим нормам ЭМС, а также климатическим и экологическим требованиям:

| Стандарт | Содержание |
|---|---|
| IEC/EN 61131-2: 2007 | Programmable controllers, Part 2<br>Equipment requirements and tests |
| IEC/EN 61000-6-2: 2005 | ЭМС<br>Generic standards, Parts 6-2<br>Immunity for industrial environments |
| IEC/EN 61000-6-4: 2007 + A1: 2011 | Electromagnetic Compatibility (EMC)<br>Generic emission standard, industrial environments |

Таблица 6: Нормы для ЭМС, климатических и экологических требований

При использовании безопасных систем управления HIMatrix необходимо соблюдать следующие общие условия:

| Условия | Содержание условия |
|---|---|
| Класс защиты | Класс защиты III в соответствии с IEC/EN 61131-2 |
| Степень загрязнения | Степень загрязнения II в соответствии с IEC/EN 61131-2 |
| Высота установки | < 2000 м |
| Корпус | Стандарт: IP20<br>Если того требуют соответствующие стандарты применения (например, EN 60204, EN 13849), систему HIMatrix необходимо встраивать в корпус с необходимой степенью защиты (например, IP54). |

Таблица 7: Общие условия

### 3.5.4.1 Климатические условия

Наиболее важные испытания и предельные значения для климатических условий перечислены в таблице ниже:

| IEC/EN 61131-2 | Климатические испытания |
|---|---|
| | Рабочая температура: 0...+60 °C<br>(Предельные значения при испытании: от -10...+70 °C) |
| | Температура хранения: от -40...+85 °C |
| | Сухое тепло и холод; испытания на прочность:<br>+70 C/-25 °C, 96 ч,<br>Электропитание не подключено |
| | Смена температуры; испытание на прочность и нечувствительность:<br>-40 C/+70 °C и 0 C/+55 °C,<br>Электропитание не подключено |
| | Циклы с влажным теплом; испытания на прочность:<br>+25 C/+55 °C, 95 % относительная влажность,<br>Электропитание не подключено |

Таблица 8: Климатические условия

Отличные от этого условия использования указаны в руководствах устройств или модулей.

### 3.5.4.2 Механические условия

Наиболее важные испытания и предельные значения для механических условий перечислены в таблице ниже:

| IEC/EN 61131-2 | Механические испытания |
|---|---|
| | Испытание на нечувствительность к вибрациям:<br>5…9 Гц/3,5 мм<br>9...150 Гц, 1 г, испытываемое оборудование в эксплуатации,<br>10 циклов на ось |
| | Нечувствительность к ударам:<br>15 г, 11 мс, испытываемое оборудование в эксплуатации, 3 удара на ось (18 ударов) |

Таблица 9: Механические испытания

### 3.5.4.3 Условия электромагнитной совместимости

Для безопасных систем требуются повышенные уровни при воздействии возмущений. Системы HIMatrix отвечают данным требованиям согласно IEC 62061 и IEC 61326-3-1. См. столбец *Критерий ФБ* (функциональная безопасность).

| IEC/EN 61131-2 | Испытания на помехоустойчивость | Критерий ФБ |
|---|---|---|
| IEC/EN 61000-4-2 | Испытание на устойчивость к электростатическим разрядам (ESD): контактный разряд 6 кВ, воздушный разряд 8 кВ | 6 кВ, 8 кВ |
| IEC/EN 61000-4-3 | Испытание RFI (10 В/м): 80 МГц…2 ГГц, 80 % AM<br>Испытание RFI (3 В/м): 2 МГц…3 ГГц, 80 % AM<br>Испытание RFI (20 В/м): 80 МГц…1 ГГц, 80 % AM | -<br>-<br>20 В/м |
| IEC/EN 61000-4-4 | Испытание на устойчивость к наносекундным импульсным помехам:<br>Питающее напряжение: 2 кВ и 4 кВ<br>Сигнальные линии: 2 кВ | <br>4 кВ<br>2 кВ |
| IEC/EN 61000-4-12 | Испытание затухающими колебаниями:<br>2,5 кВ L-, L+/PE<br>1 кВ L+/L- | <br>-<br>- |
| IEC/EN 61000-4-6 | Высокая частота, асимметрично:<br>10 В, 150 кГц…80 МГц, AM<br>20 В, ISM-частоты, 80 % AM | <br>10 В<br>- |
| IEC/EN 61000-4-3 | Импульсы 900 МГц | - |
| IEC/EN 61000-4-5 | Импульсное напряжение:<br>Питающее напряжение: 2 кВ CM, 1 кВ DM<br>Сигнальные линии: 2 кВ CM, 1 кВ DM при AC ввод/вывод | <br>2 кВ/1 кВ<br>2 кВ |

Таблица 10: Испытания на помехоустойчивость

| IEC/EN 61000-6-4 | Испытания на помехоэмиссию |
|---|---|
| EN 55011<br>Класс A | Эмиссия помех:<br>излучаемая, в сетевых кабелях |

Таблица 11: Испытания на помехоэмиссию

### 3.5.4.4 Электропитание

Наиболее важные испытания и предельные значения для электропитания системы HIMatrix перечислены в таблице ниже:

| IEC/EN 61131-2 | Дополнительная проверка характеристик подачи постоянного напряжения |
|---|---|
| | Электропитание должно отвечать следующим стандартам:<br>IEC/EN 61131-2:<br>БСНН (защитное пониженное напряжение) или<br>ЗСНН (пониженное напряжение с безопасным размыканием) |
| | Защита систем HIMatrix предохранителем должна осуществляться согласно данным, содержащимся в данном руководстве |
| | Проверка диапазона напряжений:<br>24 В пост. тока, -20…+25 % (19,2…30,0 В) |
| | Испытание на нечувствительность в случае краткого прерывания подачи электропитания от внешнего источника:<br>пост. ток, PS 2: 10 мс |
| | Изменение полярности питающего напряжения:<br>Указание в соответствующей главе руководства по системе или в таблице параметров для линии электропитания. |

Таблица 12: Дополнительная проверка характеристик подачи постоянного напряжения

# 4 Основные функции

Системы управления и устройства удаленного ввода/вывода типа F1.., F2.., F3.. представляют собой компактные системы, модификация которых невозможна.

Системы управления типа F60 представляют собой модульные системы. Для них в пределах системы управления вне блоков питания и процессорного модуля возможно использование до шести модулей ввода/вывода.

## 4.1 Блоки питания

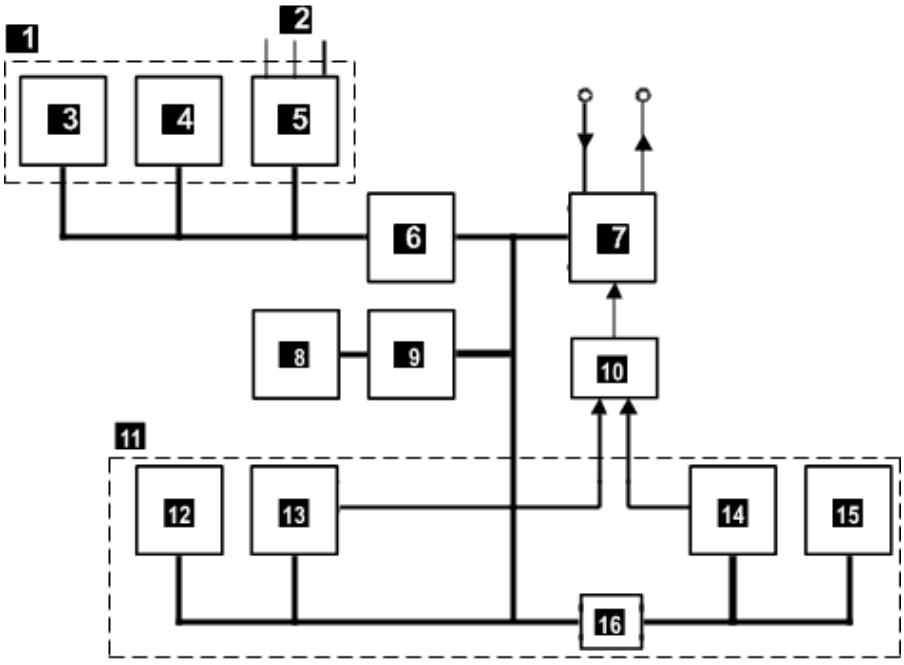
Модуль блока питания имеется только в F60. В компактных системах эта функция интегрирована в устройство и не может рассматриваться как модульная.

Модуль блока питания PS 01 (для F60) или интегрированная функция преобразуют питающее напряжение 24 В пост. тока в 3,3 В пост. тока и 5 В пост. тока (использование для внутренней шины ввода/вывода).

## 4.2 Функциональное описание процессорной системы

В модульной системе F60 процессорная система размещена на собственном модуле, а в компактных системах — в компактном устройстве управления.

Процессорная система состоит из следующих блоков функций:




1 Система коммуникации
2 Коммуникационные интерфейсы: 2 интерфейса полевой шины, переключатель Ethernet
3 ROM системы коммуникации
4 RAM системы коммуникации
5 Процессор системы коммуникации
6 Dual-Ported RAM
7 Соединение с модулями ввода/вывода
8 ROM
9 Энергонезависимая память (NVRAM)
10 Сторожевое устройство
11 Процессорная система по обеспечению безопасности
12 RAM 1 процессорной системы
13 Процессор 1 процессорной системы
14 Процессор 2 процессорной системы
15 RAM 2 процессорной системы
16 Сравнивающее устройство

Рис. 1: Изображение блоков функций на примере ЦПУ 01 системы управления F60

Характеристики процессорного модуля CPU 01 системы F60

- Два микропроцессора с тактовой синхронизацией (процессор 1 и процессор 2).
- Каждый микропроцессор имеет собственное ОЗУ
- Тестируемое сравнивающее устройство аппаратного обеспечения для всех внешних доступов обоих микропроцессоров
- В случае ошибки сторожевое устройство переводится в безопасное состояние
- Флеш-память для операционной системы и прикладной программы, пригодная для мин. 100 000 циклов обращения к памяти.
- Память данных в энергозависимой памяти
- Мультиплексор для подключения шины ввода/вывода, двухпортовое ОЗУ (DPR)
- Буферная батарея или Goldcap для даты/времени.
- Коммуникационный процессор для соединения по полевой шине и Ethernet
- Интерфейсы для обмена данными между устройствами, системами управления и PADT на базе Ethernet.
- Опциональный интерфейс(-ы) для обмена данными по полевой шине
- Сигнализация состояний системы с помощью светодиодов
- Логика шины ввода/вывода для соединения с модулями ввода вывода
- Надежное сторожевое устройство (WD)
- Контроль блока питания, тестируемый (напряжения системы 3,3 В пост. тока/5 В пост. тока).

## 4.3 Самодиагностика

Устройства самодиагностики распознают отдельные ошибки, которые могут привести к опасному рабочему состоянию, и в течение времени безопасности системы управления запускают определенные реакции на ошибки, которые, в свою очередь, переводят содержащие ошибку компоненты в безопасное состояние.

Далее кратко рассмотрены наиболее важные программы самодиагностики безопасных процессорных модулей систем управления:

### 4.3.1 Тестирование микропроцессора

Проверяет следующее:

- Все используемые команды и типы адресации,
- Возможность записи флагов и обусловленных ими команд,
- Возможность записи и взаимодействие регистров.

### 4.3.2 Тест областей памяти

Операционная система, прикладная программа, константы и параметры, а также переменные данные хранятся в областях памяти обоих процессоров и проверяются сравнивающим устройством аппаратного обеспечения.

### 4.3.3 Зафиксированные области памяти

Операционная система, прикладная программа и область параметров хранятся каждая в отдельной памяти. Они защищены защитой от записи и тестом CRC.

### 4.3.4 Тест ОЗУ

Тест записи и чтения проверяет изменяемые области RAM, в частности, на константность и взаимное влияние.

### 4.3.5 Тестирование сторожевого устройства

Сигнал сторожевого устройства отключается, если он не подается обоими ЦПУ в установленный интервал времени; а также если не удалось выполнить тестирование сравнивающего устройства аппаратного обеспечения. При помощи других тестов проверяется возможность отключения сигнала сторожевого устройства.

### 4.3.6 Тестирование шины ввода/вывода внутри системы управления

Проверяется соединение между ЦПУ и соответствующими входами и выходами (модули ввода/вывода).

### 4.3.7 Реакции на ошибки в процессорной системе

Сравнивающее устройство аппаратного обеспечения внутри центральной зоны непрерывно сравнивает, идентичны ли команды и данные системы микропроцессора 1 данным системы микропроцессора 2. Если это не так или если тестовые программы находят ошибку, сигнал сторожевого устройства автоматически отключается. Это означает, что система управления больше не обрабатывает входные сигналы и выходы переходят в обесточенное выключенное состояние.

При первой такой ошибке система управления перезапускается (Reboot). Если после перезагрузки в течение одной минуты обнаружится еще одна внутренняя ошибка, то система управления перейдет в состояние STOP/INVALID CONFIGURATION и остановится в этом состоянии.

## 4.4 Диагностика ошибок

Все модули системы F60 имеют соответственно собственные светодиоды для индикации ошибок при неисправности модуля и внешней проводки. Это обеспечивает в случае сбоя быструю диагностику ошибок модуля, с которого поступил сигнал об ошибке.

В компактных системах F1.., F2.., F3.. эта индикация ошибок объединена в группу сообщений об ошибках.

Дополнительно в прикладной программе можно проанализировать различные системные сигналы входов и выходов или системы управления.

Сигнализация неисправностей срабатывает только в том случае, если не прервана связь с процессорной системой, т. е. при помощи процессорной системы еще можно произвести анализ.

Коды ошибок всех входных и выходных сигналов, а также системных сигналов могут анализироваться при помощи логики прикладной программы.

Обширная диагностическая запись поведения системы и распознанных ошибок сохраняется в памяти диагностики процессора и системы коммуникации. Запись можно считать после системного сбоя через PADT.

Более подробную информацию о диагностических сообщениях см. также в руководстве по компактным системам (HIMatrix System Manual Compact Systems HI 800 394 RU) или руководстве по модульной системе (HIMatrix System Manual Modular System HI 800 391 RU).

# 5 Входы

Обзор входов системы HIMatrix:

| Устройство | Тип | Количество входов | Безопасный | без обратного воздействия на источник | С электрическим разделением |
|---|---|---|---|---|---|
| Система управления F20 | Цифровой | 8 | • | • | - |
| Система управления F30 | Цифровой | 20 | • | • | - |
| Система управления F31 | Цифровой | 20 | • | • | - |
| Система управления F35 | Цифровой | 24 | • | • | - |
| | Счетчик 24 бита | 2 | • | • | - |
| | Аналоговый | 8 | • | • | - |
| Remote I/O F1 DI 16 01 | Цифровой | 16 | • | • | - |
| Remote I/O F3 DIO 8/8 01 | Цифровой | 8 | • | • | - |
| Remote I/O F3 DIO 16/8 01 | Цифровой | 16 | • | • | - |
| Remote I/O F3 AIO 8/4 01 | Аналоговый | 8 | • | • | - |
| Remote I/O F3 DIO 20/8 02 | Цифровой | 20 | • | • | - |
| Модульная система управления F60: | | | | | |
| Модуль DIO 24/16 01 | Цифровой | 24 | • | • | • |
| Модуль DI 32 01 (конфигурируются для управления линией) | Цифровой | 32 | • | • | • |
| Модуль DI 24 01 (110 V) | Цифровой | 24 | • | • | • |
| Модуль CIO 2/4 01 | Счетчик 24 бита | 2 | • | • | • |
| Модуль AI 8 01 | Аналоговый | 8 | • | • | • |
| Модуль MI 24 01 | Аналоговый или цифровой | 24 | • | • | • |

Таблица 13: Обзор входов системы HIMatrix

## 5.1 Общие положения

Возможно использование безопасных входов как для безопасных, так и для небезопасных сигналов.

Системы управления выдают информацию о состоянии и ошибке следующим образом:

- Посредством светодиодов диагностики устройств и модулей.
- Посредством системных сигналов или системных переменных, которые может оценивать прикладная программа.
- Посредством записей в памяти диагностики, которые может считывать PADT.

Безопасные модули ввода во время работы автоматически выполняют качественную циклическую самодиагностику. Эти тестовые программы проверены TÜV, они контролируют безопасную работу соответствующего модуля.

При небольшой доле отказов компонентов, когда это не влияет на безопасность, диагностическая информация не генерируется.

## 5.2 Безопасность датчиков, декодеров и трансмиттеров

При безопасном применении как система управления, так и подключенные к ней датчики, декодеры и трансмиттеры должны соответствовать требованиям безопасности и указанному уровню совокупной безопасности. Подробнее см. раздел «Повышение уровня совокупной безопасности датчиков и исполнительных элементов» в приложении.

## 5.3 Безопасные цифровые входы

Описанные свойства действительны как для цифровых входных каналов модулей системы F60, так и для цифровых входных каналов всех компактных систем, если не установлено иное.

### 5.3.1 Общие положения

Один раз за цикл производится считывание и внутреннее сохранение цифровых входов; проводится циклическое тестирование их безопасной работы.

Входные сигналы, время которых меньше времени между двумя дискретизациями (то есть меньше времени цикла), при определенных обстоятельствах не регистрируются.

### 5.3.2 Тестовые программы

Тестовые онлайн-программы проверяют, в состоянии ли входные каналы последовательно подключать оба уровня сигналов (LOW и HIGH) независимо от имеющихся входных сигналов. Данный тест функциональности выполняется при каждом считывании входных сигналов.

### 5.3.3 Реакция при обнаружении ошибки

Если тестовые программы для цифровых входов обнаруживают ошибку, компактная система активирует светодиод *ERROR*, модуль F60 — светодиод *ERR*.

#### 5.3.3.1 Операционная система ЦПУ выше V7

Прикладная программа обрабатывает предустановленное значение глобальных переменных.

Не требуется обработка кода ошибки прикладной программой. Использование кода ошибки дает дополнительные возможности контролировать внешнее подключение и программировать реакции на ошибки в прикладной программе.

Код ошибки называется *->Error Code [Byte]* и доступен во вкладке **...Channels** в детальном представлении модуля или детали устройства, в строке с номером канала.

#### 5.3.3.2 Операционная система ЦПУ ниже V7

Прикладная программа в соответствии с принципом тока покоя обрабатывает низкий уровень для содержащего ошибку канала.

Прикладная программа наряду со значением сигнала канала должна учитывать соответствующий код ошибки.

Использование кода ошибки дает дополнительные возможности контролировать внешнее подключение и программировать реакции на ошибки в прикладной программе.

Код ошибки называется *DI[xx].Error Code*, при этом *xx* обозначает номер канала. Он доступен в окне *Signal Connections* модуля или детали устройства.

### 5.3.4 Перенапряжение на цифровых входах

Короткое время цикла систем HIMatrix позволяет цифровым входам считывать импульсные перенапряжения согласно EN 61000-4-5 как кратковременный высокий уровень.

Следующие меры предотвращают неправильное функционирование в средах, в которых могут возникнуть перенапряжения:

1. Установка экранированных линий ввода
2. Программирование подавления помех в прикладной программе. Сигнал должен поступить минимум в двух циклах, прежде чем его можно будет проанализировать. Реакция на ошибку выполняется с соответствующей задержкой.

i Подавление помех увеличивает время реакции системы HIMatrix!

i От вышеуказанных мер можно отказаться, если путем соответствующего расчета параметров установки можно исключить перенапряжение в системе.

К расчету параметров, в частности, относятся меры защиты, касающиеся перенапряжения, удара молнии, заземления и проводного монтажа установки на основе данных в руководстве системы (HIMatrix System Manual Compact Systems HI 800 394 RU или HIMatrix System Manual Modular Systems HI 800 391 RU) и релевантных стандартов.

### 5.3.5 Параметрируемые цифровые входы

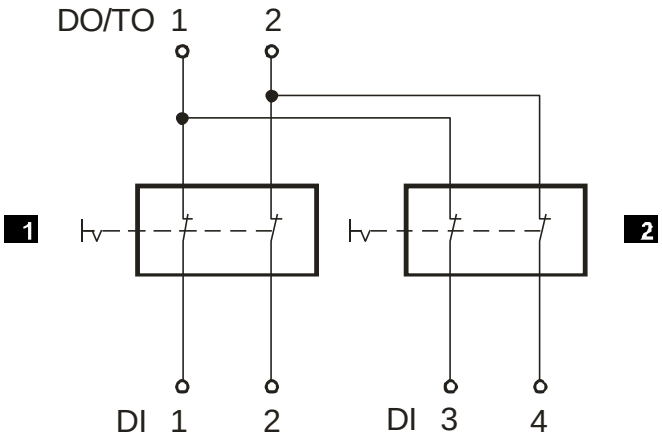
Цифровые входы системы управления F35 и модуля MI 24 01 работают по принципу аналоговых входов, но при помощи параметрирования порогов переключения выдают цифровое значение.

Для параметрируемых цифровых входов действительны указанные для аналоговых входов тестовые программы и функции безопасности, как описано в главе 5.4.

### 5.3.6 Управление линией

Управление линией (Line Control) — это устройство распознавания замыкания и обрыва линии, например, устройств автоматического останова, которое может конфигурироваться для систем HIMatrix с цифровыми входами (не для системы управления F 35 и модуля MI 24 01).

Для этого цифровые выходы системы соединяются с цифровыми входами DI той же системы следующим образом (пример):



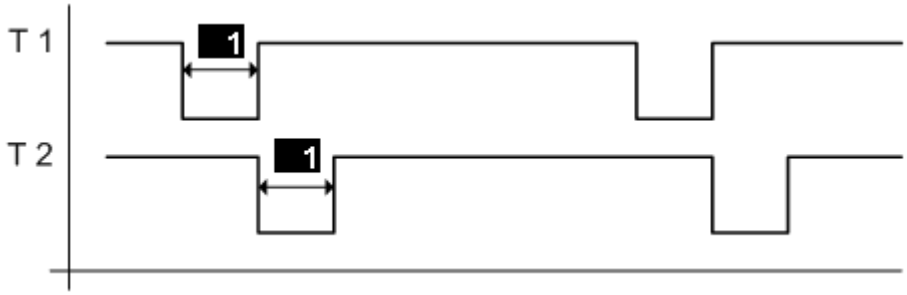

**1** EMERGENCY STOP 1
(Аварийный останов 1)

**2** EMERGENCY STOP 2
(Аварийный останов 2)

Устройства аварийного останова в соответствии со стандартами EN 60947-5-1 и EN 60947-5-5

Рис. 2: Управление линией

Система управления периодически посылает импульсы на цифровые выходы для распознавания замыкания и обрыва линий на линиях, ведущих к цифровым входам. Для этого в SILworX необходимо параметрировать системную переменную *Value [BOOL]* ->, а в ELOP II Factory — системный сигнал *DO[01].Value*. Переменные для тактовых выходов должны должны начинаться на канале 1 и находиться непосредственно друг за другом. (см. системные переменные/сигналы в руководствах).




1 Конфигурируется 5…2000 мкс

Рис. 3: Тактовые сигналы T1, T2

Управление линией может распознавать следующие ошибки:

- перекрестное замыкание между двумя параллельными линиями,
- скрещивание двух линий (например, DO 2 с DI 3),
- замыкание одной из линий на землю (только при заземленном минусе выходного сигнала),
- обрыв линии или открытие контактов.

Возникновение такой ошибки вызывает следующие реакции:

- Мигает светодиод *FAULT* на передней панели системы управления или модуля. При обрыве линии или открытии контактов светодиод не мигает.
- Входы устанавливаются на уровень Low.
- Отображается (поддающийся анализу) код ошибки.

## 5.4 Безопасные аналоговые входы (F35, F3 AIO 8/4 01 и F60)

Аналоговые входные каналы преобразуют измеренные входные токи в значение INTEGER. Значения предоставляются прикладной программе в виде переменных, присвоенных следующим системным переменным/сигналам:

| Версия операционной системы | Значение |
|---|---|
| Для версии CPU OS V7 и выше | *-> Value [INT]* |
| Для версий ниже CPU OS V7 | *AI[xx].Value* (xx = номер канала). |

Таблица 14: Значение безопасных аналоговых входов

Точность с учетом сохранения функции безопасности является гарантированной точностью аналогового входа без учета реакции модуля на ошибку. Данное значение следует учитывать при параметрировании функций безопасности.

Диапазоны значений входов зависят от устройства или модуля:

Система управления F35

| Входные каналы | Метод измерения | Ток, напряжение | Диапазон предоставляемых значений в приложении | | Точность с учетом сохранения функции безопасности |
|---|---|---|---|---|---|
| | | | FS1000[1)] | FS2000[1)] | |
| 8 | униполярн | 0...+10 V | 0...1000 | 0...2000 | 2 % |
| 8 | униполярн | 0...20 mA | 0...500[2)]<br>0...1000[3)] | 0...1000[2)]<br>0...2000[3)] | 2 % |

1) настраивается с помощью выбора типа в PADT

2) с внешним переходником с шунтом 250 Ом, номер детали: 98 2220059

3) с внешним переходником с шунтом 500 Ом, номер детали: 98 2220067

Таблица 15: Аналоговые входы системы управления F35

Remote I/O F3 AIO 8/4 01

| Входные каналы | Метод измерения | Ток, напряжение | Диапазон предоставляемых значений в приложении | Точность с учетом сохранения функции безопасности |
|---|---|---|---|---|
| 8 | униполярн | 0...+10 V | 0...2000 | 2 % |
| 8 | униполярн | 0...20 mA | 0...1000[1)]<br>0...2000[2)] | 2 % |
| [1)] с внешним переходником с шунтом 250 Ом, номер детали: 98 2220059<br>[2)] с внешним переходником с шунтом 500 Ом, номер детали: 98 2220067 | | | | |

Таблица 16: Аналоговые входы устройства удаленного ввода/вывода F3 AIO 8/4 01

Система управления F60

| Входные каналы **AI 8 01** | Метод измерения | Ток, напряжение | Диапазон предоставляемых значений в приложении | | Точность с учетом сохранения функции безопасности |
|---|---|---|---|---|---|
| | | | FS1000[1)] | FS2000[1)] | |
| 8 | униполярн | -10...+10 В | -1000...1000 | -2000...2000 | 1 % |
| 8 | униполярн | 0...20 mA | 0...1000[3)] | 0...2000[3)] | 1 % |
| 8 | униполярн | 0...20 mA | 0...500[2)] | 0...1000[2)] | 4 % |
| 4 | биполярн. | -10...+10 В | -1000...1000 | -2000...2000 | 1 % |
| **MI 24 01** | | | | | |
| 24 | униполярный | 0…20 мА | 0...2000[4)] | | 1 % |
| [1)] настраивается с помощью выбора типа в PADT (F60)<br>[2)] с внешним переходником с шунтом 250 Ом, номер детали: 00 0710251<br>[3)] с внешним измерительным шунтом 500 Ом, номер детали: 00 0603501 (точность 0,05 %, P 1 Вт)<br>[4)] внутренние измерительные шунты | | | | | |

Таблица 17: Аналоговые входы системы управления F60

В прикладной программе можно изменить конфигурацию модуля AI 8 01 системы F60 на восемь униполярных или четыре биполярные функции. Смешивание функций в одном модуле, тем не менее, не допускается.

Аналоговые входы системы управления F35, устройства удаленного ввода/вывода F3 AIO 8/4 01 и модуля AI 8 01 работают с измерением напряжения. При помощи аналоговых входов системы F35 и F3 AIO 8/4 01 можно контролировать цифровые выходы собственной системы (F35) или другой системы управления HIMatrix на обрыв линии. Более подробная информация содержится в руководствах соответствующих систем управления HIMatrix.

При обрыве линии (контроль линий системой не осуществляется) на высокоомных входах обрабатываются произвольные входные сигналы. Полученное на основании такого колеблющегося входного напряжения значение не является надежным; для входов напряжения к каналам подключается нагрузочное сопротивление 10 кОм. При этом следует учитывать внутреннее сопротивление источника.

Для измерения тока параллельно входу подключается шунт, сопротивление 10 кОм тогда не требуется.

Входы модуля MI 24 01 из-за внутреннего измерительного шунта являются токовыми входами и не могут использоваться как входы напряжения.

При неиспользуемых входных каналах измерительный вход следует соединить с опорным потенциалом. Это позволяет избежать негативного влияния на другие каналы в случае обрыва линии (колеблющихся значений напряжения).

| Версия операционной системы | Образ действия |
|---|---|
| Для версии CPU OS V7 и выше | Достаточно не присваивать неиспользуемым входам глобальные переменные. |
| Для версий ниже CPU OS V7 | Для неиспользуемого входа в ELOP II Hardware Management соответствующий сигнал *AI[0x].Used* нужно установить на значение по умолчанию *FALSE* или на *0*. Таким образом, канал в рамках прикладной программы выводится из эксплуатации, т. е. сигнальные сообщения больше недоступны. |

Таблица 18: Конфигурация неиспользуемых входов

### 5.4.1 Тестовые программы

Система управления обрабатывает аналоговые значения параллельно посредством двух мультиплексоров и двух аналоговых/цифровых преобразователей с 12-битным разрешением и сравнивает результаты друг с другом. Дополнительно система управления подключает посредством цифровых/аналоговых преобразователей тестовые значения, преобразует их в цифровые значения и сравнивает с заданными значениями.

### 5.4.2 Реакция при обнаружении ошибки

Если ошибки канала возникают в аналоговых входах, компактная система активирует светодиод *FAULT*, модуль F60 — светодиод *ERR*.

#### 5.4.2.1 Операционная система ЦПУ выше V7

Код ошибки неисправного канала устанавливается на > 0. Если речь об ошибке всего модуля, то код ошибки всего модуля устанавливается на значение > 0. Прикладная программа обрабатывает параметрированное предустановленное значение.

Если значение 0 мА находится в допустимом диапазоне измерений, прикладная программа должна дополнительно к аналоговому значению анализировать код ошибки.

Использование кода ошибки дает дополнительные возможности контролировать внешнее подключение и программировать реакции на ошибки в прикладной программе.

Системная переменная, содержащая код ошибки, называется *->Error Code [Byte]*. Она доступна во вкладке **...Channels** в детальном представлении модуля или детали устройства, в строке с номером канала.

#### 5.4.2.2 Операционная система ЦПУ ниже V7

Код ошибки неисправного канала устанавливается на > 0. Если речь об ошибке всего модуля, то код ошибки всего модуля устанавливается на значение > 0.

Прикладная программа должна дополнительно к аналоговому значению анализировать код ошибки. При значении > 0 следует конфигурировать безопасную реакцию.

Благодаря использованию кода ошибки существуют дополнительные возможности контролировать внешнее подключение и программировать реакции на ошибки в прикладной программе. Системная переменная, содержащая код ошибки, называется *AI[xx].Error Code*, при этом *xx* обозначает номер канала. Системная переменная доступна в окне *Signal Connections...* модуля или детали устройства

## 5.5 Безопасные счетчики (F35 и F60)

Указанное действительно как для блока счетчиков CIO 2/4 01 системы F60, так и для счетчиков системы F35, если не определено иное.

### 5.5.1 Общие положения

Канал счетчика параметрируется для эксплуатации в качестве быстрого счетчика прямого/обратного счета с разрешением 24 бита или в качестве декодера в коде Грея. Для использования в качестве быстрого счетчика прямого/обратного счета приложению необходимы сигналы импульсного входа и входа направления счета. Сброс производится в прикладной программе.
Разрешение декодера 4 бита или 8 бит действительно для блока счетчика CIO 2/4 01 системы F60; в системе F35 декодер имеет разрешение 3 бита или 6 бит. Возможен сброс.
Соединение двух независимых 4-битных входов с одним 8-битным входом (пример для F60) осуществляется исключительно при помощи прикладной программы. Возможность переключения для такой цели не предусмотрена.
Функция декодера контролирует изменение битовой комбинации на выходных каналах. Битовые комбинации на входах передаются прямо в прикладную программу.
Отображение в PADT происходит в виде десятичного числа, соответствующего битовой комбинации (*Counter[0x].Value*).
В зависимости от применения это число, которое соответствует битовой комбинации кода Грея, может преобразовываться в соответствующее десятичное значение.

### 5.5.2 Реакция при обнаружении ошибки

Если тестовые программы обнаруживают в компоненте счетчика устройства или модуля ошибку, то для анализа в прикладной программе устанавливается бит состояния. Дополнительно прикладная программа может учитывать также соответствующий код ошибки.
Компактная система активирует светодиод *ERROR*, модуль F60 — светодиод *ERR*.
Благодаря использованию кода ошибки существуют дополнительные возможности контролировать внешнее подключение и программировать реакции на ошибки в прикладной программе.

| Версия | Доступ к коду ошибки | Имя кода ошибки |
|---|---|---|
| Для версии CPU OS V7 и выше | Во вкладке ...*Channels* в детальном представлении модуля или детали устройства | -> Error Code [Byte] в строке с номером канала |
| Для версий ниже CPU OS V7 | В окне *Signal Connections...* модуля или детали устройства | Counter[*xx*].Error Code, *xx* = номер канала |

Таблица 19: Коды ошибок для входов счетчика

## 5.6 Контрольный перечень для безопасных входов

Данный контрольный перечень является рекомендацией для проектирования, программирования и ввода в эксплуатацию безопасных входов. Он предназначен для использования в качестве документации по планированию, а также служит для подтверждения добросовестно выполненного планирования.

Для каждого отдельного используемого в системе безопасного входного канала в рамках проектирования либо ввода в эксплуатацию следует заполнять собственный контрольный перечень для контроля учитываемых требований. Только в таком случае можно обеспечить полную и наглядную регистрацию требований. Контрольный перечень также является документом, в котором указана связь между внешней проводкой и прикладной программой.

Контрольный перечень *HIMatrix_Checklist_Inputs.doc* доступен в виде документа в формате Microsoft© Word©. ZIP-файл *HIMatrix_Checklists.zip* содержит все контрольные перечни, его можно скачать на веб-сайте HIMA www.hima.com.

# 6 Выходы

Обзор выходов системы HIMatrix

| Устройство | Тип | Количество выходов | Безопасный | С электрическим разделением |
|---|---|---|---|---|
| Система управления F20 | Цифровой | 8 | • | - |
| | Такт | 4 | - | - |
| Система управления F30 (конфигурируется для управления линией) | Цифровой | 8 | • | - |
| Система управления F31 (конфигурируется для управления линией) | Цифровой | 8 | • | - |
| Система управления F35 | Цифровой | 8 | • | - |
| Remote I/O F1 DI 16 01 | Такт | 4 | - | - |
| Remote I/O F2 DO 4 01 | Цифровой | 4 | • | - |
| Remote I/O F2 DO 8 01 | Цифровой | 8 | • | • |
| Remote I/O F2 DO 16 01 | Цифровой | 16 | • | - |
| Remote I/O F2 DO 16 01 | Реле | 16 | • | • |
| Remote I/O F3 DIO 8/8 01 | Цифровой, 1-полюсный | 8[1)] | • | - |
| | Цифровой, 2-полюсный | 2[1)] | | |
| Remote I/O F3 DIO 16/8 01 | Цифровой, 1-полюсный | 16[1)] | • | - |
| | Цифровой, 2-полюсный | 8[1)] | | |
| Remote I/O F3 AIO 8/4 01 | Аналоговый | 4 | - | - |
| Устройства удаленного ввода/вывода F3 DIO 20/8 01 и F3 DIO 20/8 02 (конфигурируются для управления линией) | Цифровой | 8 | • | - |
| Модульная система управления F60: | | | | |
| Модуль DIO 24 16 01 (конфигурируются для управления линией) | Цифровой | 16 | • | • |
| Модуль DO 8 01 (110 В) | Реле | 8 | • | • |
| Модуль CIO 2/4 01 | Цифровой | 4 | • | • |
| Модуль AO 8 01 | Аналоговый | 8 | • | • |
| [1)] Более подробную информацию см. в соответствующем руководстве | | | | |

Таблица 20: Обзор выходов системы HIMatrix

## 6.1 Общие положения

Система управления описывает безопасные выходы один раз в каждом цикле, производит обратное считывание выходных сигналов и сравнение с заданными выходными данными.

Для выходов значение 0 или открытый релейный контакт являются безопасным состоянием.

Кроме того, в безопасные выходные каналы последовательно интегрированы три тестируемых переключателя. Таким образом, в выходной канал интегрирован необходимый для обеспечения функции безопасности второй независимый способ отключения. Этот встроенный блок предохранительного отключения в случае ошибки отключает все каналы неисправного модуля вывода (обесточенное состояние).

Кроме того, сигнал сторожевого устройства ЦПУ также является второй возможностью предохранительного отключения: отсутствие сигнала сторожевого устройства приводит к незамедлительному переходу в безопасное состояние.

Эта функция действует только для всех цифровых выходов и релейных выходов систем управления.

Использование соответствующего кода ошибки дает дополнительные возможности для конфигурации в прикладной программе реакции на ошибки.

## 6.2 Безопасность исполнительных элементов

При безопасном применении как система управления, так и подключенные к ней исполнительные элементы должны соответствовать требованиям безопасности и указанному уровню совокупной безопасности. Подробнее см. раздел «Повышение уровня совокупной безопасности датчиков и исполнительных элементов» в приложении.

## 6.3 Безопасные цифровые выходы

Названные пункты действительны как для каналов цифрового вывода модулей системы F60, так и для каналов цифрового вывода компактных систем. Исключение для обоих случаев представляют релейные выходы.

### 6.3.1 Тестовые программы для цифровых выходов

Устройства и модули автоматически тестируются во время работы. Основные тестовые функции:

- Считывание выходного сигнала коммутирующего усилителя. Порог переключения для обратно считываемого низкого уровня: 2 В. Используемые диоды предотвращают обратное питание сигналов.
- Проверка встроенного двойного предохранительного отключения.
- Тест отключения выходов выполняется в качестве фонового теста соответственно макс. в течение 200 мкс. Минимальный промежуток между двумя тестами составляет ≥ 20 секунд.

Система контролирует рабочее напряжение и отключает все выходы при пониженном напряжении < 13 В.

### 6.3.2 Реакция при обнаружении ошибки

Если система управления определяет ошибочный сигнал, она переводит соответствующий выход устройства или модуля с помощью ключа безопасности в безопасное обесточенное состояние. При ошибке модуля отключаются все выходы модуля. Компактная система показывает обе ошибки дополнительно с помощью светодиода *ERROR*, а модуль F60 — с помощью светодиода *ERR*.

### 6.3.3 Поведение при коротком замыкании или перегрузке

При замыкании выхода на L- или перегрузке возможность тестирования устройства или модуля сохраняется. Отключение посредством устройства предохранительного отключения не требуется.

Система управления контролирует общее потребление тока устройства или модуля и при превышении порога переводит все выходные каналы в безопасное состояние.

В этом состоянии выходы циклически с интервалом в несколько секунд проверяются на наличие перегрузки. При нормальном состоянии выходы снова подключаются.

### 6.3.4 Управление линией

Система управления может перемещать безопасные цифровые выходы или специальные тактовые выходы и использовать вместе с безопасными цифровыми входами одной и той же системы (но не с цифровыми входами системы F35 или F60 MI 24 01) для распознавания замыкания и обрыва линии, см. главу 5.3.6.

## ПРИМЕЧАНИЯ

**Тактовые выходы нельзя использовать как безопасные выходы, напр., для включения безопасных исполнительных элементов!**

Релейные выходы не могут использоваться как тактовые выходы.

## 6.4 Безопасные 2-полюсные цифровые выходы

Описываемые здесь характеристики касаются 2-полюсных цифровых выходов устройств удаленного ввода/вывода F3 DIO 8/8 01 и F3 DIO 16/8 01.

Устройства автоматически тестируются во время работы. Основные тестовые функции:

- Считывание выходного сигнала коммутирующего усилителя. Используемые диоды предотвращают обратное питание сигналов.
- Проверка встроенного (двойного) предохранительного отключения
- Тест отключения выходов выполняется в качестве фонового теста соответственно макс. в течение 200 мкс. Минимальный промежуток между двумя тестами составляет ≥ 20 секунд.
- Диагностика линий при 2-полюсном подключении
  F3 DIO 16/8 01:
  - Короткое замыкание на L+, L-
  - Короткое замыкание между 2-полюсными подключениями.
  - Обрыв провода в одном из двух 2-полюсных подключений.

  F3 DIO 8/8 01:
  - Короткое замыкание на L+, L-

Система контролирует рабочее напряжение и отключает все выходы при пониженном напряжении < 13 В.

Для 2-полюсного подключения необходимо соблюдать следующие указания.

i Возможно непреднамеренное включение подключенного к выходу реле или исполнительного элемента!

В приложениях в машинной безопасности при обнаружении замыкания линии необходимо выключать выходы DO+, DO-.

i Если выполнение вышеуказанных требований невозможно, то нужно учитывать следующее:

При замыкании линии DO- на L- реле может втягиваться, либо иной исполнительный элемент может перемещаться в другое состояние переключения.

Причина: пока идет время контроля для диагностики линий на потребителе (реле, переключаемом исполнительном элементе) имеется уровень напряжения 24 В (выход DO+), т. е. потребитель должен быть в состоянии потреблять достаточное количество электроэнергии, чтобы переключиться в другое состояние.

Время контроля следует параметрировать таким образом, чтобы исполнительный элемент не мог активироваться от тестового импульса для диагностики линий.

i Возможная неисправность распознавания обрыва линии!

При 2-полюсном подключении нельзя соединять вход DI с выходом DO. Это препятствовало бы распознаванию обрыва линии.

### 6.4.1 Реакция при обнаружении ошибки

#### Выходы DO-

При обнаружении ошибочного сигнала устройство или модуль переводит соответствующий выход в безопасное, обесточенное состояние. Ошибка устройства или модуля приводит к отключению всех выходов. Ошибки обоих видов устройство дополнительно отображает светодиодом *ERROR*.

#### Выходы DO+

При обнаружении ошибочного сигнала устройство или модуль переводит соответствующий выход в безопасное, обесточенное состояние. Ошибка устройства или модуля приводит к отключению всех выходов. Обе ошибки устройство дополнительно отображает светодиодом *ERROR*.

### 6.4.2 Поведение при коротком замыкании или перегрузке

При замыкании выхода на L- или L+, а также при перегрузке возможность тестирования устройства или модуля сохраняется. Отключение посредством устройства предохранительного отключения не требуется.

Общее потребление тока устройства или модуля контролируется. При превышении порога устройство/модуль переводит все каналы в безопасное состояние.

В этом состоянии устройство или модуль циклически с интервалом в несколько секунд проверяет выходы на наличие перегрузки. При нормальном состоянии устройство или модуль снова включает выходы.

## 6.5 Релейные выходы

Релейные выходы по функциональности соответствуют цифровым выходам, но при этом предлагают гальваническую развязку и более высокую пробивную прочность.

### 6.5.1 Тестовые программы для релейных выходов

Устройство или модуль автоматически тестирует выходы во время работы. Основные тестовые функции:

- Обратное считывание выходных сигналов коммутирующего усилителя перед реле,
- Проверка переключения реле с принудительным управлением контактами,
- Проверка встроенного двойного предохранительного отключения.

Система контролирует рабочее напряжение и отключает все выходы при пониженном напряжении < 13 В.

В модуле DO 8 01 и устройствах удаленного ввода/вывода F2 DO 8 01 и F2 DO 16 02 выходы оснащены тремя безопасными реле:

- два реле с принудительным управлением контактами
- одно стандартное реле

Выходы используются для предохранительных отключений.

### 6.5.2 Реакция при обнаружении ошибки

При обнаружении ошибочного сигнала устройство или модуль переводит соответствующий выход с помощью ключа безопасности в безопасное, обесточенное состояние. При ошибке модуля он отключает все выходы. Компактная система

показывает обе ошибки дополнительно с помощью светодиода *ERROR*, а модуль F60 — с помощью светодиода *ERR*.

## 6.6 Безопасные аналоговые выходы (F60)

Модуль AO 8 01 имеет собственную безопасную аналогово-цифровую систему микропроцессора 1oo2 с безопасной связью. Он описывает аналоговые выходы один раз за цикл и производит внутреннее сохранение значений. Модуль тестирует свою работу сам.

DIP-переключатели на безопасных модулях аналогового вывода могут настраивать выходы напряжения или тока. При этом необходимо удостовериться, что их настройки соответствуют использованию в системе
и параметрированию в прикладной программе. Несоблюдение приводит
к неправильной работе модуля.

### ПРИМЕЧАНИЯ

**Неправильная работа модуля**

**Перед использованием модуля в системе проверьте:**

- **Настройки DIP-переключателя модуля.**
- **Параметрирование модуля в прикладной программе.**

В зависимости от выбора типа устройства (…FS1000, …FS2000) при конфигурации в логической схеме необходимо учитывать различные значения для выходных сигналов, чтобы поддерживать равные выходные значения, см. руководство (HIMatrix AO 8 01 Manual, HI 800 381 RU).

Соответственно два аналоговых выхода гальванически соединены друг с другом:

- Выход 1 и 2.
- Выход 3 и 4.
- Выход 5 и 6.
- Выход 7 и 8.

В контурах аналогового выхода имеется контроль тока и напряжения, каналы обратного считывания и тестирования, включая параллельные выходные контуры,
а также два дополнительных ключа безопасности для безопасного отключения контуров выходного тока в случае ошибки. Это обеспечивает безопасное состояние (выход тока: 0 мА, выход напряжения: 0 В).

### 6.6.1 Тестовые программы

Модуль автоматически тестируется во время работы. Основные тестовые функции:

- двойное обратное считывание выходного сигнала,
- тест на перекрестные помехи между выходами,
- проверка встроенного предохранительного отключения.

### 6.6.2 Реакция при обнаружении ошибки

Один раз в каждом цикле модуль производит обратное считывание выходных сигналов и их сравнение с сохраненными внутри выходными сигналами. Если модуль обнаруживает отклонение, он отключает содержащий ошибку выходной канал с помощью обоих ключей безопасности и сообщает об ошибке модуля с помощью светодиода *ERR*.

Благодаря использованию соответствующего кода ошибки существуют дополнительные возможности для конфигурации реакций на ошибки с помощью прикладной программы.

Для времени реакции аналоговых выходов в худшем случае к удвоенному времени сторожевого устройства ($2 * WDT_{CPU}$) следует прибавить удвоенное время сторожевого устройства AO-ЦПУ ($2 * WDT_{AO\text{-}\mu C}$).

Время реакции в худшем случае указано в руководстве.

## 6.7 Аналоговые выходы с безопасным отключением (F3 AIO 8/4 01)

Устройство удаленного ввода/вывода один раз за цикл описывает аналоговые выходы и производит внутреннее сохранение значений.

Выходы не являются безопасными, но они могут быть безопасно отключены все вместе.

Для достижения уровня совокупной безопасности SIL 3 необходимо считать выходные значения через безопасные аналоговые входы и проанализировать их в прикладной программе. В прикладной программе необходимо также определить реакции при неправильных выходных значениях.

### 6.7.1 Тестовые программы

Устройство удаленного ввода/вывода автоматически тестирует оба ключа безопасности для отключения всех четырех выходов во время работы.

### 6.7.2 Реакция при обнаружении ошибки

При внутренней ошибке устройства удаленного ввода/вывода оно отключает все четыре выходных канала одновременно при помощи обоих ключей безопасности и сообщает об ошибке модуля посредством светодиода *FAULT* на передней панели.

Благодаря использованию кода ошибки существуют дополнительные возможности для конфигурации в прикладной программе реакций на ошибки.

## 6.8 Контрольный перечень для безопасных выходов

Данный контрольный перечень является рекомендацией для проектирования, программирования и ввода в эксплуатацию безопасных выходов. Он предназначен для использования в качестве документации по планированию, а также служит для подтверждения добросовестно выполненного планирования.

Для каждого отдельного используемого в системе безопасного выходного канала в рамках проектирования либо ввода в эксплуатацию следует заполнять собственный контрольный перечень для контроля учитываемых требований. Только в таком случае обеспечивается полная и наглядная регистрация требований. Кроме того, таким образом документируется связь между внешней проводкой и прикладной программой.

Контрольный перечень *HIMatrix_Checklist_Outputs.doc* доступен в виде документа в формате Microsoft© Word©. ZIP-файл *HIMatrix_Checklists.zip* содержит все контрольные перечни, его можно скачать на веб-сайте HIMA www.hima.com.

# 7 Программное обеспечение для систем HIMatrix

Программное обеспечение для безопасных устройств автоматизации систем HIMatrix делится на следующие части:

- операционная система,
- прикладная программа,
- инструмент программирования согласно IEC 61131-3.

Операционная система загружается в центральный блок (ЦПУ) системы управления, она должна использоваться в действительной, сертифицированной TÜV форме для безопасного применения.

Инструмент программирования служит для составления прикладной программы, содержащей специфические для конкретной установки функции, которые должно выполнять устройство автоматизации. Параметрирование и управление функциями операционной системы также осуществляется при помощи инструмента программирования.

Генератор кода инструмента программирования переводит прикладную программу в машинный код. Инструмент программирования передает этот машинный код посредством интерфейса Ethernet во флеш-память устройства автоматизации.

## 7.1 Аспекты безопасности для операционной системы

Каждая допущенная операционная система имеет свое обозначение. Для лучшей идентификации указаны версия и сигнатура CRC. Действительные, допущенные TÜV для безопасных устройств автоматизации версии операционной системы и соответствующие сигнатуры (CRCs) подлежат ревизионному контролю и вносятся в перечень, составляемый TÜV совместно с HIMA.

Считать текущий номер версии операционной системы можно только с помощью инструмента программирования. Необходим контроль со стороны пользователя (ср. 7.6, «Контрольный перечень по созданию прикладной программы»).

## 7.2 Принцип работы и функции операционной системы

Операционная система циклически выполняет прикладную программу. При этом в сильно упрощенной форме она выполняет следующие функции:

- Считывание входных данных.
- Обработка логический функций, которые запрограммированы согласно IEC 61131-3.
- Запись выходных данных.

Также выполняются следующие основные функции:

- Обширная самодиагностика.
- Тесты входов и выходов во время работы.
- Передача данных.
- Диагностика.

## 7.3 Аспекты безопасности для программирования

### 7.3.1 Концепция безопасности инструмента программирования

Концепция безопасности инструментов программирования ELOP II Factory и SILworX:

- При установке инструмента программирования контрольная сумма CRC защищает целостность пакета программы на пути от изготовителя к пользователю.
- Инструмент программирования выполняет проверки достоверности, чтобы минимизировать возможность ошибки при вводе.

- Необходимо произвести двойное компилирование с последующим сравнением созданных контрольных сумм — CRC конфигураций, см. главу 8.2.3. Благодаря этому обеспечивается распознавание искажений приложения посредством временного неправильного функционирования используемого ПК.
- Благодаря инструменту программирования и указанным в настоящем руководстве по безопасности мерам практически невозможно создание семантически и синтаксически корректного кода, который еще содержит неопознанные систематически ошибки процесса создания кода.

При каждом вводе в эксплуатацию безопасного управления следует соблюдать требования верификации и валидации в соответствии со стандартами использования!

При первом вводе в эксплуатацию безопасной системы управления следует проверить безопасность всей системы, выполнив полный тест функциональности.

**Тест функциональности системы управления**

1. Проверка правильного осуществления задачи управления на основании данных и потоков сигналов.
2. Полная функциональная проверка логической схемы путем отладки (см. главу 7.3.2).

Система управления и прикладная программа проверены в достаточной степени.

#### Для версии CPU OS V7 и выше

Безопасное сравнивающее устройство версий от SILworX может выявлять изменения по сравнению с предыдущей версией и отображать их.

После изменения прикладной программы следует проверить только те части программы, которых коснулось изменение.

#### Для версий ниже CPU OS V7

После изменения прикладной программы необходимо проверить ее с помощью полного теста функциональности.

### 7.3.2 Проверка конфигурации и прикладной программы

Чтобы проверить составленную прикладную программу на соблюдение указанной функции безопасности, необходимо сгенерировать подходящие варианты теста, которые покрывают системную спецификацию.

Как правило, достаточно независимого теста каждого контура (состоит из входа, важных для эксплуатации соединений и выхода).

Также и для числового анализа формул следует сгенерировать подходящие варианты теста. Имеет смысл выполнить тесты класса эквивалентности. Это тесты в рамках определенного диапазона значений, при предельных значениях или в недопустимых диапазонах значений. Варианты теста следует выбирать таким образом, чтобы подтверждалась правильность логической схемы программы. Необходимое количество вариантов теста зависит от используемой логической схемы программы и должно охватывать критические пары значений.

Только активное моделирование с источниками может подтвердить правильность проводки датчиков и исполнительных элементов системы (в том числе подключенных посредством коммуникации с удаленными устройствами ввода/вывода). Кроме того, только так можно проверить конфигурацию системы.

### 7.3.3 Архивирование проекта

Компания HIMA рекомендует архивировать проект после загрузки программы в систему управления. Это распространяется как на загрузку, так и на перезагрузку.

Архивирование проекта принципиально различается для инструментов ELOP II Factory и SILworX.

### Архивирование проекта для версий CPU OS V7 и выше

SILworX создает проект в файле проекта. Возможно его резервное копирование, например, на внешнем носителе данных.

### Создание архива проекта ниже CPU OS V7

ELOP II создает проект в структуре подкаталога. Для архивирования ELOP II Factory может сохранять содержание данной структуры в архиве проекта в виде архивного файла. Возможно резервное копирование такого архива проекта, например, на внешнем носителе данных.

**Создание архива проекта**

1. Распечатать прикладную программу для сравнения логики с требованиями.
2. Компилировать прикладную программу для создания конфигурационных CRC ЦПУ
3. Записать версию конфигурационной CRC ЦПУ. Для этого в управлении аппаратным обеспечением (Hardware Management) нужно выбрать систему управления, и в контекстном меню **Информация о конфигурации** отобразятся версии. К определению версии относится:
   - rootcpu.config отображает безопасную конфигурацию ЦПУ, конфигурационный CRC ЦПУ
   - rootcom.config отображает небезопасную конфигурацию COM
   - root.config отображает общую конфигурацию, включая конфигурацию устройств удаленного ввода/вывода (ЦПУ + COM).
4. Создать на носителе данных архив проекта, указав имя прикладной программы, конфигурационные CRC ЦПУ и дату.
   Эта рекомендация не заменяет внутренние требования к документации, установленные для пользователя.

Архив проекта создан.

## 7.3.4 Возможность идентификации программы и конфигурации

Прикладные программы однозначно идентифицируются по конфигурационным CRC проекта. Это позволяет производить сравнение с конфигурационным CRC загруженного проекта.

### Файлы проектов для версий от CPU OS V7 и выше

Чтобы убедиться, что защищенный файл проекта не изменен, необходимо скомпилировать содержащийся ресурс и сравнить конфигурационную CRC с CRC загруженной конфигурации. Последняя может отображаться с помощью SILworX.

### Архивы для версий ниже CPU OS V7

Обозначение архива должно содержать конфигурационные CRC root.config.

Чтобы удостовериться в том, что используемый архив не был изменен, нужно компилировать ресурс после восстановления проекта из архива, а затем сравнить конфигурационную CRC root.config с CRC загруженной конфигурации, которую можно отобразить при помощи ELOP II Factory.

Для контроля в Control Panel ресурса нужно открыть меню
**Resource → Check Consistency**.

## 7.4 Параметры ресурса

**⚠ ОПАСНОСТЬ**

**Опасность травмирования персонала из-за неправильной кофигурации!**

**Ни система программирования, ни система управления не могут проверять некоторые параметры, установленные для конкретного проекта. Поэтому обязательно вносить эти параметры в систему программирования правильно и проверять сделанную запись.**

**Эти параметры:**

- **System ID**
- **Rack ID, см. руководства по системе (HIMatrix System Manual Compact Systems HI 800 394 RU) и (HIMatrix System Manual Modular System HI 800 391).**
- **Safety Time**
- **Watchdog Time**
- **Main Enable**
- **Autostart**
- **Start Allowed**
- **Load Allowed**
- **Reload Allowed**
- **Global Forcing Allowed**

Приведенные ниже параметры задаются в инструменте программирования для допустимых действий в безопасном режиме устройства автоматизации и обозначаются как безопасные параметры.

Параметры, которые могут задаваться во время безопасного режима, не привязаны к определенному классу требований, для каждого применения системы управления они должны согласовываться с полномочным отделом контроля.

### 7.4.1 Системные параметры для версий выше CPU OS V7

Для версий выше CPU OS V7 существует разделение на системные параметры ресурса и системные параметры аппаратного обеспечения.

#### 7.4.1.1 Системные параметры ресурса

Системные параметры ресурса определяют действие системы управления во время эксплуатации и задаются в SILworX в диалоговом окне *Properties* ресурса.

| Параметр | Описание | Значение по умолчанию | Настройка для безопасной эксплуатации |
|---|---|---|---|
| Name | Имя ресурса | | Произвольная |
| System ID [SRS] | Системный ID ресурса<br>1…65 535<br>ID системы должно быть присвоено значение, отличное от значения по умолчанию, в противном случае проект не будет готов к выполнению! | 60 000 | Уникальное значение внутри сети систем управления. Это все системы управления, которые потенциально связаны между собой. |
| Safety Time [ms] | Безопасное время в миллисекундах<br>20…22 500 мс | 600 мс/<br>400 мс [1)] | зависит от приложения |
| Watchdog Time [ms] | Время сторожевого устройства в миллисекундах:<br>4...5000 мс для устройств/модулей F*03, 8…5000 мс для стандартных устройств/модулей | 200 мс/<br>100 мс [1)] | зависит от приложения |

| | | | |
|---|---|---|---|
| Target Cycle Time [ms] | Необходимое или максимальное время цикла, см. *Target Cycle Time Mode*, 0...7500 мс. Заданное время цикла максимально может равняться разности времени сторожевого устройства *(watchdog time)* и минимального времени сторожевого устройства, иначе оно будет отклонено ПЭС.<br>Если значение по умолчанию выставлено на 0 мс, требуемое значение времени цикла не учитывается. | 0 мс | зависит от приложения |
| Target Cycle Time Mode | Использование *Target Cycle Time [ms],* см. Таблица 22.<br>Для устройств/модулей F*03 применяются все значения, для стандартных устройств/модулей — только фиксированные *(Fixed)*! | Fixed-tolerant | зависит от приложения |
| Multitasking Mode | Применяется только для устройств/модулей F*03! | Mode 1 | зависит от приложения |
| | Mode 1 Длительность цикла ЦПУ зависит от необходимой продолжительности выполнения всех прикладных программ. | | |
| | Mode 2 Процессор выделяет из времени выполнения, не востребованного прикладными программами с низким приоритетом, время выполнения для прикладных программ высокого приоритета. Режим функционирования, обеспечивающий высокий уровень готовности. | | |
| | Mode 3 Процессор не ждет, пока истечет время выполнения прикладных программ, и в результате увеличивается продолжительность цикла. | | |
| Max.Com.Time Slice ASYNC [ms] | Максимальное значение (в мс) временного промежутка, используемого для коммуникации в рамках цикла ресурса, см. руководство по связи (Communication Manual HI 801 062 RU), 2...5000 мс | 60 мс | зависит от приложения |
| Max. Duration of Configuration Connections [ms] | Применяется только для устройств/модулей F*03!<br>Задает промежуток времени в рамках цикла ЦПУ, доступный для коммуникации данных процесса, 2...3500 мс | 6 мс | зависит от приложения |
| Maximum System Bus Latency [µs] | Для систем управления HIMatrix не применимо! | 0 мкс | - |
| Allow Online Settings | ON Все переключатели/параметры, перечисленные под OFF, могут быть изменены онлайн с помощью PADT. | ON | Рекомендуется OFF |
| | OFF Для данных параметров **отсутствует** возможность корректировки онлайн:<br>▪ *System ID*<br>▪ *Autostart*<br>▪ *Global Forcing Allowed*<br>▪ *Global Force Timeout Reaction*<br>▪ *Load Allowed*<br>▪ *Reload Allowed*<br>▪ *Start Allowed*<br>Данные параметры имеют возможность для корректировки онлайн в случае, если *Reload Allowed* присвоено значение ON:<br>▪ *Watchdog Time* (время сторожевого устройства ресурса)<br>▪ *Safety Time*<br>▪ *Target Cycle Time*<br>▪ *Target Cycle Time Mode*<br>Они не могут быть изменены онлайн, если *Reload Allowed* имеет значение OFF. | | |
| | i Параметру *Allow Online Settings* возможно присвоить значение ON только при остановленной ПЭС! | | |

| Параметр | Описание | Значение по умолчанию | Настройка для безопасной эксплуатации |
|---|---|---|---|
| Autostart | ON: Если процессорный модуль подсоединен к питающему напряжению, прикладная программа запускается автоматически<br>OFF: после подключения питающего напряжения автоматический старт не происходит. | OFF | зависит от приложения |
| Start Allowed | ON: Разрешен холодный, теплый или горячий пуск с помощью PADT в состоянии RUN или STOP.<br>OFF: Запуск не разрешен | ON | зависит от приложения |
| Load Allowed | ON: Загрузка конфигурации разрешена<br>OFF: Загрузка конфигурации не разрешена | ON | зависит от приложения |
| Reload Allowed | Применяется только для устройств/модулей F*03!<br>ON: Перезагрузка конфигурации разрешена.<br>OFF: Перезагрузка конфигурации не разрешена. При переключении на OFF текущая перезагрузка не прерывается | ON | зависит от приложения |
| Global Forcing Allowed | ON: Глобальная инициализация для данного ресурса разрешена<br>OFF: Глобальная инициализация для данного ресурса не разрешена | ON | зависит от приложения |
| Global Force Timeout Reaction | определяет порядок действий ресурса по истечении времени ожидания инициализации:<br>▪ Stop Forcing<br>▪ Stop Resource | Stop Forcing | зависит от приложения |
| Minimum Configuration Version | Данная настройка позволяет генерировать код, который, в зависимости от требований проекта, совместим со старыми или новыми версиями операционной системы процессорного модуля.<br>SILworX V2: Генерирование кода реализовано так же, как в SILworX V2. С данной настройкой поддерживается использование кода на стандартных устройствах и модулях с операционной системой процессорного модуля V7.<br>SILworX V3: Для систем управления HIMatrix не применимо!<br>SILworX V4: Сгенерированный код совместим с операционной системой процессорного модуля V8.<br>SILworX V5: Соответствует *SILworX V4*. Данная установка гарантирует совместимость с последующими версиями. | SILworX V5 в новых проектах | зависит от приложения |
| safe**ethernet** CRC | SILworX V2.36.0: Создание CRC для safe**ethernet** выполняется так же, как в SILworX V2.36.0. Данная настройка необходима для обмена данными с ресурсами, запланированными в SILworX V2.36 или более ранней версии.<br>Current Version: Создание CRC для safe**ethernet** выполняется с помощью текущего алгоритма. | Current Version | зависит от приложения |

[1] Первое значение действует для систем управления, второе значение — для устройств удаленного ввода/вывода.

Таблица 21: Системные параметры ресурса для версии CPU OS V7 и выше

Приведенная ниже таблица описывает воздействие, оказываемое режимом заданного времени цикла.

| Target Cycle Time Mode | Воздействие на прикладные программы | Воздействие на перезагрузку процессорных модулей |
|---|---|---|
| Fixed | ПЭС обеспечивает соответствие заданному времени цикла и при необходимости продлевает цикл. Если время обработки прикладных программ превышает заданное время цикла, цикл продлевается. | Перезагрузка выполняется только при достаточном заданном времени цикла. |
| Fixed-tolerant | Как при *Fixed*. | Максимум каждый четвертый цикл увеличивается для выполнения перезагрузки. |
| Dynamic-tolerant | Как при *Dynamic*. | Максимум каждый четвертый цикл увеличивается для выполнения перезагрузки. |
| Dynamic | HIMatrix по возможности выдерживает заданное время цикла и выполняет цикл за максимально короткое время. | Перезагрузка выполняется только при достаточном заданном времени цикла. |

Таблица 22: Воздействие режима заданного времени цикла

Указания к параметру *Minimum Configuration Version*:

- При создании каждого нового проекта выбирается самая актуальная *Minimum* Configuration Version. Необходимо удостовериться в том, что эти настройки совместимы с используемым аппаратным обеспечением. Например, стандартные устройства HIMatrix требуют для *Minimum Configuration Version* значение *SILworX V2*.
- Если проект был конвертирован из предыдущей версии SILworX, то установленное в предыдущей версии значение параметра *Minimum Configuration Version* сохраняется. Благодаря этому генерирование кода создает ту же конфигурацию CRC, что и в предыдущей версии, а генерированная конфигурация совместима с операционной системой в аппаратном обеспечении.

  Поэтому при работе с конвертированными проектами не следует менять параметр *Minimum Configuration Version*.
- SILworX автоматически генерирует более высокую версию конфигурации, чем установленное значение параметра *Minimum Configuration Version*, если в проекте используются возможности, предоставляемые только более высокой версией. Об этом SILworX сообщает, предоставляя результаты генерирования кода. Аппаратное обеспечение не может загрузить более высокую версию конфигурации, чем та, которая совместима с его операционной системой.

  Чтобы легче было разобраться, нужно просто сопоставить данные, предоставленные функцией сравнения версий, с информацией, которую дает обзор данных модуля.
- Если для ресурса параметру *Minimum Configuration Version* присвоено значение *SILworX V4* или выше, то в каждой прикладной программе (см. ниже) следует установить для параметра *Code Generation Compatibility* значение *SILworX V4*.

#### 7.4.1.2 Системная переменная аппаратного обеспечения для версий от CPU OS V7 и выше

Эти переменные служат для изменения поведения системы управления во время работы в определенных состояниях. Эти переменные настраиваются в редакторе аппаратных устройств SILworX в режиме детального представления аппаратного обеспечения.

| Параметр/переключатель | Функция | Настройка по умолчанию | Настройка для безопасной эксплуатации |
|---|---|---|---|
| Force Deactivation | Служит для предотвращения и непосредственного отключения инициализации | FALSE | зависит от приложения |
| Spare 0... Spare 16 | Функция отсутствует | - | - |
| Emergency Stop 1...Emergency Stop 4 | Аварийный выключатель для отключения системы управления при сбоях, распознанных прикладной программой | FALSE | зависит от приложения |
| Relay Contact 1...Relay Contact 4 | Применимо только для F*03! Управляет соответствующими контактами реле при наличии таковых. | FALSE | зависит от приложения |
| Read-only in Run | После запуска системы управления никакие действия по управлению (остановка, запуск, загрузка) больше не могут реализовываться через SILworX; исключения: инициализация и перезагрузка | FALSE | зависит от приложения |
| Reload Deactivation | Применимо только для F*03! Предотвращает загрузку системы управления посредством перезагрузки. | FALSE | зависит от приложения |
| User LED 1 ... User LED 2 | Применимо только для специальных систем управления! Управляет соответствующими светодиодами при наличии таковых. | FALSE | - |

Таблица 23: Системные переменные аппаратного обеспечения для версии CPU OS V7 и выше

Для этих системных переменных устанавливается связь с глобальными переменными, значение которых изменяется посредством физического входа или логической схемы прикладной программы.

Пример: к цифровому входу подключен кодовый переключатель. Цифровой вход присвоен глобальной переменной, которая присвоена системным переменным *Read only in Run*. В этом случае, используя кодовый переключатель, владелец ключа может разрешать или блокировать такие действия обслуживания, как останов, запуск и загрузка.

### 7.4.2 Системные параметры для версий ниже CPU OS V7

| Переключатель | Функция | Значение по умолчанию | Настройка для безопасной эксплуатации |
|---|---|---|---|
| Main Enable | Следующие кнопки-флажки/параметры можно изменять во время работы (=RUN) с помощью PADT. | ON | OFF [1] |
| Autostart | Автоматический запуск после Power ON системы управления. | OFF | зависит от приложения |
| Start/Restart Allowed | Холодный, теплый или горячий пуск с помощью PADT в состоянии RUN или STOP. | ON | OFF [1] |
| Load Allowed | Разрешение загрузки прикладной программы. | ON | ON |
| Test Mode Allowed | Разрешен или запрещен тестовый режим прикладной программы. В тестовом режиме обработка программы фиксируется или останавливается. Выходы остаются включенными, а обработка программы может быть выполнена в рамках отдельных шагов цикла. | OFF | OFF |
| Change Variables in OLT Allowed | Значения и переменные могут отображаться и изменяться в полях онлайн-теста (OLT) логической схемы. | OFF | OFF [2] |
| Forcing Allowed | Разрешены ввод и активация значений для переменных/сигналов ПЭС, независимо от текущего значения сигнала процесса или логической схемы. | OFF | Установлено отделом контроля |
| Stop at Force Timeout | Останов ЦПУ после превышения времени инициализации. | ON | Установлено отделом контроля |

[1] В режиме RUN возможно только изменение на значение OFF.

[2] В режиме RUN возможно только изменение на ON.

Таблица 24: Системные параметры ресурса для версии ниже CPU OS V7

Для инициализации можно предварительно задать другие кнопки-флажки и параметры.

## 7.5 Защита от манипуляций

Пользователь совместно с полномочным отделом контроля должен определить, какие меры будут использоваться для защиты от манипуляций.

В ПЭС и в инструмент программирования встроены механизмы защиты, предотвращающие случайные или несанкционированные изменения в системе безопасности:

- Изменение прикладной программы или конфигурации приводит к созданию нового CRC.
- Чтобы иметь возможность управления, пользователь должен войти в ПЭС.
- Для входа в ПЭС инструмент программирования запрашивает пароль при входе пользователя в систему.
- Соединение между PADT и ПЭС во время режима RUN не требуется и может прерываться.

Необходимо соблюдать требования стандартов безопасности и использования в отношении защиты от манипуляций. Авторизация сотрудников и принятие необходимых мер защиты входят в сферу ответственности эксплуатирующей стороны.

## ПРИМЕЧАНИЯ

**Доступ к системе управления HIMatrix должен иметь только уполномоченный персонал!**

**Для защиты от несанкционированных изменений в системе управления необходимо предпринять следующие меры:**

- **Измените настройки по умолчанию для имени пользователя и пароля.**
- **Каждый пользователь должен сохранять свой пароль в тайне.**
- **PADT после завершения ввода в эксплуатацию необходимо отсоединить от системы управления и подсоединять только в том случае, если необходимы изменения.**

Доступ к данным ПЭС возможен только в том случае, если используемый PADT имеет инструмент программирования и проект пользователя в актуальной версии (обслуживание архива!).

Соединение между PADT и ПЭС необходимо только для загрузки прикладной программы или считывания переменных/сигналов. Во время обычной эксплуатации PADT не требуется. Отделение PADT и ПЭС на этапе обычной работы защищает от несанкционированного доступа.

## 7.6 Контрольный перечень по созданию прикладной программы

Данный контрольный перечень представляет собой рекомендацию пользователю для соблюдения аспектов безопасности при программировании, перед загрузкой новой или измененной программы, а также после нее.

Контрольный перечень *HIMatrix_Checklist_Program.doc* доступен в виде документа в формате Microsoft© Word©. ZIP-файл *HIMatrix_Checklists.zip* содержит все контрольные перечни, его можно скачать на веб-сайте HIMA www.hima.de.

# 8 Аспекты безопасности для прикладной программы

Общая последовательность программирования устройств автоматизации HIMatrix для безопасного применения:

- Спецификация функции управления.
- Запись прикладной программы.
- Компиляция прикладной программы при помощи генератора C-кода.
- Двукратная компиляция прикладной программы, оба результата (конфигурационные CRC) необходимо сравнить друг с другом.
- Программа не содержит ошибок и может работать.
- Верификация и валидация.

Затем PES может начинать безопасную работу.

## 8.1 Рамки безопасного применения

(Предзаданные параметры и правила, пояснения требований безопасности, глава 3.4)

Ввести прикладную программу с помощью допустимого инструмента программирования:

- SILworX для операционных систем с версией от CPU OS V7 и выше.
- ELOP II Factory для операционных систем с версией ниже CPU OS V7.

Разрешенные операционные системы для персональных компьютеров см. в информации к версии инструмента программирования.

Инструмент программирования содержит следующие основные функции:

- Ввод (редактор функциональных блоков), контроль и документацию.
- Переменные с символическими именами и типом данных (BOOL, UINT и т. д.).
- Присвоение систем управления системы HIMatrix.
- Генератор кода (компиляция программы в машинный код).
- Конфигурацию аппаратного обеспечения.
- Конфигурацию связи.

### 8.1.1 Основы программирования

Задача системы управления должна быть представлена в форме спецификации или технического задания. Данная документация является основой для проверки корректного внедрения в прикладную программу. Вид отображения спецификации зависит от постановки задачи. Это может быть:

- Комбинаторная логическая схема
  - Схема причина/действие (cause/effect diagram).
  - Логическая схема соединения с функциями и функциональными блоками.
  - Функциональные блоки с указанными свойствами.
- Системы циклового управления (цикловое программное управление).
  - Словесное описание шагов с условиями поэтапного переключения и управляемых исполнительных элементов.
  - Блок-схемы
  - Матричная или табличная форма условий поэтапного переключения и управляемых исполнительных элементов.
  - Определение краевых условий, напр., режимов работы, EMERGENCY STOP и т. д.

Концепция входов/выходов установки должна содержать анализ цепей возбуждения, т. е. вид датчиков и исполнительных элементов:

- Датчики (цифровые или аналоговые).
  - Сигнал в нормальном режиме (принцип тока покоя для цифровых датчиков, life-zero для аналоговых датчиков).
  - Сигнал в случае ошибки.
  - Определение избыточностей (1oo2, 2oo3), необходимых для сохранения функции безопасности
    (см. главу «Повышение уровня совокупной безопасности датчиков и исполнительных элементов»).
  - Контроль расхождений и реакция.
- Исполнительные элементы.
  - Положение и активация в нормальном режиме.
  - Безопасная реакция/положение при отключении или отказе питания.

Цели при программировании прикладной программы:

- Легко понять.
- легко проследить.
- Легко изменить.
- Легко тестировать.

### 8.1.2 Функции прикладной программы

Программирование не ограничивается аппаратным обеспечением. Функции прикладной программы программируются произвольно.

- В логической схеме используются исключительно элементы согласно IEC 61131-3 с их соответствующими условиями функционирования.
- Физические входы и выходы, как правило, работают по принципу тока покоя, т. е. их безопасное состояние — *0*. Это необходимо учитывать при программировании.
- Прикладная программа содержит соответствующие логические и/или арифметические функции без учета принципа тока покоя физических входов и выходов.
- Логическая схема должна быть наглядно составлена и понятно документирована для простого поиска ошибок. Это включает в себя использование функциональных диаграмм.
- Допускается любое выполнение логических операций отрицания.
- Сигналы об ошибках входов/выходов или элементов логической схемы должны анализироваться.

Важным является включение функций в создаваемые пользователем функциональные блоки, а также в функции, основанные на стандартных функциях. Таким образом программу можно четко структурировать по модулям (функции, функциональные блоки). Каждый модуль может рассматриваться в отдельности,
а посредством подключения модулей к более крупному модулю или программе возникает готовая, комплексная функция.

### 8.1.3 Описание переменных и сигналов

Переменная является заполнителем для значения в логической схеме программы. Посредством имен переменных символически выбирается адрес, определяющий место в памяти с сохраненными значениями. Переменная создается в описании переменной программы или функционального блока.

| Версия операционной системы | Количество знаков для имени переменной |
|---|---|
| Для версии CPU OS V7 и выше | 31 |
| Для версий ниже CPU OS V7 | 256 |

Таблица 25: Длина имен переменных

Использование символических имен вместо физического адреса имеет два существенных преимущества:

- В прикладной программе можно использовать обозначения установки для входов и выходов.
- Изменения в присвоении переменных входным и выходным каналам не оказывают влияния на прикладную программу.

В версиях от CPU OS V7 и выше сигналы не используются, только переменные.

Переменные без определенного пользователем предустановленного значения после холодного пуска имеют предустановленное значение по умолчанию 0 или FALSE.

Переменные, источник которых недействителен, например, из-за ошибки аппаратного обеспечения при физическом входе, принимают сконфигурированное предустановленное значение.

#### Сигналы для версий ниже CPU OS V7

Сигнал служит для распределения между различными областями системы управления в целом. Сигнал создается в редакторе сигналов и соответствует глобальному уровню VAR_EXTERNAL программы, если было создано соотношение.

### 8.1.4 Приемка органом, выдающим разрешение

При проектировании установки, требующей приемки, компания HIMA рекомендует как можно раньше обратиться к организациям, выдающим такое разрешение.

## 8.2 Порядок действий

Данная глава описывает типичный порядок действий при создании прикладных программ для безопасных систем управления HIMatrix.

### 8.2.1 Назначение переменных входам/выходам

Необходимые тестовые программы для безопасных устройств ввода/вывода, модулей ввода/вывода или входных/выходных каналов автоматически выполняются операционной системой.

Назначение используемых в прикладной программе переменных различается для инструментов ELOP II Factory и SILworX.

#### Версия операционной системы от 7 и выше

**Назначение переменной входному/выходному каналу**

1. Определить глобальную переменную соответствующего типа.
2. При определении указать соответствующее предустановленное значение по умолчанию.
3. Присвоить глобальную переменную значению входного/выходного канала.
4. В прикладной программе проанализировать код ошибки -> *Error Code [Byte]* и запрограммировать безопасную реакцию на ошибку.

Глобальная переменная присвоена входному/выходному каналу.

#### Версия операционной системы ниже 7

Если значение переменной необходимо присвоить входному/выходному каналу, следует поступать следующим образом:

**Назначение сигнала входному/выходному каналу**

1. Определить сигнал в Signal Editor управления аппаратным обеспечением.
2. Затем при помощи Drag&Drop переместить сигнал в описание переменных программы.
   ☑ VAR_EXTERNAL создается автоматически.
3. При помощи Drag&Drop переместить сигнал в список каналов модуля ввода/вывода.
4. В прикладной программе проанализировать код ошибки и запрограммировать безопасную реакцию на ошибку.

Сигнал присвоен входному/выходному каналу.

Имя системного сигнала для кода ошибки зависит от типа входного/выходного канала.

### 8.2.2 Блокировка и деблокировка системы управления

*Блокировка* системы управления предполагает блокирование функций и возможностей вмешательства пользователя во время работы. Это предотвращает несанкционированное управление прикладной программой. Объем блокировок должен рассматриваться в зависимости от требований безопасности к использованию ПЭС, а также может согласовываться с отделом контроля, ответственным за приемку установки.

*Деблокировка* системы управления обозначает снятие активной блокировки, например, для выполнения действий с системой управления.

i Блокировка и деблокировка возможны только для систем управления и устройства удаленного ввода/вывода F3 DIO 20/8 01, но не для других устройств удаленного ввода/вывода!

#### Для версии CPU OS V7 и выше

Для блокировки служат три системные переменные:

| Переменная | Функция |
|---|---|
| Read-only in Run | ON: Запуск, останов и загрузка системы управления заблокированы.<br>OFF: Запуск, останов и загрузка системы управления возможны. |
| Reload Deactivation | ON: Перезагрузка заблокирована.<br>OFF: Перезагрузка возможна. |
| Force Deactivation | ON: инициализация отключается.<br>OFF: Инициализация возможна. |

Таблица 26: Системная переменная для блокировки и деблокировки ПЭС

Если все три системные переменные имеют значение ON, то доступ к системе управления уже невозможен. В этом случае перевести систему управления в состояние STOP/VALID CONFIGURATION можно только посредством перезапуска. Это позволяет перезапустить прикладную программу.

Пример использования этих системных переменных:

**Приведение системы управления в состояние возможности блокировки**

1. Определить глобальную переменную типа BOOL, предустановленное значение по умолчанию установить на OFF.
2. Приписать глобальную переменную трем системным переменным: *Read only in Run*, *Reload Deactivation* и *Force Deactivation*.
3. Присвоить глобальную переменную значению канала цифрового входа.
4. Подключить к цифровому входу кодовый переключатель.
5. Компилировать программу, загрузить в систему управления и запустить.

Владелец подходящего кода может блокировать и деблокировать систему управления. При ошибке в соответствующем цифровом устройстве ввода или модуле ввода система управления деблокирована.

### Для версий ниже CPU OS V7

**Блокировка**: при блокировке ПЭС необходимо соблюдать следующий порядок действий:

**Блокировка системы управления**

1. Перед компиляцией нужно настроить на системе управления следующие значения (см. также главу ):

| | | |
|---|---|---|
| Main Enable | на | ON |
| Forcing Allowed | на | OFF (в зависимости от использования) |
| Test Mode Allowed | на | OFF |
| Start/Restart allowed | на | ON |
| Load Allowed | на | ON |
| Autostart | на | ON/OFF |
| Stop at Force Timeout | на | ON (в зависимости от использования) |

2. После загрузки и запуска в системе управления в режиме онлайн нужно изменить следующие кнопки-флажки в данной последовательности:

| | | |
|---|---|---|
| Start/Restart allowed | на | OFF |
| Load Allowed | на | OFF |
| Main Enable | на | OFF |

i Только после согласование с отделом контроля следующие кнопки-флажки можно установить на другие значения:

| | | |
|---|---|---|
| Forcing Allowed | на | ON |
| Stop at Force Timeout | на | ON/OFF |
| Start/Restart allowed | на | ON |
| Autostart | на | ON |

Система управления заблокирована.

**Деблокировка**: условием для деблокировки (главная деблокировка на ON) является состояние STOP системы управления. Активация главной деблокировки работающей системы управления (в состоянии RUN) невозможна; напротив, в состоянии RUN можно деактивировать главную деблокировку.

Чтобы обеспечить возможность повторного запуска после инициализации ЦПУ (после сбоя в подаче напряжения), для деблокировки ПЭС следует выполнить следующие действия:

**Деблокировка системы управления**

1. Main Enable установить на ON
2. Start/Restart установить на ON.
3. Запуск прикладной программы.

Система управления деблокирована.

## 8.2.3 Генерирование кода

После полного ввода прикладной программы и назначения входов/выходов системы управления следует сгенерировать код. При этом генератор кода создает конфигурационную CRC. Она является сигнатурой для всей конфигурации ЦПУ, входов/выходов и коммуникации и выдается как шестнадцатеричный код в 32-битном

формате. Сигнатура охватывает все конфигурируемые или изменяемые элементы, например логическую схему, переменные и настройки переключателей.

Для исключения влияния небезопасного ПК сгенерируйте код дважды. Конфигурационная CRC в обеих операциях должна быть идентичной.

**Генерирование кода для безопасной эксплуатации**

1. Запустите генератор кода для создания конфигурационной CRC.
   ☑ Готовый к выполнению код 1 с CRC 1.
2. Заново запустите генератор кода для создания кода с конфигурационной CRC.
   ☑ Готовый к выполнению код 2 с CRC 2.
3. Сравните CRC 1 с CRC 2.
   ☑ Обе одинаковые.

Созданный код применим для безопасной эксплуатации, а также для сертификации отделами контроля.

### 8.2.4 Загрузка и запуск прикладной программы

Процесс загрузки (Download) ПЭС системы HIMatrix может осуществляться только в том случае, если перед этим система была приведена в состояние STOP.

| Версия аппаратного обеспечения | Число прикладных программ на систему управления |
|---|---|
| Стандартное | 1 |
| F*03 | 1...32 |

Таблица 27: Число прикладных программ в PES

Выполняется контроль полной загрузки прикладной программы. Затем можно запустить прикладную программу, т. е. начинается циклическое выполнение программы.

i HIMA рекомендует после каждой загрузки прикладной программы в систему управления архивировать данные проекта, например, на сменный носитель данных.

Это должно обеспечить постоянную доступность данных проекта, подходящих для конфигурации системы управления, даже в случае выхода из строя PADT.

HIMA рекомендует регулярно выполнять архивирование данных независимо от загрузки программы.

### 8.2.5 Перезагрузка для устройств F*03

Если в прикладную программу вносились изменения, то во время работы их можно перенести в ПЭС. Встроенное ПО проверяет и активирует измененную прикладную программу, которая берет на себя задачу управления.

i **При перезагрузке цепочек шагов необходимо учитывать следующее:**

Информация по перезагрузке для цепочек шагов не учитывает актуальный статус цепочки. Поэтому перезагрузка соответствующего изменения цепочки шагов может привести ее в неопределенное состояние. Ответственность за такой исход лежит на пользователе.

Примеры:

- Удаление активного шага. В результате в цепочке шагов не остается ни одного шага в состоянии *Active.*
- Переименование начального шага, когда активен другой шаг.
  В результате образуется цепочка шагов с двумя активными шагами!

**При перезагрузке действий необходимо учитывать следующее:**

В результате перезагрузки загружаются действия вместе с полным набором их данных. Последствия этого следует тщательно обдумать до начала перезагрузки.

Примеры:

- Удаление маркера таймера в результате перезагрузки приводит к тому, что время таймера сразу же истекает. Вследствие этого для выхода *Q*, в зависимости от остаточной загрузки, может установиться значение TRUE.
- Удаление установленных определителей действия у ответственных элементов (например, определителя действия *S*) ведет к тому, что они продолжают оставаться установленными.
- Удаление маркера *P0*, имеющего значение TRUE, запускает триггер.

### 8.2.6 Инициализация

Инициализация означает замену текущего значения переменной на значение инициализации. Переменная может сохранить свое текущее значение посредством физического ввода, связи или логической схемы. Если переменная инициализируется, то ее значение больше не зависит от процесса, а задается пользователем.

**⚠ ПРЕДУПРЕЖДЕНИЕ**

**Возможно нарушение безопасности работы в результате использования инициализированных значений!**

- **Инициализированные значения могут привести к неверным выходным значениям.**
- **Инициализация увеличивает время цикла. В результате этого может быть превышено время сторожевого устройства.**

**Инициализация допускается только после согласования с отделом контроля, ответственным за приемку установки.**

Во время инициализации ответственное лицо должно обеспечивать надежный контроль процесса с помощью дополнительных технических и организационных мер. HIMA рекомендует ограничить время инициализации.

Более подробную информацию по инициализации см. в руководстве по компактным системам (HIMatrix System Manual Compact Systems HI 800 394 RU) и модульным системам (HIMatrix System Manual Modular System HI 800 391 RU).

### 8.2.7 Изменение системных параметров в режиме онлайн для версий от CPU OS V7 и выше

Некоторые системные параметры/переключатели могут быть изменены в системе управления в режиме онлайн. Одним из случаев применения является временное увеличение времени сторожевого устройства, обеспечивающее возможность проведения перезагрузки.

Для данных параметров имеется возможность корректировки онлайн:

| Параметр | Аппаратное обеспечение | Версия операционной системы |
|---|---|---|
| System ID | Все | Все |
| Watchdog Time | Все | Все |
| Safety Time | Все | Все |
| Target Cycle Time | Все | Для версии CPU OS V8 и выше |
| Target Cycle Time Mode | F*03 | Для версии CPU OS V8 и выше |
| Allow Online Settings | Все | Все |
| Autostart | Все | Все |
| Start Allowed | Все | Все |
| Load Allowed | Все | Все |
| Reload Allowed | F*03 | Для версии CPU OS V8 и выше |
| Global Forcing Allowed | Все | Все |
| Global Force Timeout Reaction | Все | Все |

Таблица 28: Параметры, изменяемые в режиме онлайн, в зависимости от размещения аппаратного обеспечения и версии операционной системы

Прежде чем вводить параметры с помощью команды в режиме онлайн, следует удостовериться, что такое изменение параметра не приведет к переходу в опасное состояние. В случае необходимости примите надлежащие организационные и/или технические меры для недопущения материального ущерба.

*Allow Online Settings* позволяет изменение прочих параметров. *Allow Online Settings* в состоянии STOP можно устанавливать только на TRUE.

Значения безопасного времени и времени сторожевого устройства нужно проверить и сравнить с установленным значением безопасного времени, требуемого прикладной программой, или с фактическим временем цикла. Эти значения не могут быть верифицированы ПЭС!

Для устройств/модулей F*03 изменить системные параметры во время работы возможно также с помощью перезагрузки.

### 8.2.8 Документация программы для безопасных случаев применения

Инструмент программирования позволяет автоматически распечатывать документацию проекта. Важнейшие виды документации:

- Описание интерфейсов
- Перечень сигналов
- Логическая схема
- Описание типов данных
- Конфигурации для системы, модулей и системных параметров
- Конфигурация сети
- Список перекрестных ссылок сигналов
- Информация генератора кода

Документация является составляющей частью функциональной приемки установки отделом контроля, требующей разрешения (напр., TÜV). Приемка касается только функции пользователя, а не безопасных модулей и устройств автоматизации системы HIMatrix, которые уже прошли испытание типового образца.

### 8.2.9 Многозадачность для устройств F*03

Многозадачностью называется способность систем HIMatrix F*03 обрабатывать с помощью процессорной системы до 32 прикладных программ.

Отдельные прикладные программы можно запускать, останавливать, загружать и удалять — в том числе и с помощью перезагрузки — независимо друг от друга.

Цикл прикладной программы может длиться в течение нескольких циклов процессора. Это регулируется параметрами ресурса и прикладной программы. На основе этих параметров SILworX рассчитывает время сторожевого устройства прикладной программы:
$\text{Watchdog Time}_{\text{User Program}} = \text{W}atchdog\ Time_{\text{Processor Module}} * Maximum\ Number\ of\ Cycles$ (Время сторожевого устройства прикладной программы = Время сторожевого устройства процессорного модуля * Максимальное количество циклов)

Отдельные прикладные программы, как правило, выполняются без обратного воздействия на источник. Однако возможно и взаимное влияние, связанное со следующими причинами:

- Применение одних и тех же глобальных переменных в нескольких прикладных программах.
- Незапланированно длинные сроки выполнения отдельных прикладных программ в случае, если ограничение не было определено параметром *Max. Duration for Each Cycle*.
- Распределение циклов прикладных программ по циклам процессорных модулей существенно влияет на время реакции прикладной программы и переменных, которые она описывает!
- Прикладная программа анализирует глобальные переменные, описанные другой прикладной программой, с задержкой на столько циклов процессорной системы, сколько установлено для программы с помощью системного параметра *Program's Maximum Number of CPU Cycles*. В неблагоприятном случае возможна следующая последовательность:
  - Программа A записывает глобальную переменную, которая требуется программе B.
  - Программа A завершает свой цикл в том же цикле процессорной системы, в котором программа B начинает свой цикл.
  - Затем программа B только при начале своего следующего цикла может считывать записанные программой A значения.
  - Начавшийся цикл программы B может длиться в течение *Program's Maximum Number of CPU Cycles* * время цикла. Программа B получает записанные программой A значения только в этот момент.
  - Прежде чем будет иметь место реакция программы B на данные значения, может быть превышено количество циклов процессорной системы *Program's Maximum Number of CPU Cycles*!

## ПРИМЕЧАНИЯ

**Возможно взаимное влияние прикладных программ!**

**Применение одних и тех же глобальных переменных в нескольких прикладных программах может стать причиной взаимного влияния прикладных программ, приводящего к различным последствиям.**

- **Поэтому необходимо точно планировать использование одинаковых глобальных переменных в нескольких прикладных программах.**
- **Следует использовать перекрестные ссылки в SILworX для проверки глобальных данных. Глобальные данные можно описывать только в одном месте: либо в прикладной программе, с использованием безопасных входов, либо с помощью протоколов связи, отвечающих за безопасность!**

**Пользователь должен следить за тем, чтобы в результате взаимных влияний прикладных программ не возникало эксплуатационных сбоев!**

Подробнее о многозадачности см. в руководстве по компактным системам (HIMatrix System Manual Compact Systems HI 800 394 RU) или руководстве по модульным системам (HIMatrix System Manual Modular System HI 800 391 RU).

### 8.2.10 Приемка органом, выдающим разрешение

При проектировании установки, требующей приемки, органы, выдающие такое разрешение, рекомендуется подключать как можно раньше.

Приемка касается только функции пользователя, а не безопасных модулей и устройств автоматизации системы HIMax, которые уже прошли испытание типового образца.

# 9 Конфигурацию связи

Наряду с физическими входными и выходными переменными переменные могут обмениваться также с другой системой через канал передачи данных. Для этого переменные соответствующего ресурса описываются в редакторе протоколов инструмента программирования.

Такой обмен данными может происходить как считывание, а также как запись.

## 9.1 Стандартные протоколы

Ряд протоколов связи обеспечивает лишь небезопасную передачу данных. Они могут использоваться только для небезопасных частей функции автоматизации.

**⚠ ОПАСНОСТЬ**

**Травмирование персонала из-за использования ненадежных данных импорта!**

**Не использовать данные, импортированные из ненадежных источников, для функций безопасности прикладной программы!**

Предлагаются следующие стандартные протоколы в зависимости от исполнения системы управления:

- SNTP
- Send/Receive TCP
- Modbus (ведущее/ведомое устройство)
- PROFIBUS DP (ведущее/ведомое устройство)
- INTERBUS

## 9.2 Безопасный протокол (safeethernet)

Безопасная коммуникация через safe**ethernet** сертифицирована до уровня совокупной безопасности 3 (SIL 3).

Контроль безопасной связи параметрируется в редакторе safe**ethernet** Editor/P2P Editor.

Для расчета параметров safeethernet *Receive Timeout* и *Response Time* имеет силу следующее условие:
Временной интервал коммуникации должен быть достаточно большим, чтобы обработать в одном цикле ЦПУ все соединения safe**ethernet**.

Для безопасных функций, которые реализуются через safe**ethernet**, разрешается использовать только настройку **Use Initial Data**.

**ПРИМЕЧАНИЯ**

**Возможен непреднамеренный переход в безопасное состояние!**

***Receive Timeout* время ожидания приема) является безопасным параметром!**

Значение сигнала должно быть больше чем *Receive Timeout* (время ожидания приема) или контролироваться с помощью кольцевой проверки, если должно переноситься каждое значение.

### 9.2.1 Время ожидания приема (Receive Timeout)

*Receive Timeout* — время контроля в миллисекундах (мс), в течение которого от участника коммуникации должен быть получен корректный ответ.

Если в течение *Receive Timeout* (времени ожидания приема) от участника коммуникации не поступает корректного ответа, то безопасная связь закрывается. Входные переменные данного соединения safe**ethernet** ведут себя согласно настроенному параметру *Freeze Data on Lost Connection [ms]*.

Для безопасных функций, которые реализуются через safe**ethernet**, разрешается использовать только настройку **Use Initial Data**.

Поскольку *Receive Timeout* (время ожидания приема) является релевантным для безопасности параметром и составной частью Worst Case Reaction Time $T_R$ (времени реакции в худшем случае, см. главу 9.2.3и далее), то *Receive Timeout* должно рассчитываться, как показано далее, и заноситься в редактор safe**ethernet**.

**Receive Timeout ≥ 4 * Delay + 5 * макс. время цикла**

Условие: временной интервал коммуникации должен быть достаточно большим, чтобы обработать в одном цикле ЦПУ все соединения safe**ethernet**.

| | |
|---|---|
| Delay: | Задержка на линии передачи, например, вызванная сетевым коммутатором или спутником |
| Max. Cycle Time: | Максимальное время цикла обеих систем управления |

i Необходимая отказоустойчивость связи может быть достигнута путем увеличения *Receive Timeout* (времени ожидания приема), если это допустимо по времени для процесса использования.

## ПРИМЕЧАНИЯ

**Максимально допустимое значение для времени ожидания приема (*Receive Timeout*) зависит от процесса применения и настраивается в редакторе** safe**enthernet вместе с максимальным ожидаемым временем ответа (Response Time) и профилем (Profil).**

### 9.2.2 Время ответа (Response Time)

*Response Time* - это время в миллисекундах (мс), которое проходит, пока отправитель сообщения не получит подтверждение приема от получателя.

Для параметрирования с применением профиля safe**ethernet** должно быть задано *Response Time* (время ответа), ожидаемое ввиду физических данных маршрута.

Заданное время ответа *(Response Time)* влияет на конфигурацию всех параметров соединения safe**ethernet**, время ответа рассчитывается следующим образом:

**Response Time ≤ Receive Timeout / n**

**n = 2, 3, 4, 5, 6, 7, 8.....**

Соотношение времени ожидания приема *Receive Timeout* и времени ответа *ResponseTime* воздействует на способность к отказоустойчивости, например, при потере пакета (повтор потерянных пакетов данных) или задержках на тракте передачи.

В сети, в которой может произойти потеря пакета, должно быть выполнено следующее условие:

**Min. Response Time ≤ Receive Timeout/2 ≥ 2 * Delay + 2,5 * Max. Cyvcle Time**

Если это условие выполнено, то можно предотвратить потерю минимум одного пакета данных, не прерывая при этом соединение safe**ethernet**.

i Если это условие не выполнено, то доступность соединения safe**ethernet** гарантирована только при бесконфликтной и бесперебойной работе сети. Однако это не влияет на безопасность процессорного модуля!

i Необходимо убедиться, что система коммуникации содержит параметрированное время ответа!

Для случаев, когда это не может быть обеспечено, для контроля времени ответа имеется соответствующая системная переменная соединения. Если не только в редких отдельных случаях происходит превышение измеренного времени ответа более чем на половину Receive Timeout, необходимо увеличить параметрированное время ответа.

Время ожидания ответа следует согласовывать с новым параметрированным временем ответа.

**ПРИМЕЧАНИЯ**

**На следующих примерах формулы для расчета максимального времени реакции в случае соединения с системами управления HIMatrix действительны только в том случае, если на них настроено безопасное время = 2 * время сторожевого устройства.**

### 9.2.3 Максимальное время цикла системы управления HIMatrix

Для определения максимального времени цикла для системы управления HIMatrix компания HIMA рекомендует следующий порядок действий:

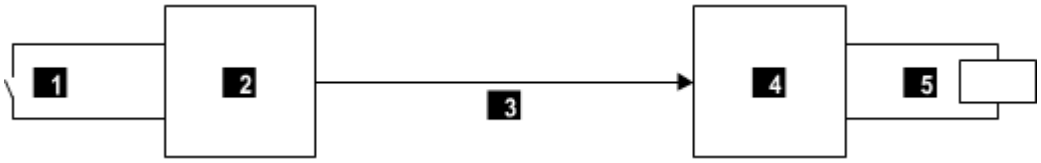
**Определение максимального времени цикла системы управления HIMatrix**

1. Эксплуатировать систему с полной нагрузкой. Все коммуникационные соединения работают как через safeethernet, так и через стандартные протоколы. Чаще считывать время цикла в Control Panel и отмечать максимальное время цикла.
2. Повторить шаг 1 для партнера коммуникации (вторая система управления HIMatrix).
3. Большее из обоих определенных максимальных значений времени цикла является искомым максимальным временем цикла.

Максимальное время цикла определено и входит в дальнейшие расчеты.

### 9.2.4 Расчет максимального времени реакции

Расчет максимального времени реакции $T_R$ (*Worst Case*) от смены входа PES 1 до реакции выхода PES 2 может выполняться следующим образом:




1 Вход
2 Система управления HIMatrix PES 1
3 Безопасный протокол
4 Система управления HIMatrix PES 2
5 Выход

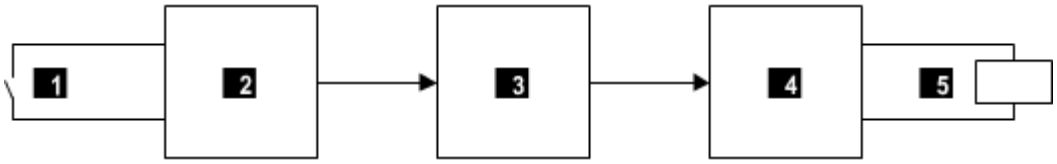
Рис. 4: Время реакции при соединении двух систем управления HIMatrix

$$T_R = t_1 + t_2 + t_3$$

$T_R$ Максимальное время реакции (Worst Case Reaction Time)
$t_1$ 2 * Время сторожевого устройства системы управления HIMatrix 1
$t_2$ Receive Timeout
$t_3$ 2 * Время сторожевого устройства системы управления HIMatrix 2
Максимальное время реакции зависит от процесса и должно быть согласовано с приемочным контрольным отделом.

### 9.2.5 Расчет макс. времени реакции с двумя устройствами удаленного ввода/вывода

Максимальное время реакции $T_R$ от смены входа первого PES HIMatrix или устройства удаленного ввода/вывода (например, F3 DIO 20/8 01) до реакции выхода второго PES HIMatrix или устройства удаленного ввода/вывода может рассчитываться следующим образом:




1 Вход
2 Remote I/O 1
3 Система управления HIMatrix
4 Remote I/O 2
5 Выход

Рис. 5: Время реакции с устройством удаленного ввода/вывода

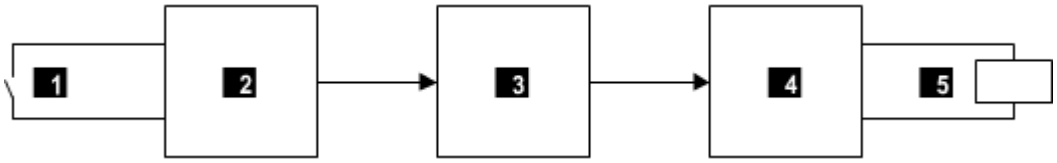
$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

$T_R$ Максимальное время реакции (Worst Case Reaction Time)
$t_1$ 2 * Время сторожевого устройства удаленного устройства ввода/вывода 1
$t_2$ Receive Timeout$_1$
$t_3$ 2 * Время сторожевого устройства системы управления HIMatrix
$t_4$ Receive Timeout$_2$
$t_5$ 2 * Время сторожевого устройства удаленного устройства ввода/вывода 2

Примечание: оба устройства удаленного ввода/вывода 1 и 2 могут быть идентичными. Значения времени действительны также в том случае, если вместо устройства удаленного ввода/вывода используется система управления HIMatrix.

### 9.2.6 Расчет максимального времени реакции двух HIMatrix и одной системы управления HIMax

Максимальное время реакции $T_R$ от смены входа первого PES HIMatrix до реакции выхода второго PES HIMatrix может рассчитываться следующим образом:




1 Вход
2 Система управления HIMatrix 1
3 Система управления HIMax
4 Система управления HIMatrix 2
5 Выход

Рис. 6: Время реакции с двумя системами управления HIMatrix и одной системой управления HIMax

$$T_R = t_1 + t_2 + t_3 + t_4 + t_5$$

$T_R$ Максимальное время реакции (Worst Case Reaction Time)
$t_1$ 2 * Время сторожевого устройства системы управления HIMatrix 1
$t_2$ Receive $Timeout_1$
$t_3$ 2 * Время сторожевого устройства системы управления HIMatrix
$t_4$ Receive $Timeout_2$
$t_5$ 2 * Время сторожевого устройства системы управления HIMatrix 2

Примечание: обе системы управления HIMatrix 1 и 3 могут быть идентичными.

### 9.2.7 Понятия

| | |
|---|---|
| Receive Timeout | Время контроля в системе управления 1, в течение которого должен быть принят действительный ответ от системы управления 2. По истечении времени безопасная связь завершается. |
| Production Rate | Минимальный интервал между двумя передачами данных. |
| Watchdog Time | Максимально допустимая продолжительность цикла RUN системы управления |
| Worst Case Reaction Time | Максимальное время реакции для передачи изменения сигнала физического входа системы управления 1 до изменения физического выхода системы управления 2. |

### 9.2.8 Присвоение адресов safe**ethernet**

При присвоении сетевых адресов (IP-адресов) для safe**ethernet** следует учитывать следующие пункты:

- Адреса должны быть однозначными в используемой сети.
- При соединении safe**ethernet** с другой сетью (внутренняя сеть LAN и т. д.) следует обратить внимание на то, чтобы исключалась возможность сбоев. Примеры возможных источников сбоев:
  - Выполняющаяся там передача данных.
  - Соединение с другими сетями (напр., Интернет).

В таких случаях принять соответствующие меры, например использовать сетевые коммутаторы Ethernet, сетевое устройство защиты, чтобы препятствовать возникновению сбоев.

# 10 Использование в приемно-контрольных приборах пожарной сигнализации

Системы HIMatrix могут использоваться в приемно-контрольных приборах пожарной сигнализации согласно DIN EN 54-2 и NFPA 72, если настроен контроль линии для входов и выходов.

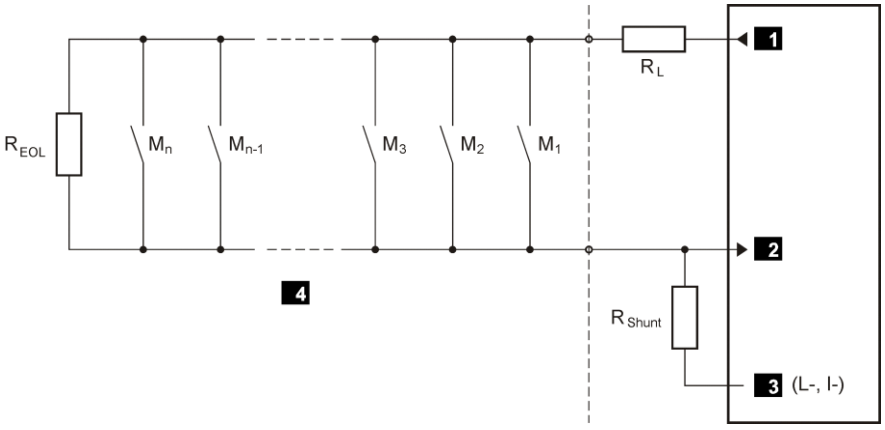
Для этого необходимо, чтобы прикладная программа отвечала функциональным требованиям для приемно-контрольных приборов пожарной сигнализации согласно указанным стандартам.

Системы могут легко достигать требуемого DIN EN 54-2 максимального времени цикла для приемно-контрольных устройств пожарной сигнализации 10 секунд, поскольку время цикла в этих системах может измеряться в миллисекундах, при необходимости также достигается безопасное время в 1 секунду (время реакции при ошибке).

Согласно EN 54-2 приемно-контрольный прибор пожарной сигнализации должен перейти в состояние сообщения о неисправности в течение 100 секунд после поступления сообщения о неисправности в систему HIMatrix.

Подключение пожарного извещателя осуществляется по принципу рабочего тока с контролем линии на короткое замыкание и обрыв. Для этого нужно использовать следующие устройства и модули:

- цифровые и аналоговые входы системы управления F35
- аналоговые входы устройства удаленного ввода/вывода F3 AIO 8/4 01
- цифровые входы и выходы устройств удаленного ввода/вывода F3 DIO 16/8 01 и F3 DIO 8/8 01
- модули ввода AI 8 01 и MI 24 01 системы управления F60




| | | | |
|---|---|---|---|
| 1 | Питание датчика | M | Пожарный извещатель |
| 2 | Аналоговый вход | $R_{EOL}$ | Нагрузочное сопротивление на последнем датчике контура |
| 3 | Опорный полюс | $R_L$ | Ограничение максимального тока контура |
| 4 | Сигнальный контур | $R_{шунт}$ | измерительное сопротивление |

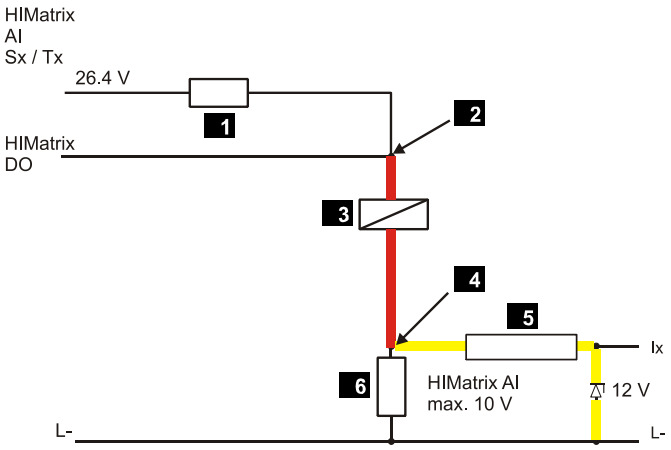
Рис. 7: Подключение пожарных извещателей

Для применения необходимо рассчитать сопротивление $R_{EOL}$, $R_L$ и $R_{шунт}$ в зависимости от используемых датчиков и числа датчиков в каждом сигнальном контуре. Необходимые для этого данные указаны в соответствующем техническом паспорте изготовителя датчика.

Выходы сигнала тревоги для управления лампами, сиренами, акустическими сигналами и т. д. работают по принципу рабочего тока. Выходы необходимо проверять на обрыв линии и замыкание. Это можно осуществить посредством возврата выходных сигналов непосредственно с исполнительного элемента на входы.

Ток в цепи исполнительного элемента можно контролировать при помощи аналогового входа с подходящим шунтом. Последовательное соединение стабилитрона и добавочного сопротивления защищает вход от перенапряжения в случае короткого замыкания линии.

Для однозначного распознавания обрыва линии (при отключенных выходах DO) дополнительно к аналоговым входам необходима линия питания трансмиттера (см. чертеж ниже):




1 Добавочное сопротивление
2 Клемма подключения поля
3 Исполнительный элемент
4 Клемма подключения поля
5 Добавочное сопротивление диодов
6 Шунт
Диапазон контроля обрыва/короткого замыкания цепи
Схема защиты при замыкании линии

Рис. 8: Пример контроля обрыва и замыкания линии для цифровых выходов (цепь исполнительного элемента)

Пример параметрирования контроля замыкания линии с дополнительным контролем обрыва линии исполнительных элементов при помощи аналоговых входов приводится в руководства HIMatrix F35 (HIMatrix HI 800 149 E).

Управление системами визуализации, панелями световых индикаторов, светодиодными индикаторами, алфавитно-цифровыми дисплеями, акустическими сигналами тревоги и т. д. может быть реализовано с помощью соответствующим образом подготовленной прикладной программы.

Передача сообщений о неисправности через каналы ввода и вывода или на устройства передачи сообщений о неисправности должна осуществляться по принципу тока покоя.

Передача сообщений о пожаре от системы HIMatrix сторонней системе может быть реализована с помощью имеющегося стандарта связи Ethernet (OPC). О сбое связи необходимо сообщить.

Системы HIMatrix, используемые в качестве приемно-контрольных приборов пожарной сигнализации, должны иметь избыточный источник питания. Примите меры против выхода из строя энергоснабжения, например используйте сирену на батарейках. Переключение между электроснабжением от сети и запасным источником питания должно гарантировать бесперебойную эксплуатацию. Допускаются посадки напряжения продолжительностью до 10 мс.

При сбоях системы операционная система описывает системные сигналы/переменные, определенные в прикладной программе. Это позволяет программировать сигнализацию неисправностей на распознаваемые системой ошибки. В случае сбоя система HIMatrix отключает безопасные входы и выходы, что приводит к следующему:

- Обработка низкого уровня сигнала во всех каналах дефектных входов.
- Отключение всех каналов дефектных выходов.

# 11 Использование в качестве предохранительного, контрольного и регулирующего приспособления с сигнализатором газоопасности

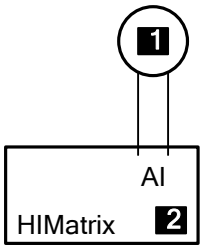
Устройства HIMatrix предназначены для надлежащего применения в промышленных приложениях с опасными средами до зоны 2 (газ, пар, туман). HIMatrix F35, F35 03 и F3 AIO 8/4 01 испытаны как устройства сертифицированной системы безопасности HIMatrix для использования в качестве предохранительного, контрольного и регулирующего приспособления с сигнализатором газоопасности. Имеется сертификат Ec на типовой образец на основе ATEX.

Приложение следует создавать и проверять согласно требованиям соответствующих стандартов по взрывозащите.

IEC / EN 60079-0
IEC / EN 60079-29-1

К устройствам HIMatrix подключаются испытанные и сертифицированные датчики для измерения расхода газа. При этом следует учитывать заданные параметры изготовителя.

При использовании в зоне 2 HIMatrix и датчик соединяются непосредственно друг с другом, см. Рис. 9:

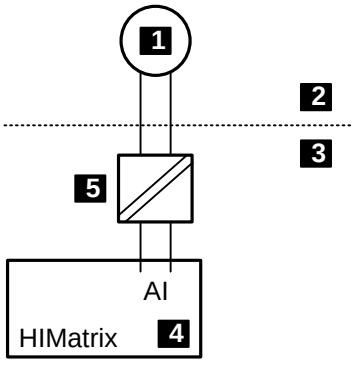



**1** Датчик 4…20 мА

**2** F35, F35 03 или F3 AIO 4/8 01

Рис. 9: Использование в зоне 2

Рис. 10 показывает использование в зоне 1. HIMatrix находится в зоне 2 и соединяется с помощью подходящего разделительного усилителя с датчиком в зоне 1.




**1** Датчик 4…20 мА

**2** зона класса 1

**3** зона класса 2

**4** F35, F35 03 или F3 AIO 4/8 01

**5** Разделительный усилитель, например H 6200A

Рис. 10: Использование в зоне 1

Прикладная программа может быть создана с помощью SILworX или ELOP II Factory (F35 03: только SILworX). При этом при параметрировании порогов необходимо соблюдать требования, предъявляемые изготовителем датчиков и стандартами.

Функция обеспечения безопасности HIMatrix с подключенными датчиками — контроль соответствующих горючих газов. Безопасные контрольные, регулирующие и предупредительные функции необходимо программировать в приложении. Приложение следует тестировать перед началом безопасной эксплуатации.

# Приложение

## Повышение уровня совокупной безопасности датчиков и исполнительных элементов

Безопасные системы управления HIMatrix используются для безопасного применения до уровня совокупной безопасности 3 (SIL 3). Одним из условий этого является то, что даже использованные датчики и исполнительные элементы (сигнальные датчики и актуаторы) выполняют требования уровня совокупной безопасности.

Может произойти, что датчики или исполнительные элементы недоступны для поставленных для применения требований, например, величина процесса, диапазон значений, уровень совокупной безопасности. В этом случае требуемое значение уровня совокупной безопасности достигается следующим образом:

- Для входов: использовать доступные датчики, которые удовлетворяют требованиям вне уровня совокупной безопасности. Использовать такое их количество, чтобы комбинация обеспечивала входной сигнал с требуемым уровнем совокупной безопасности.
- Для выходов: использовать доступные исполнительные устройства, которые удовлетворяют требованиям вне уровня совокупной безопасности. Использовать такое их количество, чтобы комбинация оказывала воздействие на процесс с требуемым уровнем совокупной безопасности.

**Для входов** так объединять значения отдельных датчиков и их информацию по состоянию в одной части прикладной программы, чтобы результат такой комбинации содержал глобальную переменную, которая имеет необходимый уровень совокупной безопасности.

**Для выходов** распределить значение глобальной переменной на несколько выходов так, чтобы в случае сбоя процесс принял безопасное состояние. Для этого у комбинации исполнительных элементов должна быть возможность соответствующего воздействия на процесс (пример: последовательное или параллельное подключение клапанов).

Для входов, как и для выходов взаимодействие нескольких датчиков/исполнительных элементов для такой же величины процесса следует планировать так, чтобы в процессе достигалась максимальная безопасность. Для расчета совокупного уровня безопасности следует использовать инструмент расчета.

i Описанное здесь использование нескольких датчиков/исполнительных элементов для ввода/вывода одного сигнала служит для повышения уровня совокупной безопасности, и его не разрешается изменять посредством применения избыточных входов/выходов для повышения готовности!

Указания по достижению необходимого уровня совокупной безопасности для датчиков и исполнительных элементов, например, в IEC 61511-1, раздел 11.4.

## Глоссарий

| Обозначение | Описание |
|---|---|
| AI | Analog input, аналоговый вход |
| ARP | Address resolution protocol, сетевой протокол для присвоения сетевых адресов аппаратным адресам |
| COM | Коммуникационный модуль |
| CRC | Cyclic redundancy check, контрольная сумма |
| DI | Digital input, цифровой вход |
| DO | Digital output, цифровой выход |
| ELOP II Factory | Инструмент программирования для систем HIMatrix |
| EN | Европейские нормы |
| ESD | Electrostatic discharge, электростатическая разгрузка |
| FB | Fieldbus, полевая шина |
| FBD | Function block diagrams, язык функциональных модулей |
| FTA | Field Termination Assembly |
| FTT | Fault tolerance time, время допустимой погрешности |
| ICMP | Internet control message protocol, сетевой протокол для сообщений о статусе и неисправностях |
| ID стойки | Идентификация основного носителя (номер) |
| IEC | Международные нормы по электротехнике |
| PADT | Programming and debugging tool, инструмент программирования и отладки (согласно IEC 61131-3), ПК с SILworX или ELOP II Factory |
| PE | Protective earth, защитное заземление |
| PFD | Probability of failure on demand, вероятность индикации ошибки при требовании обеспечения безопасности |
| PFH | Probability of failure per hour, вероятность опасного отказа в работе за час |
| R | Read: системная переменная/сигнал посылает значение, например, в пользовательскую программу |
| R/W | Read/Write, чтение/запись (заголовок столбца для типа системной переменной/сигнала) |
| SB | Модуль системной шины |
| SFF | Safe failure fraction, доля безопасных сбоев |
| SIL | Safety integrity level, уровень совокупной безопасности (согл. IEC 61508) |
| SILworX | Инструмент программирования для систем HIMatrix |
| SNTP | Simple network time protocol, простой сетевой протокол времени (RFC 1769) |
| SRS | System.Rack.Slot: адресация модуля |
| SW | Software, программное обеспечение |
| TMO | Timeout, время ожидания |
| W | Write: системная переменная/сигнал получает значение, например, от прикладной программы |
| Watchdog (WD) | Контроль времени для модулей или программ. При превышении показателя контрольного времени модуль или программа выполняют контрольную остановку. |
| WDT | Watchdog time, время сторожевого устройства |
| Адрес MAC | Адрес аппаратного обеспечения сетевого подключения (media access control) |
| без обратного воздействия на источник | Предположим, к одному и тому же источнику (например, трансмиттеру) подключены два входных контура. В этом случае входной контур обозначается как контур *без обратного воздействия на источник*, если он не искажает сигналы другого входного контура. |
| БСНН | Safety extra low voltage, защитное пониженное напряжение |
| ЗСНН | Protective extra low voltage, пониженное напряжение с безопасным размыканием |
| ПЭС | Programmable electronic system, программируемая электронная система |
| ЭМС | Electromagnetic compatibility, электромагнитная совместимость |

## Перечень изображений


| | | |
|---|---|---|
| Рис. 1: | Изображение блоков функций на примере ЦПУ 01 системы управления F60 | 25 |
| Рис. 2: | Управление линией | 30 |
| Рис. 3: | Тактовые сигналы T1, T2 | 31 |
| Рис. 4: | Время реакции при соединении двух систем управления HIMatrix | 64 |
| Рис. 5: | Время реакции с устройством удаленного ввода/вывода | 64 |
| Рис. 6: | Время реакции с двумя системами управления HIMatrix и одной системой управления HIMax | 65 |
| Рис. 7: | Подключение пожарных извещателей | 66 |
| Рис. 8: | Пример контроля обрыва и замыкания линии для цифровых выходов (цепь исполнительного элемента) | 67 |
| Рис. 9: | Использование в зоне 2 | 68 |
| Рис. 10: | Использование в зоне 1 | 68 |

## Перечень таблиц


Таблица 1: Варианты системы HIMatrix 8
Таблица 2: Условия окружающей среды 12
Таблица 3: Документация по системе HIMatrix 13
Таблица 4: Диапазон значений безопасного времени 16
Таблица 5: Диапазон значений времени сторожевого устройства 17
Таблица 6: Нормы для ЭМС, климатических и экологических требований 22
Таблица 7: Общие условия 23
Таблица 8: Климатические условия 23
Таблица 9: Механические испытания 23
Таблица 10: Испытания на помехоустойчивость 24
Таблица 11: Испытания на помехоэмиссию 24
Таблица 12: Дополнительная проверка характеристик подачи постоянного напряжения 24
Таблица 13: Обзор входов системы HIMatrix 28
Таблица 14: Значение безопасных аналоговых входов 31
Таблица 15: Аналоговые входы системы управления F35 31
Таблица 16: Аналоговые входы устройства удаленного ввода/вывода F3 AIO 8/4 01 32
Таблица 17: Аналоговые входы системы управления F60 32
Таблица 18: Конфигурация неиспользуемых входов 33
Таблица 19: Коды ошибок для входов счетчика 34
Таблица 20: Обзор выходов системы HIMatrix 35
Таблица 21: Системные параметры ресурса для версии CPU OS V7 и выше 46
Таблица 22: Воздействие режима заданного времени цикла 47
Таблица 23: Системные переменные аппаратного обеспечения для версии CPU OS V7 и выше 48
Таблица 24: Системные параметры ресурса для версии ниже CPU OS V7 49
Таблица 25: Длина имен переменных 53
Таблица 26: Системная переменная для блокировки и деблокировки ПЭС 54
Таблица 27: Число прикладных программ в PES 56
Таблица 28: Параметры, изменяемые в режиме онлайн, в зависимости от размещения аппаратного обеспечения и версии операционной системы 58

## Индекс

Fault tolerance time, время допустимой погрешности ... 16
Multitasking (многозадачность) ... 59
Безопасное время ... 16
Блокировка системы управления для версий ниже CPU OS V7 ... 55
Время сторожевого устройства ... 17
  прикладная программа ... 17
Деблокировка системы управления для версий ниже CPU OS V7 ... 55
Повторная проверка ... 17
Приведение системы управления в состояние возможности блокировки для версий от V7 и выше ... 54
Принцип рабочего тока ... 11
Принцип тока покоя ... 11
Реакции на ошибку
  аналоговые входы ... 33
  аналоговые выходы ... 39, 40
  цифровые входы ... 29
  цифровые выходы ... 36
Реакция на ошибку
  2-полюсные цифровые выходы ... 38
  входы счетчика ... 34
  релейные выходы ... 38
Сигнализатор газоопасности ... 68
Тест функциональности системы управления ... 42
Условия использования
  защита от воздействия электростатического разряда ... 12
Условия испытаний ... 22
  механические ... 23
  ЭМС ... 24
Условия испытания
  климатические ... 23
Условия проверки
  электропитание ... 24


HIMA Paul Hildebrandt GmbH
Postfach 1261
D-68777 Brühl
Тел.: +49-6202-709-0
Факс: +49-6202-709-107
Эл. почта: info@hima.com · Веб-сайт: www.hima.com

(1538)