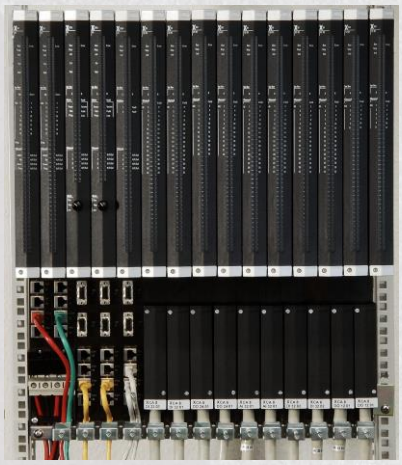


HIMax®

руководство по безопасности

SAFETY
NONSTOP

HIMA

БЕЗОПАСНОСТЬ

8

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

HIMax®, HIMatrix®, SILworX®, XMR® и FlexSILon® являются зарегистрированными торговыми марками компании HIMA Paul Hildebrandt GmbH

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, пожалуйста, непосредственно в компанию HIMA. Компания HIMA будет благодарна за отзывы и пожелания, например, в отношении информации, которая должна быть включена дополнительно в руководство.

Право на внесение технических изменений сохраняется. Компания HIMA оставляет за собой также право обновлять написанный материал 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 801 002 D, Rev. 6.00 (1408)	Перевод на русский язык с немецкого оригинала

Содержание

1 Руководство по безопасности

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

Чтобы обеспечить безопасность установки, ввода в эксплуатацию, использования и технического обслуживания автоматизированных систем HIMax, 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 HIMax 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 HIMax. Более подробная информация изложена в соответствующих руководствах.

Настоящее руководство по функциональной безопасности является «оригинальным руководством» в понимании Директивы по машинам и механизмам (Директива 2006/42/EC).

Исходная техническая документация для системы HIMA составлена на немецком языке. Преимущественной силой обладают положения немецкоязычной документации.

1.1 Действительность и актуальность

Версия 6.0	Данная версия применима к системе HIMax и SILworX версии 6 и выше.

Действительным является соответственно последнее издание руководства по функциональной безопасности с самым высоким номером редакции. Последняя редакция представлена на веб-сайте *www.hima.com* или на актуальном DVD компании HIMA.

При использовании более ранних версий HIMax и SILworX следует соблюдать требования соответствующих предыдущих редакций руководства.

1.2 Задачи руководства

Данное руководство содержит информацию по использованию безопасных устройств автоматизации HIMax по назначению. Оно представляет собой введение в концепцию безопасности системы HIMax и должно повысить осведомленность читателя в вопросах безопасности.

Руководство по безопасности основывается на содержании сертификата и отчета об испытаниях к сертификату.

1.3 Целевая аудитория

Данное руководство предназначено для планировщиков, проектировщиков и программистов автоматических установок, а также специалистов, выполняющих ввод в эксплуатацию, эксплуатацию и техническое обслуживание устройств и систем. Требуется наличие специальных знаний в области автоматизированных систем обеспечения безопасности.

1.4 Оформление текста

Для лучшей разборчивости и четкости в данном документе используются следующие способы выделения и написания текста:

Полужирный шрифт	Выделение важных частей текста Маркировка кнопок управления, пунктов меню и вкладок в SILworX, по которым можно щелкнуть мышкой
Курсив	Системные параметры и переменные величины
`Курьер / Courier`	Слова, вводимые пользователем
RUN	Обозначение режима работы заглавными буквами
Гл. 1.2.3	Ссылки могут не иметь особой маркировки. При наведении на них указателя мышки его форма меняется. При щелчке по ссылке происходит переход к соответствующему месту в документе.

Указания по безопасности и применению выделены особым образом.

1.4.1 Указания по безопасности

Указания по безопасности представлены в документе следующим образом.
Эти указания должны обязательно соблюдаться, чтобы максимально уменьшить степень риска. Они имеют следующую структуру:

- Сигнальные слова: 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

УКАЗАНИЕ

Вид и источник ущерба!

Избежание ущерба

1.4.2 Указания по применению

Дополнительная информация представлена следующим образом:

i В этом месте расположена дополнительная информация.

Полезные советы и рекомендации представлены в следующей форме:

РЕКОМЕНДАЦИЯ В этом месте расположен текст рекомендации.

2 Указания по использованию систем HIMax

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 по технике безопасности.

2.1 Применение по назначению

В данной главе описываются условия использования систем HIMax.

2.1.1 Область применения

Системы управления HIMax предназначены для обеспечения безопасности и имеют соответствующие сертификаты для использования в системах управления процессом, системах защиты, системах управления работой котла и системах контрольных механизмов.

Режим работы с резервированием модулей HIMax допускает одновременно режим работы без резервирования других модулей.

2.1.1.1 Применение по принципу 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 Использование по принципу рабочего тока

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

Система, работающая по принципу рабочего тока, может запускать исполнительное устройство, чтобы выполнять функции 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

Все системы HIMax с аналоговыми входами прошли проверку для использования в установках пожарной сигнализации и имеют сертификаты согласно DIN EN 54-2 и NFPA 72.

2.1.2 Условия окружающей среды

Условия	
Класс защиты (Protection Class)	Класс защиты III (Protection Class III) в соответствии с IEC/EN61131-2
Температура окружающей среды	0...+60 °C
Температура хранения	-40...+85 °C
Степень загрязнения	Степень загрязнения II (Pollution Degree II) в соответствии с IEC/EN 61131-2
Высота установки	< 2000 м
Корпус	Стандарт: IP20
Питающее напряжение	24 В пост. тока

Таблица 1: Условия окружающей среды

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

2.2 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 HIMax в автоматических установках и комплексах.

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

2.2.1 Подключение участников коммуникации

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

2.2.2 Использование безопасной связи

При использовании безопасной связи между различными устройствами необходимо следить за тем, чтобы общее время реакции системы не превышало время отказоустойчивости. Необходимо использовать основы расчета, приведенные в главе 11.

2.3 Меры по защите от электростатического разряда

Изменение и расширение системы или замену модуля может выполнять только персонал, ознакомленный с защитными мерами от воздействия электростатического разряда.

УКАЗАНИЕ

Электростатические разряды могут повредить встроенные в системы управления электронные конструктивные элементы!

- **Выполнять работу на рабочем месте с антистатической защитой и носить ленточный заземлитель.**
- **Если модули не используются, из следует хранить с обеспечением электростатической защиты, например, в упаковке.**

Изменения или расширения в проводке системы может выполнять только персонал, ознакомленный с мерами защиты от электростатического разряда.

2.4 Дополнительная документация по системе

Для проектирования систем HIMax, кроме того, предоставляется следующая документация:

Название	Содержание	№ документа
HIMax System Manual	Описание аппаратного обеспечения модульной системы	HI 801 060 RU
Сертификат	Результаты проверки	
Список версий	Допущенные TÜV версии операционной системы	
Руководства по компонентам	Описание отдельных компонентов	
Communication Manual	safe**ethernet** и стандартные протоколы	HI 801 062 RU
SILworX First Steps Manual	Использование SILworX при проектировании, вводе в эксплуатацию, проверках и эксплуатации	HI 801 301 RU
SILworX Online Help	Использование SILworX	

Таблица 2: Обзор документации по системе

Документы представлены в виде файлов в формате PDF на веб-сайте `www.hima.com`.

3 Концепция безопасности для применения ПЭС

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

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

3.1 Безопасность и готовность

Системы HIMax не являются источником непосредственной опасности.

⚠ ПРЕДУПРЕЖДЕНИЕ

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

Проверить подключения перед вводом в эксплуатацию и испытать установку в целом на соответствие указанным требованиям безопасности!

HIMA настоятельно рекомендует проводить замену вышедших из строя модулей в кратчайшие сроки.

Чтобы начать использовать запасной модуль, установленный вместо модуля, вышедшего из строя, не требуется какое-либо предварительное обслуживание. Он берет на себя выполнение текущей функции вышедшего из строя модуля, если принадлежит к тому же типу или к типу, допущенному для замены.

3.1.1 Расчеты PFD, PFH и SFF

Для систем HIMax были выполнены расчеты PFD, PFH и SFF согласно IEC 61508.

Значения для PFD, PFH и SFF сообщаются фирмой HIMA по запросу.

Интервал повторной проверки для систем HIMax составляет 10 лет (проверочный тест в режиме оффлайн, см. IEC 61508-4, раздел 3.8.5).

Функции безопасности, состоящие из безопасного контура (вход, обрабатывающее устройство, выход и безопасная связь между системами HIMA), во всех комбинациях выполняют описанные выше требования.

3.1.2 Самодиагностика и диагностика ошибок

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

- Процессоры
- Зоны памяти (ОЗУ, энергонезависимая память)
- Сторожевое устройство
- Соединения между модулями
- Отдельные каналы для модулей ввода/вывода

Если при выполнении данного теста обнаруживаются ошибки, то неисправный модуль или неисправный канал (в случае модулей ввода/вывода) отключается. Если уже при запуске во время теста модуля обнаруживается ошибка модуля, то он не включается.

В системе без избыточности это означает, что может произойти отключение подфункций или всей ПЭС. В системе с избыточностью в случае обнаружения ошибки выполнение текущей функции берет на себя избыточный модуль или канал.

Все модули HIMax соответственно оснащены собственными светодиодами для индикации обнаруженных ошибок. Это позволяет быстро диагностицировать ошибку в модуле или внешней проводке при появлении сообщения об ошибке.

Кроме того, прикладная программа может анализировать различные системные переменные, которые отображают состояние модулей.

Обширная диагностическая запись поведения системы и распознанных ошибок сохраняется в памяти диагностики процессорного модуля и других модулей. Запись можно считать после системного сбоя через PADT.

Детали анализа диагностических сообщений также см. в руководстве по системе (HIMA System Manual HI 801 060 RU), глава *Диагностика*.

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

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.

3.1.4 Избыточность

Для повышения готовности допускается резервное использование всех компонентов, содержащих активные конструктивные элементы, а также их замена во время работы.

Резервирование не снижает уровень безопасности. Уровень совокупной безопасности 3 обеспечен и для резервных компонентов системы.

3.1.5 Конструкция системы безопасности по принципу рабочего тока

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

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

3.1.5.1 Диагностирование неисправных компонентов

Процесс автоматической диагностики позволяет системе безопасности распознавать неисправное состояние модулей.

3.1.5.2 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:

- На входных и выходных модулях необходимо параметрировать резервные группы.
- Обеспечить контроль за замыканием и обрывом линий на входных и выходных модулях.
  Их необходимо параметрировать.
- Обеспечить контроль функций исполнительных элементов можно с использованием позиционной обратной связи.

3.1.5.3 Резервирование компонентов

Может возникнуть необходимость создать резервную структуру компонентов, см. руководство по системе (HIMax System Manual HI 801 060 RU):

- Электропитание управления

- Модули HIMax
- Датчики и исполнительные элементы

В случае утраты резервирования система управления подлежит ремонту в кратчайшие сроки.

Резервная структура модулей системы безопасности не требуется, если нужный уровень безопасности при выходе системы безопасности из строя обеспечивается иными способами, например организационными мерами.

3.2 Время, важное для безопасности

Показатели времени, важные для безопасности:

- Безопасное время процесса
- Watchdog Time
- Безопасное время
- Время реакции

3.2.1 Безопасное время процесса

Безопасное время процесса является характеристикой процесса и обозначает тот промежуток времени, в течение которого могут накапливаться ошибочные сигналы процесса; состояние системы при этом может оставаться неопасным.

Безопасное реагирование ПЭС HIMAX, включая все задержки датчиков, исполнительных устройств, входных и выходных модулей, должно укладываться во временные рамки максимально допустимого безопасного времени процесса.

3.2.2 Время сторожевого устройства ресурса

Время сторожевого устройства задается как время в SILworX в диалоге для настройки характеристик ресурса. Это максимально допустимая продолжительность цикла RUN (время цикла). Если время цикла превышает заданное время сторожевого устройства, процессорный модуль переходит в состояние ERROR STOP.

При измерении времени сторожевого устройства следует учитывать следующие факторы:

- Время, необходимое для приложения, напр., продолжительность цикла прикладной программы.
- Время, необходимое для обмена данными процесса
- Время, необходимое для синхронизации зарезервированных процессорных модулей.
- Время системы, необходимое для выполнения перезагрузки.

Диапазон настройки времени сторожевого устройства ресурса составляет от 6 мс до 7 500 мс макс.

Настройка по умолчанию составляет 200 мс.

Для времени сторожевого устройства должно действовать соотношение: **время сторожевого устройства ≤ ½ * безопасное время**

3.2.2.1 Определение времени сторожевого устройства

Для достаточно высокого уровня готовности HIMA настоятельно рекомендует следующую установку:

2 * Время сторожевого устройства + Макс. время цикла ЦПУ + 2 * Время цикла ввода/вывода ≤ Безопасное время

Максимальное время цикла в конкретном приложении измеряется заменой зарезервированного процессорного модуля. Полученное максимальное время цикла подставляется в приведенную выше формулу.

Если невозможно привести достоверное значение максимального времени цикла ЦПУ, то сторожевое устройство настраивается по следующей формуле:

3 * Время сторожевого устройства + Макс. время цикла ЦПУ + 2 * Время цикла ввода/вывода ≤ Безопасное время

Время цикла ввода/вывода составляет 2 мс.

3.2.2.2 Точное определение времени сторожевого устройства

При работе с критическими по времени приложениями или с очень большими системами может возникнуть необходимость в точном определении времени сторожевого устройства.

Точное определение времени сторожевого устройства для проекта проводится тестированием на всей системе. При этом все проектированные модули должны быть вставлены. Система работает в режиме RUN при полной нагрузке.

Все коммуникационные соединения работают (safe**ethernet** и стандартные протоколы).

Определение времени сторожевого устройства

1. Настроить на высокую отметку время сторожевого устройства для испытания.
2. Эксплуатировать систему с полной нагрузкой. Все коммуникационные соединения работают как через safe**ethernet**, так и через стандартные протоколы. При этом нужно чаще считывать время цикла на панели управления и отмечать колебания или предельные нагрузки времени цикла.
3. Каждый процессорный модуль удалить по очереди и вновь установить на несущий каркас. Всякий раз перед удалением процессорного модуля дождаться синхронизации только что установленного модуля.

i Когда вы вставляете процессорный модуль, он автоматически синхронизируется с конфигурацией имеющихся процессорных модулей. Время, требуемое для синхронизации, продлевает цикл управления до максимального значения времени цикла.

Время синхронизации возрастает с количеством уже синхронизированных процессорных модулей.

Описание установки и демонтажа процессорного модуля см. в руководстве X-CPU 01, (HIMax X-CPU 01 Manual HI 801 064 RU).

4. Считывать в истории диагностики не синхронизированных процессорных модулей время синхронизации процессорных модулей с n по n + +1 при каждой синхронизации. Наибольший из этих показателей времени синхронизации используется для определения времени сторожевого устройства.
5. Время сторожевого устройства T_{WD} рассчитывается на основе следующих показателей:

   $T_{WD} = T_{Sync} + T_{Marg} + T_{Com} + T_{Config} + T_{Latency} + T_{Peak}$ где

   T_{Sync} Установленное время синхронизации процессорного модуля

   T_{Marg} Запас надежности 12 мс

   T_{Com} Установленный системный параметр *Max. Com.Time Slice ASYNC [ms]*

   T_{Config} Установленный системный параметр *Max. Duration of Configuration Connections [ms]*

   $T_{Latency}$ Установленный системный параметр *Maximum System Bus Latency [µs]* * 4

   T_{Peak} Наблюдаемые предельные нагрузки прикладных программ

Так определяется подходящее заданное значение для времени сторожевого устройства.

i Рассчитанного таким образом времени сторожевого устройства в некоторых случаях может оказаться мало для перезагрузки.

РЕКОМЕНДАЦИЯ Полученное время сторожевого устройства может использоваться как максимальное время цикла для параметрирования safe**ethernet,** см. руководство по модулю связи (Communication Manual HI 801 062 RU).

3.2.3 Время сторожевого устройства прикладной программы

Каждая прикладная программа имеет собственное сторожевое устройство и, следовательно, собственное время сторожевого устройства.

Время сторожевого устройства прикладной программы не задается непосредственно. HIMax вычисляет время сторожевого устройства прикладной программы, используя параметры *Watchdog Time [ms]* ресурса и *Maximum Number of CPU Cycles*. Подробнее см. в главах 11.2.3 и 11.2.11.

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

3.2.4 Безопасное время ресурса

Безопасное время ресурса представляет собой максимально допустимое время, в течение которого ресурс должен отреагировать на запрос. Запросы:

- Изменения входных сигналов процесса
- Возникновение ошибки ресурса

В рамках параметрируемого безопасного времени ресурса система HIMax реагирует на ошибки, которые могут привести к опасному рабочему состоянию. Заданные реакции системы на ошибки переводят неисправные элементы в безопасное состояние. Для этого должны выполняться следующие условия:

- Не происходит задержка входных сигналов в результате действий элементов задержки, настроенных во входных модулях (задержка включения, задержка выключения)
- Не происходит задержка внутри прикладной программы
- Прикладная программа реагирует в цикле ПЭС.
- Нет задержки выходных сигналов в результате действий элементов задержки, настроенных в выходных модулях (T_{on} задержка включения, T_{off} задержка выключения)

Необходимо учитывать следующие факторы, увеличивающие безопасное время ресурса:

- Физические задержки на входах и выходах, такие как время срабатывания реле
- Задержки выходных сигналов из-за подавления помех на выходе, см. главу 8.3.2

Для ресурсов HIMax безопасное время устанавливается в диапазоне 20...22 500 мс.

3.2.5 Безопасное время прикладной программы

Безопасное время прикладной программы не устанавливается вручную. Оно рассчитывается HIMax на основе параметра ресурса *Safety Time* и параметра *Maximum Number of Cycles*. Подробнее см. в главах 11.2.3 и 11.2.11.

3.2.6 Время реакции

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

Значение времени реакции не может быть выше, чем значение безопасного времени процесса.

3.3 Повторная проверка (Proof Test по IEC 61508)

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 с интервалом в 10 лет**.

Интервал этот нередко можно и продлить, если анализировать реализованные цепи безопасности на основе расчетов.

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 HIMax может подвергаться повторной проверке во время 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 HIMax. Если пользователь проверяет всю цепь безопасности из-за полевого устройства, то система управления HIMax автоматически включается в эту проверку. В этом случае для системы управления HIMax не требуется никаких дополнительных повторных проверок.

Если повторная проверка полевых устройств не включает в себя систему управления HIMax, то для обеспечения 3-го уровня совокупной безопасности ее следует проверять не реже чем один раз в 10 лет. Этого можно добиться, перезапустив систему управления HIMax.

3.4 Требования безопасности

При использовании безопасной ПЭС системы HIMax действуют следующие требования безопасности:

3.4.1 Проектирование аппаратного обеспечения

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

Требования, не зависящие от изделия

- Для обеспечения безопасной работы используйте только допущенные для этого безопасные модули аппаратного обеспечения и компоненты программного обеспечения. Допущенные модули и компоненты ПО перечислены в Version List of Modules and Firmware for HIMax Systems from HIMA Paul Hildebrandt GmbH. Соответственно текущие номера версий содержатся в списке версий, составляемом совместно с отделом контроля.
- Необходимо строго соблюдать указанные условия использования (см. главу *Условия окружающей среды*), касающиеся ЭМС, а также механических, химических и климатических воздействий.

Требования, зависящие от изделия

- К системе должны подключаться только те устройства, которые имеют безопасное разделение от сети.
- Необходимо соблюдать названные в руководстве по системе условия использования, в частности касающиеся питающего напряжения, вентиляции и т. д.
- Для обработки задач безопасности применяйте только безопасные модули.
- Для обеспечения электропитанием разрешается использовать только блоки питания в исполнениях для ЗСНН или БСНН. Подаваемое питающее напряжение и напряжение при сбое должно быть ≤ 35 В!

3.4.2 Программирование

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

Требования, не зависящие от изделия

- В приложениях, связанных с безопасностью, необходимо следить за правильным параметрированием имеющих значение для безопасности системных величин.
- Особое внимание следует уделить определению конфигурации системы, максимального времени цикла и безопасного времени.

3.4.3 Требования к использованию системы программирования

- Для программирования следует использовать инструмент SILworX.
- **Необходимо подтверждать, проверять и документировать правильность внедрения спецификации приложения. Следует провести полную проверку логической схемы путем отладки.**
- При изменении приложения проверьте элементы логической схемы, по крайней мере все те, что были затронуты изменением.
- Реакция системы на ошибку в безопасных модулях ввода и вывода должна определяться теми условиями, которые заданы в конфигурации прикладной программой и служат для обеспечения безопасности. Примеры:
  - Реакция прикладной программы на ошибку
  - Параметрирование безопасных начальных значений переменных

3.4.4 Коммуникация

- При настройке коммуникации между различными устройствами, связанной с обеспечением безопасности, необходимо следить за тем, чтобы общее время реакции системы не превышало безопасное время процесса. Расчеты должны проводиться на основе принципов, приведенных в главе 12.2.
- При передаче данных (связанных с безопасностью) необходимо соблюдать правила информационной безопасности.

  Передача данных, связанных с безопасностью, в сетях общего пользования (например, Интернет) разрешена только при соблюдении дополнительных мер безопасности, таких как использование VPN-канала и межсетевой экран.
- Если передача данных осуществляется по внутренним сетям организации/предприятия, то с помощью административных или технических мер нужно обеспечить достаточный уровень защиты от манипулирования (например, отделение части сети, связанной с безопасностью, от других сетей посредством межсетевого экрана).
- Не разрешается использовать стандартные протоколы для передачи данных, связанных с безопасностью.
- Ко всем интерфейсам связи можно подключать только такие устройства, которые обеспечивают безопасное электрическое разделение.

3.4.5 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.

При необходимости эксплуатирующая сторона по согласованию с органом технического надзора, ответственным за применение, должна определить административные меры для защиты системы от несанкционированного доступа.

3.4.6 Информационная безопасность систем HIMax

Установленное оборудование HIMax должно иметь защиту от источников опасности, типичных для сферы информационных технологий. К таким источникам опасности относятся:

- Потенциальные взломщики внутри клиентской системы и за ее пределами
- Эксплуатационные ошибки
- Ошибки программного обеспечения

Установленное оборудование HIMax состоит из следующих компонентов, подлежащих защите:

- ПЭС HIMax
- PADT
- OPC-сервер: X-OPC DA, X-OPC AE (опция)
- Коммуникационные соединения с внешними системами (опция)

Даже с настройками по умолчанию HIMax уже является системой, соответствующей требованиям информационной безопасности (безопасности информационных технологий). Процессорные модули X-CPU 01, X-CPU 31 и коммуникационный модуль X-COM 01 были удостоены сертификата Achilles Level I канадской компании Unternehmen wurldtech.

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

В результате тщательного проектирования должны выявляться необходимые мероприятия. После анализа рисков эти необходимые мероприятия необходимо провести. Например, к таким мероприятиям относятся:

- Целесообразная классификация групп пользователей
- Тщательно проработанные сетевые графики, которые обеспечивают постоянное разграничение между безопасными сетями и сетями общего пользования, а если необходимо, имеют один определенный переход (например, с помощью межсетевого экрана или зоны DMZ).
- Применение подходящих паролей, которые трудно разгадать

Рекомендуется регулярно проверять меры безопасности (например, ежегодно).

Надлежащее проведение необходимых для оборудования мероприятий находится в сфере ответственности пользователя!

Подробнее см. в руководстве (HIMA Cyber Security Manual HI 801 373 E).

3.5 Сертификация

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

TÜV Rheinland Industrie Service GmbH
Автоматизация, программное обеспечение и информационные технологии
Am Grauen Stein
51105 Köln

Сертификат и протокол испытаний
Безопасные устройства автоматизации HIMax

Предусмотренное применение: Safety Related Programmable Electronic System for process control,
Burner Management (BMS), emergency shut down and machinery, where the demand safe state is the de-energized state. Applications, where the demand state is the de-energized or energized state.
Applications, where the demand state is the de-energized or energized state.
(Безопасная программируемая электронная система для устройств управления процессом, управления работой котла (BMS), систем аварийного отключения и систем управления оборудованием, в которых принимаемым по требованию безопасным состоянием является обесточенное состояние.
Случаи применения, когда принимаемым по требованию безопасным состоянием является обесточенное состояние или состояние с подводом тока.)

Международные стандарты:		
EN / IEC 61508, Parts 1-7: 2000		SIL 3
EN / IEC 61511: 2004		SIL 3
EN / ISO 13849-1: 2008		Performance Level e
EN / IEC 62061: 2005	Включая Ber 1 и Ber 2: 2009	
EN 50156-1: 2006		
EN 12067-2: 2004		
EN 298: 2004	+ Ber 1: 2006	
EN 230: 2005		
NFPA 85: 2007		
NFPA 86: 2007		
EN / IEC 61131-2: 2007		
EN / IEC 61000-6-2: 2005		
EN 61000-6-4: 2007		
EN 54-2: 1997	/A1: 2007	
NFPA 72: 2002		

Глава "Условия использования" содержит подробный список всех проведенных испытаний по экологии и электромагнитной совместимости.

Все устройства имеют знак технического контроля CE.

Для программирования систем управления HIMax используется PADT, т. е. ПК с системой программирования **SILworX**.

Этот инструмент помогает пользователю создавать безопасные программы при помощи таких языков программирования, как язык диаграмм функциональных блоков (FBD) и язык последовательных функциональных схем (SFC), в соответствии с IEC 61131-3, а также управлять устройствами автоматизации. Подробную информацию вы найдете в онлайн-справке SILworX и в руководстве (SILworX First Steps Manual HI 801 301 RU).

3.5.1 Условия испытаний

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

Стандарт	Содержание
IEC/EN 61131-2	Программируемые логические контроллеры, часть 2 Требования к ресурсам и испытания
IEC/EN 61000-6-2	EMC, ЭМС Отраслевая норма, часть 6-2 Помехоустойчивость, промышленная сфера
IEC/EN 61000-6-4	Электромагнитная совместимость (ЭМС) Отраслевая норма, эмиссия помех, промышленная сфера

Таблица 3: Нормы ЭМС, климатические и экологические требования

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

Условия	Inhalt der Bedingung
Класс защиты (Protection Class)	Класс защиты III (Protection Class III) в соответствии с IEC/EN 61131-2
Степень загрязнения	Степень загрязнения II (Pollution Degree II) в соответствии с IEC/EN 61131-2
Высота установки	< 2000 м
Корпус	Стандарт: IP20/IP00 Если того требуют соответствующие стандарты применения (напр., EN 60204), устройство необходимо встраивать в корпус с необходимой степенью защиты (напр., IP54).

Таблица 4: Общие условия

3.5.1.1 Климатические условия

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

Стандарт	Климатические испытания
IEC/EN 61131-2	Рабочая температура: 0...+60 °C (Предельные значения при испытании: от -10 до +70 °C)
	Температура хранения: от -40...+85 °C
	Сухое тепло и холод; испытания на прочность: +70 °C/-40 °C, 16 ч, +85 °C, 1 ч электропитание не подключено
	Изменение температуры; испытание на прочность: Быстрое изменение температуры: -40 °C/+70 °C, электропитание не подключено
	Испытание на нечувствительность Медленное изменение температуры: -10 °C / +70 °C, электропитание подключено
	Циклы с влажным теплом; испытания на прочность: +25 °C / +55 °C, 95 % относительная влажность, электропитание не подключено
EN 54-2	Влажное тепло Относительная влажность 93 %, 40 °C, 4 рабочих дня Относительная влажность 93 %, 40 °C, 21 день, электропитание не подключено

Таблица 5: Климатические условия

3.5.1.2 Механические условия

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

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

Таблица 6: Механические испытания

3.5.1.3 Условия ЭМС

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

Стандарт на метод испытания	Испытания на помехоустойчивость	Критерий ФБ
IEC/EN 61000-4-2	Испытание на воздействие электростатических разрядов: 6 кВ контактный разряд, 8 кВ воздушный разряд	6 кВ, 8 кВ
IEC/EN 61000-4-3	Испытание RFI (10 В/м): 80 МГц…2 ГГц, 80% AM Испытание RFI (3 В/м): 2 МГц…3 ГГц, 80% AM Испытание RFI (20 В/м): 80 МГц…1 ГГц, 80% AM	- - 20 В/м
IEC/EN 61000-4-3	Импульсы 900 МГц	-
IEC/EN 61000-4-4	Испытание на устойчивость к наносекундным импульсным помехам: Питающее напряжение: 2 кВ и 4 кВ Сигнальные линии: 2 кВ	 4 кВ 2 кВ
IEC/EN 61000-4-5	Импульсное напряжение: Питающее напряжение: 2 кВ и 4 кВ Сигнальные линии: 2 kB CM, 1 kB DM при AC вход/выход	 2 кВ/1 кВ 2 кВ
IEC/EN 61000-4-6	Высокая частота, асимметрично: 10 В, 150 кГц…80 МГц, 80 % AM 20 В, ISM-частоты, 80 % AM	 10 В -
IEC/EN 61000-4-12	Испытание затухающими колебаниями: 2,5 кВ L-,L+ / PE 1 kV L+ / L -	 - -

Таблица 7: Испытания на помехоустойчивость

IEC/EN 61000-6-4	Испытания на помехоэмиссию
EN 55011 Класс A	Эмиссия помех: излуч., проводной

Таблица 8: Испытания на помехоэмиссию

3.5.1.4 Питающее напряжение

Наиболее важные испытания и предельные значения для подачи питающего напряжения на устройства перечислены в следующей таблице:

IEC/EN 61131-2	Дополнительная проверка характеристик подачи постоянного напряжения
	Подача напряжения альтернативно должна отвечать следующим стандартам: IEC/EN 61131-2 или БСНН (Safety Extra Low Voltage, SELV) или ЗСНН (Protective Extra Low Voltage, PELV)
	Защита устройств HIMax должна осуществляться в соответствии с данными, содержащимися в руководстве X-BASE PLATE (HIMax X-BASE PLATE 01 Manual HI 801 071 RU).
	Проверка диапазона напряжений: 24 В пост. тока, -20…+25% (19,2…30,0 В)
	Испытание на нечувствительность в случае краткого прерывания подачи электропитания от внешнего источника: пост. тока, PS 2: 2 мс
	Изменение полярности питающего напряжения: Указание в соответствующей главе руководства по системе или в таблице параметров для линии электропитания.
	Буферное время, испытание на прочность: Испытание B, 1000 ч

Таблица 9: Дополнительная проверка характеристик подачи постоянного напряжения

4 Процессорный модуль

Функция безопасности процессорного модуля состоит в выполнении прикладной программы двумя процессорами, которые непрерывно сравнивают свои данные. В случае ошибки сторожевое устройство переводит модуль в безопасное состояние и сигнализирует состояние ЦПУ.

Более подробную информацию о процессорных модулях см. в руководствах.

4.1 Самодиагностика

Далее перечислены наиболее важные программы самодиагностики безопасных процессорных модулей:

- Тестирование процессора
- Тестирование памяти
- Тестирование сравнивающего устройства
- Тест CRC для энергонезависимой памяти
- Тестирование сторожевого устройства

4.2 Реакции на ошибки в процессорном модуле

Сравнивающее устройство АО внутри процессорного модуля непрерывно сопоставляет данные системы микропроцессора 1 с данными системы микропроцессора 2. Если они не идентичны или тестовые программы находят ошибку в процессорном модуле, то процессорный модуль автоматически переходит в состояние ERROR STOP (останов из-за ошибки). Если время цикла превышает заданное время сторожевого устройства ресурса, процессорный модуль также переходит в состояние ERROR STOP (останов из-за ошибки).

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

Если автоматический перезапуск нежелателен, то параметр ресурса *Autostart* следует установить на OFF.

4.3 Замена процессорных модулей

Перед заменой процессорных модулей убедитесь, что такая замена не повлечет за собой остановку работающей системы HIMax.

Это в первую очередь относится к системам, функционирующим по принципу рабочего тока. Выход таких систем из строя приводит к потере функции безопасности.

Избыточные процессорные модули можно заменять во время работы, если имеется минимум еще один процессорный модуль, который обеспечивает безопасную работу при замене.

УКАЗАНИЕ

Возможно прерывание безопасной работы!

Работа системы управления может быть прервана в результате замены процессорного модуля, на котором горит или мигает светодиод Ess**.**

Не вынимать процессорные модули, на которых горит или мигает светодиод Ess**!**

Горящий или мигающий светодиод **Ess** указывает на то, что процессорный модуль необходим для функционирования системы.

Даже если светодиод не горит/мигает, следует с помощью SILworX проверить резервирование системы, частью которой является данный процессорный модуль. При этом также учитывать коммуникационные соединения, осуществляемые процессорным модулем.

Более подробную информацию о замене процессорных модулей вы найдете в руководствах (HIMax X-CPU 01 Manual HI 801 064 RU) и (HIMax X-CPU 31 Manual HI 801 432 RU), а также в руководстве по системе (HIMax System Manual HI 801 060 RU).

4.4 Процессорный модуль X-CPU 01

Процессорный модуль X-CPU 01 может применяться с резервированием до 4-кратного. Модуль может быть установлен в стойку 0 или 1, в слоты с 3...6.

4.5 Процессорный модуль X-CPU 31

Процессорный модуль X-CPU 31 совмещает функции процессорного модуля и модуля системной шины. Поэтому модуль можно устанавливать только в стойку 0, слот 1 или 2. В этом случае никакой другой процессорный модуль в стойке 0 или 1 в слотах с 3...6 не устанавливается!

5 Модуль системной шины

Модуль системной шины управляет одной из двух безопасных системных шин. Обе системные шины работают с избыточностью по отношению друг к другу. Каждая системная шина соединяет все модули и несущие каркасы между собой. Через системные шины безопасные данные передаются с помощью безопасного протокола.

При пониженной готовности систему HIMax только **с одним процессорным модулем** можно эксплуатировать только с одной системной шиной.

Вместо модулей системной шины на стойке 0 можно также устанавливать и процессорные модули типа X-CPU 31. К этим модулям применимы положения настоящей главы. Для процессорных модулей X-CPU 31 требуется специальная плата сопряжения двойной ширины.

5.1 ID стойки

ID стойки идентифицирует несущий каркас в рамках одного ресурса и для каждого несущего каркаса должен быть однозначным.

ID стойки является **параметром безопасности** для адресации отдельных несущих каркасов и находящихся на них модулей!

ID стойки сохраняется в плате сопряжения модуля системной шины. Если необходимо изменить ID стойки, напр., при сборке новой системы HIMax, следует придерживаться порядка действий, описанного в руководстве по системе (HIMax System Manual HI 801 060 RUN).

Установка ID стойки описана в руководстве по системе (HIMax System Manual HI 801 060 RU) и в руководстве Первые шаги (SILworX First Steps Manual HI 801 301 RU).

5.2 Responsibility

На каждой системной шине только один модуль системной шины может иметь атрибут *Responsible* и параметрироваться в качестве ответственного за работу шины.

- Для системной шины A задан атрибут *Responsible* для модуля системной шины или для процессорного модуля X-CPU 31 на стойке 0, слот 1.
- Для системной шины B действует следующее:
  - При использовании X-SB 01 и X-CPU 01 атрибут устанавливается с помощью SILworX.
  - При использовании X-CPU 31 атрибут установлен для X-CPU 31 в стойке 0, слот 2.

  Модуль системной шины с параметром *Responsible* должен находиться либо в несущем каркасе 0, слот 2, либо в несущем каркасе 1, слот 2.

Перед запуском безопасного режима это должно быть обеспечено.

Методика установки Responsibility описана в руководстве Первые шаги (SILworX First Steps Manual HI 801 301 RU).

⚠ ПРЕДУПРЕЖДЕНИЕ

Опасность травмирования персонала!

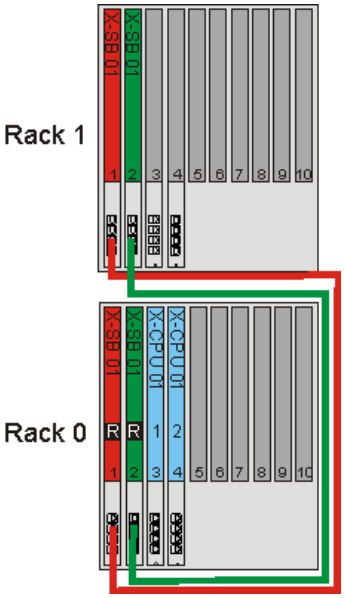
Параметрирование должно верифицироваться с помощью SILworX.

При этом обязательно соблюдать следующий порядок действий:

- **Войти в SILworX, используя логин модуля на модуле системной шины в стойке 0, слот 2**
- **Войти в SILworX, используя логин модуля на модуле системной шины в стойке 1, слот 2**
- **При открытых панелях управления обоих модулей системных шин убедиться в том, что атрибут "responsible" установлен только для правильного модуля системной шины (см. Рис. 1 и Рис. 2)!**

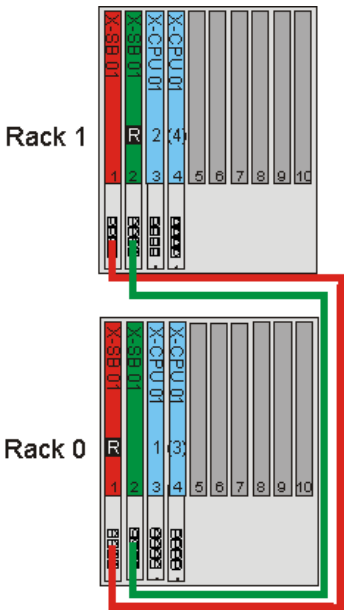
Рекомендуемые конфигурации:

- Если процессорные модули установлены только на стойке 0, то атрибут *Responsible* следует задать обоим модулям системных шин стойки 0 (Рис. 1).
- Если процессорные модули (Рис. 2) установлены также на стойке 1, то атрибут *Responsible* должны иметь следующие модули системных шин:
  - в стойке 0 — модуль системной шины на слоте 1 (автоматически).
  - в стойке 1 - модуль системной шины на слоте 2.



R Модуль системной шины является ответственным

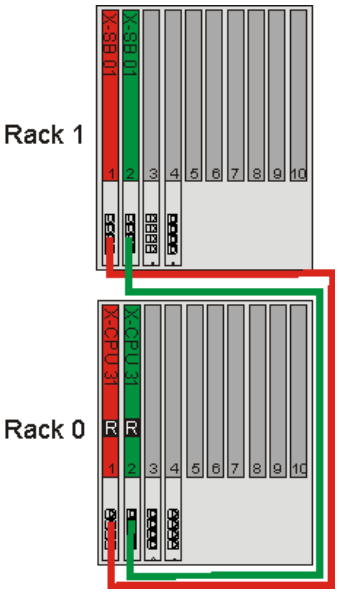
Рис. 1: Рекомендованная конфигурация: все процессорные модули на стойке 0



R Модуль системной шины является ответственным

Рис. 2: Рекомендованная конфигурация: процессорные модули X-CPU 01 на стойке 0 и стойке 1

- Если процессорные модули X-CPU 31 установлены на стойке 0, слоты 1 и 2 (Рис. 3), такие как X-CPU 31, всегда являются ответственными. В этом случае не устанавливайте системный модуль в стойке 1, слот 2, в качестве ответственного!



R Процессорный модуль является ответственным

Рис. 3: Конфигурация с процессорными модулями X-CPU 31 на стойке 0, слоты 1 и 2

6 Коммуникационный модуль

Коммуникационные модули имеют как безопасный сетевой трафик посредством других систем управления HIMA, так и небезопасный сетевой трафик через полевые шины и Ethernet.

- Процессорный модуль управляет безопасным сетевым трафиком с использованием протокола передачи safe**ethernet**, сертифицированного по уровню SIL 3. Модуль связи перенаправляет пакеты данных другим системам. Безопасный протокол обнаруживает искажения сообщений (принцип «черного канала»).

  Это позволяет осуществлять безопасную коммуникацию с использованием небезопасных путей передачи, т. е. через стандартные компоненты сети.
- К стандартным протоколам относятся, например:
  - Modbus
  - Ведущее/ведомое устройство PROFIBUS

Система HIMax может быть оснащена максимум 20 модулями связи.

Более подробную информацию см. в главе 12.1, руководство по модулю связи (HIMax X-COM 01 Manual HI 801 065 RU) и руководство по связи (Communication Manual HI 801 062 RU).

7 Модули ввода

Модуль	Количество каналов	Безопасные	Каналы без реактивного воздействия	Примечание
Цифровые входы				
X-DI 16 01	16	SIL 3	•	120 В перем. тока
X-DI 32 01	32	SIL 3	•	
X-DI 32 02	32	Уровень совокупной безопасности 3	•	Неконтактные датчики (NAMUR)
X-DI 32 03	32	SIL 3	•	48 В пост. тока
X-DI 32 04	32	SIL 3	•	С регистрацией последовательности событий
X-DI 32 05	32	SIL 3	•	Неконтактные датчики (NAMUR) с регистрацией последовательности событий
X-DI 32 51	32	-	•	
X-DI 32 52	32	-	•	Неконтактные датчики (NAMUR)
X-DI 64 01	64	SIL 3	•	
X-DI 64 51	64	-	•	
Аналоговые входы				0/4…20 мА
X-AI 16 51	16	SIL 1	•	
X-AI 32 01	32	SIL 3	•	
X-AI 32 02	32	SIL 3	•	С регистрацией последовательности событий
X-AI 32 51	32	-	•	
Входы счетчика				
X-CI 24 01	24	SIL 3	•	
X-CI 24 51	24	-	•	

Таблица 10: Обзор модулей ввода

7.1 Общие положения

Безопасные входы разрешается использовать как для безопасных, так и для небезопасных сигналов. Однако небезопасные сигналы не разрешается использовать для функций безопасности!

Безопасные модули ввода во время работы автоматически выполняют качественную циклическую самодиагностику.

При возникновении ошибки прикладная программа через глобальную переменную получает предустановленное значение, а затем по возможности генерируется информация об ошибке. Эту информацию об ошибке можно анализировать в прикладной программе, считав код ошибки.

Помимо индикации контрольными светодиодами на модулях системы управления также генерируют сообщения об ошибках и статусные сообщения, которые сохраняются в память. PADT считывает эти сообщения, сохраненные в памяти диагностики.

Более детальную информацию о модулях ввода см. в руководствах по модулям.

7.2 Безопасность датчиков, декодеров и трансмиттеров

При безопасном применении как ПЭС, так и подключенные к ней датчики, декодеры и трансмиттеры должны соответствовать требованиям безопасности и указанному уровню совокупной безопасности. Рекомендации по достижению необходимого уровня совокупной безопасности для датчиков можно найти, например, в IEC 61511-1, раздел 11.4.

7.3 Безопасные цифровые входы

Цифровой входной модуль считывает сигналы цифровых входов и выдает безопасные значения в каждом цикле процессорного модуля. Модуль циклически тестирует входы на безопасное функционирование.

7.3.1 Тестовые программы

Тестовые онлайн-программы проверяют, в состоянии ли входные каналы последовательно подключать оба уровня сигналов (сигнал 0 и 1) независимо от имеющихся входных сигналов. Данный тест функциональности выполняется при каждом считывании входных сигналов.

7.3.2 Избыточность

Допускается резервное подключение цифровых входов. Резервное подключение обычно служит повышению уровня готовности.

Для прочих подключений (для повышения уровня совокупной безопасности) требуется обработка аварийных состояний в логической схеме прикладной программы.

7.3.3 Перенапряжение на цифровых входах

Короткое время цикла системы HIMax позволяет цифровым входам считывать импульсные перенапряжения согласно EN 61000-4-5 как кратковременный сигнал 1.

В случае применения экранированных кабелей для цифровых входов дополнительных мер по предупреждению перенапряжения не требуется.

Если экранированный кабель не применяется, следует использовать задержку включения/выключения канала, чтобы избежать подобных сбоев. Сигнал должен подаваться в течение определенного минимального промежутка времени, прежде чем его можно будет проанализировать. К значению времени реакции и установленному для ресурса значению безопасного времени следует прибавить сумму установленного времени задержки и удвоенного времени цикла ввода/вывода.

7.4 Безопасные аналоговые входы и входы инициаторов

Аналоговые входные каналы преобразуют измеренные значения входных токов в значение типа данных DINT (double integer) (*исходное значение*) и в *технологическое значение*, относящееся к типу данных REAL. *Исходное значение* представляет собой результат измерений входного сигнала, а технологическое значение является масштабированным значением.

Входы инициаторов генерируют цифровое значение, сравнивая исходное значение с параметрируемыми пороговыми значениями.

7.4.1 Тестовые программы

Модуль регистрирует аналоговые значения двумя способами и сравнивает результаты. Кроме того, выполняется циклическое тестирование путей ввода.

7.4.2 Избыточность

Допускается резервное подключение цифровых входов. Резервное подключение обычно служит повышению уровня готовности.

Для прочих подключений (для повышения уровня совокупной безопасности) требуется обработка аварийных состояний в логической схеме прикладной программы.

7.4.3 Состояние LL, L, N, H, HH в X-AI 32 01 и X-AI 32 02

Если для канала аналогового входного модуля X-AI 32 01 или X-AI 32 02 определены скалярные события для предельных значений, то переменные состояния *-> State LL*, *-> State L*, *->State N*, *-> State H*, *-> State HH* **для безопасных прикладных программ необходимо соотнести с переменной** *Channel OK* **! В случае ошибки эти переменные состояния принимают значение FALSE.**

7.5 Безопасные входы для счетчиков

Безопасный вход счетчика в зависимости от своей конфигурации может выдавать следующие значения процесса:

- Показания счетчика как целое значение или как скалярное значение с плавающей запятой
- Скорость вращения или частота как целое значение или как скалярное значение с плавающей запятой
- Другие вспомогательные показания, например переполнение.

Подробнее см. в руководстве по модулям (HIMax X-CI 24 01 Manual HI 801 140 RU).

7.5.1 Тестовые программы

Модуль параллельно регистрирует значения счетчика тремя способами и сравнивает полученные показания между собой. Кроме того, выполняется циклическое тестирование путей ввода.

7.5.2 Это нужно учитывать при использовании модуля счетчика X-CI 24 01!

При использовании модуля счетчика X-CI 24 01 следует соблюдать следующие особые условия, см. также соответствующее руководство по работе с модулем (HIMax X-CI 24 01 Manual HI 801 140 RU):

- При перезагрузке в ходе первых 3 циклов могут теряться входные импульсы, если во время перезагрузки изменить следующие параметры:
  - Способ анализа счетных импульсов
  - Задействованные пары каналов
- Если при обнаружении фронтов «2 фазы, 4 фронта» выходит из строя датчик одного канала, но при этом не обнаруживается разрыва цепи или замыкания, модуль выдает значение, соответствующее половине фактической частоты.
- При автоматическом повторном запуске модуля подсчитываемые импульсы могут быть потеряны.
- В зависимости от приложения следует рассмотреть возможность автоматического или ручного перезапуска модуля.
- Рекомендация по приложению:
  - при многофазном анализе и определении направления вращения рекомендуется применять резервные модули, т. к. только таким образом можно распознать дефект датчика.
  - Параметрирование подавления помех при измерении частот не имеет значения для обеспечения безопасности.

7.5.3 Избыточность

Допускается резервное подключение входов счетчика. Резервное подключение обычно служит повышению уровня готовности.

Для прочих подключений (для повышения уровня совокупной безопасности) требуется обработка аварийных состояний в логической схеме прикладной программы.

7.6 Контрольные перечни для входов

HIMA рекомендует пользоваться доступными контрольными перечнями для проектирования, программирования и ввода в эксплуатацию безопасных входов. Контрольные перечни можно использовать в качестве проектной документации, но они также могут служить и доказательством тщательно выполненного планирования.

Целесообразно для каждого отдельного используемого в системе безопасного входного канала в рамках проектирования или ввода в эксплуатацию 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.

Контрольные перечни в формате Microsoft® Word® можно найти на веб-сайте компании HIMA.

8 Модули вывода

Модуль	Количество каналов	Безопасные	С безопасным электрическим соединением	Примечание
Цифровые выходы				
X-DO 12 02	12	SIL 3	-	
X-DO 24 01	24	SIL 3	-	
X-DO 24 02	24	SIL 3	-	48 В пост. тока
X-DO 32 01	32	SIL 3	-	
X-DO 32 51	32	-	-	
Цифровые релейные выходы				
X-DO 12 01	12	SIL 3	•	230 В перем. тока
X-DO 12 51	12	-	•	
Аналоговые выходы				
X-AO 16 01	16	SIL 3	попарно	
X-AO 16 51	16	-	-	

Таблица 11: Обзор модулей вывода

8.1 Общие положения

Безопасные модули вывода описываются один раз в каждом цикле, выполняется обратное считывание выходных сигналов и сравнение с заданными выходными данными.

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

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

Более детальную информацию по модулям вывода см. в руководствах по модулям.

8.2 Безопасность исполнительных элементов

При безопасном применении как ПЭС, так и подключенные к ней исполнительные элементы, должны соответствовать требованиям безопасности и указанному уровню совокупной безопасности. Указания по достижению необходимого уровня совокупной безопасности для датчиков и исполнительных элементов см., например, в IEC 61511-1, раздел 11.4.

8.3 Безопасные цифровые выходы

Кроме того, в безопасных выходных каналах для отключения отдельного канала последовательно интегрированы три тестируемых переключателя. Таким образом выполняется требование для 3-го уровня совокупной безопасности безопасным независимым вторым способом отключения. Этот встроенный блок предохранительного отключения в случае ошибки отключает отдельные каналы неисправного модуля вывода (обесточенное состояние).

Кроме того, сигнал сторожевого устройства модуля является вторым способом отключения: потеря сигнала сторожевого устройства ведет к немедленному переходу в безопасное состояние.

8.3.1 Тестовые программы для цифровых выходов

Модули тестируются автоматически во время работы. К существенным функциям тестирования относится:

- Обратное считывание выходного сигнала
- Проверка встроенного двойного предохранительного отключения
- Тест отключения выходов
- Контроль рабочего напряжения

8.3.2 Output Noise Blanking

При активированном подавлении помех выхода (Output Noise Blanking) выходной модуль задерживает реакцию отключения канала.

i **При активированном подавлении помех выхода (Output Noise Blanking) необходимо учитывать, что при подавлении помех от переходного процесса возрастает время реакции на значение параметра *безопасное время – время сторожевого устройства*.**

В любом случае ошибка дополнительно отображается светодиодом *Error* на передней панели.

8.3.3 Поведение при коротком замыкании или перегрузке

При замыкании выхода на L- или при перегрузке безопасность модуля сохраняется.

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

8.3.4 Избыточность

Допускается резервное подключение цифровых выходов. Резервное подключение обычно служит повышению уровня готовности.

Для прочих подключений (для повышения уровня совокупной безопасности) требуется обработка аварийных состояний в логической схеме прикладной программы.

8.4 Безопасные релейные выходы

Модули релейного выхода используются в случае, если для подключенного исполнительного элемента действует одно или несколько из следующих условий:

- Требуется электрическое разделение.
- Увеличенная сила тока.
- Переключение переменного тока.

В модуле выходы оснащены двумя безопасными реле с контактами с принудительным управлением. Таким образом выходы для безопасных отключений используются в соответствии с уровнем совокупной безопасности 3 (SIL 3).

Кроме того, сигнал сторожевого устройства модуля является вторым способом предохранительного отключения: потеря сигнала сторожевого устройства ведет к немедленному переходу в безопасное состояние.

8.4.1 Тестовые программы для релейных выходов

Модуль автоматически тестируется во время работы. К существенным функциям тестирования относится:

- Обратное считывание выходных сигналов коммутирующего усилителя перед реле
- Проверка переключения реле с принудительным управлением контактами
- Проверка встроенного двойного предохранительного отключения
- Контроль рабочего напряжения

8.4.2 Избыточность

Допускается резервное подключение цифровых релейных выходов. Резервное подключение обычно служит повышению уровня готовности.

Для прочих подключений (для повышения уровня совокупной безопасности) требуется обработка аварийных состояний в логической схеме прикладной программы.

8.5 Безопасные аналоговые выходы

Эти выходы передают значения, полученные в прикладной программе, на исполнительные элементы.

Безопасные аналоговые выходы считывают выходные значения и сравнивают их с выдаваемыми значениями. При наличии расхождений следует реакция на ошибку.

8.5.1 Тестовые программы для аналоговых выходов

Модули тестируются автоматически во время работы. К существенным функциям тестирования относится:

- Обратное считывание выходного сигнала.
- Проверка встроенного двойного предохранительного отключения.

При возникновении ошибок выходы устанавливаются на безопасное значение 0 мА.

8.5.2 Output Noise Blanking

При активированном подавлении помех выхода (Output Noise Blanking) выходной модуль задерживает реакцию отключения канала.

i **При активированном подавлении помех выхода (Output Noise Blanking) необходимо учитывать, что при подавлении помех от переходного процесса возрастает время реакции на значение параметра *безопасное время – время сторожевого устройства*.**

В любом случае ошибка дополнительно отображается светодиодом *Error* на передней панели.

8.5.3 Поведение при внешнем разрыве цепи

При разрыве цепи модуль подключает ток примерно на 8 мс и выполняет проверку на разрыв цепи. В случае обнаружения разрыва цепи модуль отключается прим. на 10 с. Этот процесс может повторяться бесконечно часто.

8.5.4 Это нужно учитывать при использовании аналогового выходного модуля X-AO 16 01!

При использовании аналогового выходного модуля необходимо соблюдать следующие особые условия, см. также руководство по модулям (HIMax X-AO 16 01 Manual HI 801 139 RU):

- Допустимы только схемы коммутации, указанные в руководстве (HIMax X-AO 16 01 Manual HI 801 139 RU)!
- При серийном резервировании более чем двух модулей напряжение БСНН может превышаться!
- При серийном резервировании из каждой группы из двух каналов следует использовать только один!
- Если между подсоединенным исполнительным элементом и HART-терминалом осуществляется коммуникация по протоколу HART, возможно искажение выходного сигнала до 1 % к результату!
- При возникновении ошибки максимальное время до достижения безопасного состояния может в худшем случае составить до 16 мс. Необходимо учитывать это время при расчете времени реакции и безопасного времени!
- Прикладная программа должна описывать аналоговые выходы в циклах не менее 6 мс.
- В случае сбоя модуль выдаст безопасное значение 0 мА, как и в случае превышения верхней границы диапазона настройки.

8.5.5 Избыточность

Допускается резервное подключение цифровых выходов. Резервное подключение обычно служит повышению уровня готовности.

Для прочих подключений (для повышения уровня совокупной безопасности) требуется обработка аварийных состояний в логической схеме прикладной программы.

8.6 Контрольные перечни для выходов

HIMA рекомендует пользоваться доступными контрольными перечнями для проектирования, программирования и ввода в эксплуатацию безопасных выходов. Контрольные перечни можно использовать в качестве проектной документации, но они также могут служить и доказательством тщательно выполненного планирования.

Целесообразно для каждого отдельного используемого в системе безопасного выходного канала в рамках проектирования или ввода в эксплуатацию 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.

Контрольные перечни в формате Microsoft® Word® можно найти на веб-сайте компании HIMA.

9 Специальные модули ввода/вывода

9.1 HART-модуль X-HART 32 01

HART-модуль предназначен для коммуникации с HART-совместимыми датчиками и исполнительными элементами,

Подробнее см. в руководстве по модулям (HIMax X-HART 32 01 Manual HI 801 366 RU).

9.1.1 Обеспечение безопасности

Функция безопасности X-HART-модуля охватывает следующие аспекты:

- Деактивация HART: при выключении модуля каналы HART безопасно деактивируются в соответствии с требованиями к уровню совокупной безопасности SIL 3.
- Фильтрация HART: HART-доступ к трансмиттерам или датчикам HART запрещен в соответствии с требованиями к уровню совокупной безопасности SIL 3.
- Коммуникация HART искажает точность аналоговых измерений примерно на 1 %.

  Другого влияния на аналоговые модули не оказывается.
- Если на HART-модуле отключается функция фильтрации HART, возможно перепрограммирование соответствующего аналогового датчика или исполнительного элемента. Это может отрицательно сказаться на безопасности.

9.2 Модуль защиты от превышения частоты вращения X-MIO 7/6 01

Модуль предназначен для контроля за частотой оборотов и для -аварийного останова (функция аварийного отключения) турбины. Подробнее см. в руководстве по модулям (HIMax X-MIO 7/6 01 Manual HI 801 365 RU).

При помощи модуля могут реализовываться приложения в соответствии с API 670. Модуль осуществляет контроль числа оборотов и выполнения стандартных программ выключения турбин в соответствии с API 670. При этом система контроля числа оборотов и стандартные программы выключения функционируют независимо от общей системы HIMax и программы пользователя.

9.2.1 Обеспечение безопасности

Модуль выполняет контроль числа оборотов турбины независимо от общей системы HIMax и программы пользователя. Модуль производит самостоятельно отключение турбины через цифровые выходы.

В зависимости от измерительного входа модуль получает от датчика значения количества оборотов и направления вращения с точностью, необходимой для обеспечения уровня безопасности. Для выполнения расчета числа оборотов для каждой турбины предусмотрено 3 сенсора. На основе значения числа оборотов, полученного от трех датчиков, модуль выполняет анализ 2oo3. Результат передается безопасной процессорной системе X-MIO 7/6 01 и прикладной программе.

При потере сигнала датчика модуль выдает предупреждение. При потере двух из трех сигналов модуль активирует функцию аварийного отключения (Trip function).

Модуль имеет цифровые безопасные выходы, см. главу 8.3.

Функция безопасности всех входов и выходов реализована в соответствии с требованиями уровня совокупной безопасности SIL 3. Релейный выход выполнен как беспотенциальный, небезопасный сигнальный контакт (переключающий контакт).

9.2.2 Избыточность

Для повышения готовности модуль подлежит двукратному резервированию. Для этого рекомендуется использовать исключительно двойные платы сопряжения.

10 Software, программное обеспечение

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

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

Операционная система загружена в каждый модуль системы управления. Рекомендуется использовать последнюю действительную версию для безопасного использования. В этой главе особое внимание уделяется операционной системе процессорного модуля.

Прикладная программа составляется посредством *системы программирования* SILworX и включает в себя функции для конкретной установки, которые должно выполнять устройство автоматизации. Параметрирование также выполняется с помощью SILworX.

Прикладная программа переводится при помощи генератора кода, а затем переносится в энергонезависимую память устройства автоматизации через интерфейс Ethernet.

10.1 Аспекты безопасности для операционной системы

Каждая допущенная операционная система имеет однозначный номер версии и сигнатуру CRC. Действительные версии операционной системы, допущенные TÜV к использованию в безопасных устройствах автоматизации, а также соответствующие сигнатуры (CRC) подлежат контролю версий и вносятся в составляемый совместно с TÜV *Version List of Modules and Firmware for HIMax Systems from HIMA Paul Hildebrandt GmbH*.

Считать текущий номер версии операционной системы можно с помощью системы программирования SILworX. Необходимо проверить, загружена ли в модули допустимая версия операционной системы (ср. 11.3 Контрольный перечень по созданию прикладной программы).

10.2 Аспекты безопасности для программирования

При составлении прикладной программы следует учитывать указанные здесь требования.

10.2.1 Концепция безопасности SILworX

Концепция безопасности SILworX:

- При установке SILworX с помощью контрольной суммы CRC защищается целостность пакета программы на пути от изготовителя к пользователю.
- SILworX выполняет проверки достоверности, чтобы минимизировать возможность ошибки при вводе.

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

- Проверка правильного осуществления задачи управления на основании данных и потоков сигналов.
- Полная функциональная проверка логической схемы путем отладки (см. главу 10.2.2).

После внесения изменений в прикладную программу следует проверить только те части программы, которых коснулись изменения. Кроме того, безопасное сравнивающее устройство версии SILworX может определять изменения по сравнению с предыдущей версией и показывать их пользователю.

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

10.2.2 Проверка конфигурации и прикладной программы

Чтобы проверить составленную прикладную программу на соблюдение указанной функции безопасности, пользователь должен сгенерировать подходящие варианты теста, которые покрывают 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 так, чтобы подтверждалась правильность расчета. Необходимое количество вариантов теста зависит от используемой формулы и должно охватывать критические пары значений.

Фирма HIMA рекомендует не отказываться от активного моделирования с источниками, поскольку только так можно подтвердить правильность проводки датчиков и исполнительных элементов системы (также подключенные посредством блока связи с удаленным устройством ввода/вывода). Только так можно проверить конфигурацию системы.

SILworX можно использовать как вспомогательное средство проверки:

- Проверка входов
- Инициализация выходов

Данные действия необходимо соблюдать как при первом составлении прикладной программы, так и при ее изменениях.

10.3 Параметры ресурса

Некоторые параметры устанавливаются в SILworX для допустимых действий при безопасной работе ресурса и именуются параметрами безопасности.

⚠ ПРЕДУПРЕЖДЕНИЕ

Опасность травмирования персонала из-за неправильной кофигурации!

Ни система программирования, ни система управления не могут проверять параметры, специально установленные для конкретного проекта. Поэтому обязательно корректно вносить эти параметры безопасности в систему программирования и после загрузки сделанной записи в ПЭС проверять ее там же.

К таким параметрам относятся:

- **ID стойки, см. 5.1 и руководство по системе (HIMax System Manual HI 801 060 RU).**
- **Атрибут responsible модулей системной шины или процессорных модулей, см. 5.2**
- **выделенные в таблице Таблица 12 параметры**

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

10.3.1 Системные параметры ресурса

Системные параметры ресурса устанавливаются в SILworX в диалоговом окне *Properties* (Свойства) ресурса.

Параметр / кнопка-флажок [1)]	Описание	Значение по умолчанию	Настройка для безопасной эксплуатации
Name	Имя ресурса		Произвольное
System ID [SRS]	Системный ID ресурса 1…65 535 Необходимо присвоить ID системы значение, отличное от значения по умолчанию; в противном случае проект не будет готов к выполнению!	60 000	Однозначное значение внутри сети систем управления. Это все системы управления, которые потенциально связаны между собой.
Safety Time [ms]	Безопасное время в миллисекундах 20...22 500 мс (возможна корректировка онлайн)	600 мс	Зависит от приложения
Watchdog Time [ms]	Время сторожевого устройства в миллисекундах: 6...7500 мс (возможна корректировка онлайн)	200 мс	Зависит от приложения
Target Cycle Time [ms]	Необходимое или максимальное время цикла, см. *Target Cycle Time Mode (Режим заданного времени цикла)*, 0...7500 мс. Требуемое время цикла максимально может равняться требуемому времени сторожевого устройства минус 6 мс; в противном случае оно будет отклонено ПЭС. Если значение по умолчанию выставлено на 0 мс, требуемое значение времени цикла не учитывается. (возможна корректировка онлайн)	0 мс	Зависит от приложения
Target Cycle Time Mode	Использование *Target Cycle Time [ms]*. (возможна корректировка онлайн) см. Таблица 13	Fixed-tolerant	Зависит от приложения
Multitasking Mode	Mode 1 Длительность цикла ЦПУ зависит от необходимой продолжительности исполнения всех прикладных программ.	Mode 1	Зависит от приложения
	Mode 2 Процессор выделяет из времени выполнения, не востребованного прикладными программами низкого приоритета, время выполнения для прикладных программ высокого приоритета. Режим функционирования, обеспечивающий высокий уровень готовности.		
	Mode 3 Процессор не ждет, пока истечет время выполнения прикладных программ, таким образом увеличивая 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]	Задает промежуток времени в рамках цикла ЦПУ, доступный для конфигурационных соединений: 2...3500	12 мс	Зависит от приложения

Параметр / кнопка-флажок [1)]	Описание		Значение по умолчанию	Настройка для безопасной эксплуатации
Maximum System Bus Latency [µs]	Максимальная задержка сообщения между модулем входа/выхода и процессорным модулем. 0, 100...50 000 мкс		0 мкс	Зависит от приложения
	i Для установки максимального значения задержки системной шины > 0 необходима лицензия.			
Allow Online Settings	ON: **Все** переключатели/параметры, перечисленные под OFF, могут быть изменены онлайн с помощью PADT. Это возможно только в случае, если системная переменная *Read-only in RUN* имеет значение OFF.		ON	Рекомендуется OFF
	OFF: Следующие параметры **не** имеют возможности корректировки онлайн: ▪ *System ID* ▪ *Autostart* ▪ *Global Forcing Allowed* ▪ *Global Force Timeout Reaction* ▪ *Loading Allowed* ▪ *Reload Allowed* ▪ *Start Allowed*	Следующие параметры имеют возможность для корректировки онлайн в случае, если *Reload Allowed* присвоено значение ON: ▪ *Watchdog Time* (Время сторожевого устройства ресурса) ▪ *Safety Time* ▪ *Target Cycle Time* ▪ *Target Cycle Time Mode* Если *Reload Allowed* имеет значение OFF, они не могут быть изменены онлайн.		
	i Параметру *Allow Online Settings* возможно присвоить значение ON при остановленной ПЭС и с помощью перезагрузки.			
Autostart	ON	Если процессорный модуль подсоединен к питающему напряжению, прикладная программа запускается автоматически	OFF	Зависит от приложения
	OFF	После подключения питающего напряжения автоматический старт не происходит.		
Start Allowed	ON	Разрешен холодный, теплый или горячий пуск с помощью PADT в состоянии RUN или STOP.	ON	Зависит от приложения
	OFF	Запуск не разрешен		
Load Allowed	ON	Загрузка конфигурации разрешена	ON	Зависит от приложения
	OFF	Загрузка конфигурации не разрешена		
Reload Allowed	ON	Перезагрузка конфигурации разрешена.	ON	Зависит от приложения
	OFF	Перезагрузка конфигурации не разрешена. При переключении на OFF текущая перезагрузка не прерывается		

Параметр / кнопка-флажок [1]	Описание		Значение по умолчанию	Настройка для безопасной эксплуатации
Global Forcing Allowed	ON	Разрешена глобальная инициализация для данного ресурса	ON	Зависит от приложения
	OFF:	Глобальная инициализация для данного ресурса не разрешена		
Global Force Timeout Reaction	Определяет порядок действий ресурса по истечении времени ожидания инициализации: ▪ Завершить инициализацию ▪ Остановить ресурс		Завершить инициализацию	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 HIMax.		SILworX V6 в новых проектах	Зависит от приложения
	SILworX V2	Генерирование кода реализовано так же, как в SILworX V2, за исключением новых функций.		
	SILworX V3	Генерирование кода для HIMax V3.		
	SILworX V4	Генерирование кода для HIMax V4.		
	SILworX V5	Генерирование кода для HIMax V5.		
	SILworX V6	Генерирование кода для HIMax V6. Данная установка гарантирует совместимость с последующими версиями.		
[1] **Безопасные параметры** выделены жирным шрифтом.				

Таблица 12: Системные параметры ресурса

10.3.1.1 Применение параметров *Target Cycle Time* и *Target Cycle Time Mode*

Эти параметры можно использовать для того, чтобы по возможности постоянно поддерживать значение времени цикла в соответствии с установкой *Target Cycle Time [ms]*. Для этого следует установить значение параметра > 0. HIMax таким образом ограничивает перезагрузку и синхронизацию резервных процессорных модулей, чтобы соблюдалось соответствие заданному времени цикла.

Таблица ниже описывает воздействие, оказываемое режимом заданного времени цикла.

Target Cycle Time Mode	Воздействие на прикладные программы	Воздействие на перезагрузку, синхронизацию 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 или синхронизация выполняются только при достаточном заданном времени цикла
Fixed-tolerant		Максимум каждый пятый цикл может быть увеличен во время перезагрузки. Во время синхронизации можно продлить время только одного цикла.
Dynamic-tolerant	HIMax выполняет цикл за минимально возможное время.	Максимум каждый пятый цикл может быть увеличен во время перезагрузки. Во время синхронизации можно продлить время только одного цикла.
Dynamic		Перезагрузка или синхронизация выполняются только при достаточном заданном времени цикла

Таблица 13: Воздействие режима заданного времени цикла

10.3.1.2 Вычисление максимальной продолжительности конфигурационных соединений

Если обработка данных коммуникации не выполнена за один цикл ЦПУ, она будет продолжена с точки прерывания в рамках непосредственно следующего цикла ЦПУ.

Хотя коммуникация из-за этого замедляется, но зато все соединения с внешними абонентами при этом обрабатываются по одному приоритету и полностью.

Для встроенного ПО HIMax-CPU V3 максимальная продолжительность конфигурационных соединений устанавливается SILworX в размере 6 мс. Однако допустимо, что время обработки коммуникации со внешними абонентами в рамках одного цикла ЦПУ может превысить заданное значение.

Для встроенного ПО HIMax-CPU V4 или выше максимальную продолжительность конфигурационных соединений следует устанавливать, соблюдая соответствие заданному времени сторожевого устройства.

Оптимальная настройка: выбрать такое значение, чтобы за время, оставшееся в результате вычисления *Watchdog Time – Max. Duration of Configuration Connections*, могли быть выполнены циклические задачи процессора.

Количество конфигурационных данных, предназначенных для передачи, зависит от количества сконфигурированных удаленных устройств ввода/вывода, имеющихся соединений с PADT, а также модулей в системе, имеющих интерфейс Ethernet.

Первое значение для настройки рассчитывается следующим образом:

$T_{Config} = (n_{Com} + n_{RIO} + n_{PADT}) * 0{,}25$ мс + 2 мс + 4 * $T_{Latency}$, где:

T_{Config}	Системный параметр *Max. Duration of Configuration Connections [ms]*
n_{Com}	Количество модулей с интерфейсом Ethernet {SB, ЦПУ, COM}
n_{RIO}	Количество сконфигурированных удаленных устройств ввода-вывода
n_{PADT}	Макс. количество PADT-соединений = 5
$T_{Latency}$	Системный параметр *Maximum System Bus Latency [µs]*

Если вычисленное время составляет менее 6 мс, оно округляется до 6 мс. Допускается исправление вычисленного времени позже на основе онлайн-статистики либо в окне «Свойства ресурса», либо напрямую онлайн.

i Во время генерирования кода и во время конвертации проекта через PADT выдается соответствующее указание, если установленный параметр *Max. Duration of Configuration Connections* оказывается меньше результата, полученного по приведенной выше формуле.

10.3.1.3 Указания к параметру *Minimum Configuration Version*:

- При создании каждого нового проекта выбирается самая актуальная минимальная конфигурация (*Minimum Configuration Version*). Необходимо удостовериться в том, что эта настройка совместима с используемой версией операционной системы.
- Если проект был конвертирован в предыдущей версии SILworX, то установленное в предыдущей версии значение параметра *Minimum Configuration Version* сохраняется. Благодаря этому при генерировании кода создается та же CRC конфигурации, что и в предыдущей версии, а генерированная конфигурация совместима с операционной системой модулей.
- 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. Модули не могут загрузить более высокую версию конфигурации, чем та, которая совместима с их операционной системой.

Чтобы легче было разобраться, просто сопоставьте данные, предоставленные функцией сравнения версий, с информацией, которую дает обзор данных модуля.

- Если для ресурса в качестве минимальной конфигурации установлена версия *SILworX V4* или выше, то в каждой прикладной программе (см. ниже) следует установить для параметра Code Generation Compatibility значение SILworX V4.
- При использовании процессорных модулей X-CPU 31 установите для параметра *Minimum Configuration Version* значение SILworX V6 или выше.

10.3.2 Системная переменная стойки

Эти переменные служат для изменения поведения системы управления во время работы при определенных состояниях.

Параметр / кнопка-флажок	Функция	Настройка по умолчанию	Настройка для безопасной эксплуатации
Force Deactivation	Служит для предотвращения и непосредственного отключения инициализации	OFF	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	OFF	Зависит от приложения
Read-only in Run	После запуска системы управления никакое из действий по управлению (останов, запуск, загрузка) через SILworX уже невозможно; исключения: инициализация и перезагрузка	OFF	Зависит от приложения
Reload Deactivation	Блокирует выполнение перезагрузки	OFF	Зависит от приложения

Таблица 14: Системные переменные аппаратного обеспечения

Этим системным переменным в редакторе аппаратного обеспечения SILworX могут быть приписаны глобальные переменные, значение которых определяется данными физического входа или логикой прикладной программы.

10.3.2.1 Пример: блокировка и деблокировка ПЭС

«**Блокировка**» ПЭС исключает возможность вмешательства пользователя во время работы. Таким образом предотвращается несанкционированное использование прикладной программы.

«Деблокировка» ПЭС обозначает снятие активной блокировки, например, для выполнения действий с системой управления.

Для блокировки используются три системные переменные: *Read only in Run*, *Reload Deactivation* и *Force Deactivation*.

Если все три системные переменные имеют значение ON, то доступ к системе управления уже невозможен. В таком случае систему управления можно вернуть в состояние STOP только путем перезагрузки всех процессорных модулей посредством приведения переключателя режимов в положение *Init*. Это позволяет перезапустить прикладную программу.

Приведение системы управления в состояние возможности блокировки

1. Определить глобальную переменную типа BOOL, предустановленное значение по умолчанию установить на FALSE.
2. Глобальную переменную как выходную переменную приписать 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 модуле ввода система управления деблокирована.

10.4 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 безопасной работы из-за 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 ответственным за приемку установки отделом контроля.

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

Подробнее об инициализации см. руководство по системе (HIMax System Manual HI 801 060 RU).

10.4.1 Инициализация физических входов и данных коммуникации

Изменение инициализированных глобальных переменных, привязывающее их значение к перечисленным ниже источникам данных, может привести к неожиданным результатам:

- Физические входы
- Протоколы связи

Следующий порядок действий приводит к непреднамеренной инициализации переменной:

1. Для глобальной переменной A задается инициализированный источник данных, и она становится инициализированной.
2. Присваивание значения отменяется.
3. Источнику данных присвоена другая глобальная переменная — B.
4. Изменения в проекте загружаются в ПЭС путем перезагрузки.

В результате переменной B **заново присваивается** значение, и она инициализируется совершенно непреднамеренно!

Обходное решение: сначала завершить инициализацию соответствующей переменной, в данном случае A.

В режиме отображения каналов в редакторе инициализации (Force Editor) можно увидеть, какие каналы инициализированы.

Глобальные переменные, для которых источником данных является прикладная программа, сохраняют статус *Forced* при изменении присваиваемого значения.

10.5 Безопасная функция сравнения версий

Безопасная функция сравнения версий в SILworX может сопоставлять различные конфигурации ресурсов:

- Конфигурацию ресурса, загруженную в систему управления
- Конфигурацию ресурса в PADT
- Экспортированную (архивированную) конфигурацию ресурса

Качество результата сравнения соответствует SIL 3, так как он был получен на основе подгружаемых файлов с сигнатурами (CRC).

Безопасную функцию сравнения версий следует установить для того, чтобы проверять изменения в программе, прежде чем загружать ее в систему управления.

Она позволяет точно определить измененные области конфигурации ресурса. Это облегчает проверку изменений и определение тестовых данных.

Структурированное программирование и использование интуитивно понятных имен, начиная с первых версий конфигурации, помогают легче разобраться в результатах сравнения.

10.6 Защита от манипуляций

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

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

- Изменение прикладной программы или конфигурации приводит к созданию нового CRC. Эти изменения могут быть перенесены в ПЭС путем загрузки или перезагрузки.
- Возможности управления зависят от прав зарегистрированного в ПЭС пользователя.
- Система программирования SILworX для соединения с ПЭС запрашивает пароль при входе пользователя в систему.
- Соединение между PADT и ПЭС во время режима RUN не требуется.

Необходимо соблюдать требования стандартов безопасности и использования в отношении защиты от манипуляций. Авторизация сотрудников и принятие необходимых мер защиты относятся к сфере ответственности эксплуатирующего предприятия.

⚠ ПРЕДУПРЕЖДЕНИЕ

Возможно травмирование персонала в результате несанкционированных манипуляций с системой управления!

Защищайте систему управления от несанкционированного доступа!

Например:

- **измените настройки по умолчанию для имени пользователя и пароля**
- **Контролируйте физический доступ к системе управления и PADT!**

Доступ к данным ПЭС возможен только в том случае, если используемый PADT имеет систему программирования SILworX и актуальную версию проекта пользователя (сохранение архива!).

Соединение между PADT и ПЭС требуется только для загрузки прикладной программы или для диагностики. Во время обычной эксплуатации PADT не требуется, отделение PADT и ПЭС на этапе обычной работы защищает от несанкционированного доступа.

11 Прикладная программа

В данной главе рассматриваются вопросы технической безопасности для прикладных программ.

11.1 Общая последовательность

Общая последовательность программирования устройств автоматизации HIMax для безопасного применения:

1. Спецификация функции управления.
2. Запись прикладной программы.
3. Перевод прикладной программы:
   прикладная программа не содержит ошибок и может работать.
4. Верификация и валидация.

Затем пользователь может протестировать прикладную программу, а затем ПЭС может перейти в безопасный режим работы.

11.2 Рамки безопасного применения

(Предзаданные параметры и правила, пояснения требований безопасности см. в главе 3.4 „Требования безопасности“)

Прикладная программа записывается при помощи программы для программирования SILworX. Одобренная версия операционной системы для персонального компьютера указана в документации к используемой версии SILworX.

По существу система для программирования SILworX включает в себя:

- Ввод (FBD Editor - программный редактор, Structured Text Editor - редактор структурированного текста), контроль и документация
- Глобальные переменные с символическими именами и типом данных (BOOL, UINT и т. д.)
- Присвоение систем управления системы HIMax (Hardware Editor - редактор аппаратного обеспечения)
- Перевод прикладной программы в форму, которую можно загрузить в ПЭС
- Конфигурацию связи

11.2.1 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 необходимой для безопасности избыточности (1oo2, 2oo3) (ср. приложение "Увеличение значения 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 тестировать.
- Легко изменить.

11.2.2 Функции прикладной программы

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

При программировании на физических входах и выходах должен учитываться принцип тока покоя. В логической схеме используются исключительно элементы согласно IEC 61131-3 с их соответствующими условиями функционирования.

- Физические входы и выходы в основном работают по принципу тока покоя, т. е. их безопасное состояние – 0.
- Прикладная программа может состоять из логических и/или арифметических функций 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.
- Для упрощения логической схемы входы и выходы всех функциональных блоков, а также переменные можно произвольно инвертировать.
- Сигналы об ошибках входов/выходов или из логических блоков должны анализироваться программистом.

Рекомендуется включение функций в самостоятельно создаваемые функциональные блоки, а также функций, состоящих из стандартных функций. Таким образом прикладную программу можно четко структурировать по модулям (функции, функциональные блоки). Каждый модуль может рассматриваться – и тестироваться – отдельно. Благодаря соединению модулей в один более крупный модуль и в одну прикладную программу образуется готовая, сложная функция.

11.2.3 Системные параметры прикладной программы

Следующие кнопки-флажки и параметры прикладной программы можно настраивать в диалоговом окне *Properties* прикладной программы:

Кнопка-флажок / Параметр	Функция	Значение по умолчанию	Настройка для безопасной эксплуатации
Name	Имя прикладной программы		Произвольное
Program ID	ID для идентификации программы, отображаемой в SILworX: 0...4 294 967 295. Если параметру *Code Generation Compatibility* присвоено значение *SILworX V2,* то для Program ID допустимо только значение 1.	0	Зависит от приложения
Priority	Приоритет прикладной программы: 0...31	0	Зависит от приложения
Program's Maximum Number of CPU Cycles	Максимальное количество циклов ЦПУ, допустимое для выполнения в рамках цикла прикладной программы.	1	Зависит от приложения
Max. Duration for Each Cycle [µs]	Максимальная продолжительность исполнения на цикл процессорного модуля для прикладной программы: 1...4 294 967 295 мкс. Установка на 0: без ограничений.	0 мкс	Зависит от приложения
Watchdog Time [ms] (calculated)	Время контроля прикладной программы, рассчитанное на основе максимального числа циклов и времени сторожевого устройства ресурса Неизменяемо!		
Classification	Классификация прикладной программы: Safety-related или Standard (только для документации).	Safety-related	Зависит от приложения
Allow Online Settings	Разрешение на оперативное изменение состояния других переключателей прикладной программы. Срабатывает только в случае, если переключатель ресурса *Allow Online Settings* находится в положении ON!	ON	-
Autostart	Разрешенный способ автозапуска: Cold Start, Warm Start, Off	Cold Start	Зависит от приложения
Start Allowed	ON Запуск прикладной программы с помощью PADT разрешен. OFF Запуск прикладной программы с помощью PADT запрещен.	ON	Зависит от приложения
Test Mode Allowed	ON Для прикладной программы разрешен режим тестирования. OFF Для прикладной программы не разрешен режим тестирования.	OFF	Зависит от приложения1)
Reload Allowed	ON Разрешена загрузка прикладной программы. OFF Загрузка прикладной программы не разрешена.	ON	Зависит от приложения
Local Forcing Allowed	ON Разрешена инициализация на уровне программы. OFF Инициализация на уровне программы не разрешена.	OFF	Рекомендуется OFF
Local Force Timeout Reaction	Поведение прикладной программы по истечении времени инициализации: ▪ Stop Forcing Only (Завершить только инициализацию). ▪ Stop Program (Остановить программу).	Stop Forcing Only (Завершить только инициализацию).	-

Кнопка-флажок / Параметр	Функция		Значение по умолчанию	Настройка для безопасной эксплуатации
Code Generation Compatibility	Генерирование кода совместимо с предыдущими версиями SILworX		SILworX V4 в новых проектах	Зависит от приложения
	SILworX V4	Генерирование кода совместимо с SILworX V4.		
	SILworX V3	Генерирование кода совместимо с SILworX V3.		
	SILworX V2	Генерирование кода совместимо с SILworX V2.		
[1] По завершении работы в тестовом режиме перед началом безопасной эксплуатации требуется холодная загрузка программы!				

Таблица 15: Системные параметры прикладной программы

Указания по использованию параметра *Code Generation Compatibility:*

- При создании нового проекта SILworX выбирает самое новое значение для параметра *Code Generation Compatibility.* Благодаря этому активируются актуальные и улучшенные настройки, а также обеспечивается поддержка последних версий модулей и OS. Необходимо удостовериться в том, что эти настройки совместимы с используемым аппаратным обеспечением.
- Если конвертированный проект был создан в более ранней версии SILworX, то для параметра *Code Generation Compatibility* сохраняется значение, заданное в предыдущей версии. Благодаря этому при генерировании кода создается та же CRC конфигурации, что и в предыдущей версии, а генерированная конфигурация совместима с операционной системой модулей.

  Поэтому при работе с конвертированными проектами не следует менять значение параметра *Code Generation Compatibility*.
- Если для ресурса в качестве *Minimum Code Generation* установлена версия *SILworX V4* или выше, то в каждой прикладной программе (см. выше) следует установить для параметра *Code Generation Compatibility* значение *SILworX V4*.

11.2.4 Генерирование кода

После полного ввода прикладной программы и назначения входов/выходов системы управления генерируется код. При этом генерируется CRC конфигурации — контрольная сумма файлов конфигурации.

Он является сигнатурой для всей конфигурации и выдается как шестнадцатеричный код в 32-битном формате. Все конфигурируемые или изменяемые элементы, как, например, логическая схема, переменные, настройки переключателей, входят сюда.

Чтобы обеспечить безопасность эксплуатации, перед загрузкой прикладной программы необходимо провести ее двукратную компиляцию. Обе созданные версии должны иметь одинаковые контрольные суммы.

SILworX автоматически выполняет двукратную конфигурацию проекта и сопоставляет контрольные суммы, если для генерирования кода выбрана опция *CRC Comparison*. Это предустановленная опция.

Результат сопоставления CRC можно увидеть в регистрационном журнале.

Благодаря двукратной компиляции со сравнением контрольных сумм можно обнаружить возможные искажения прикладной программы, которые были вызваны единичными ошибками в аппаратном обеспечении или в операционной системе используемого ПК.

11.2.5 Загрузка и запуск прикладной программы

Процесс загрузки ПЭС системы HIMax посредством Download может осуществляться только, если прежде система была приведена в состояние STOP.

Процесс загрузки охватывает все прикладные программы конфигурации проекта. Весь процесс загрузки конфигурации проекта контролируется. Затем можно запустить прикладную программу, т. е. начинается циклическое выполнение программы.

i PADT может обслуживать ресурс, например выполнить перезагрузку и инициализацию, если проект, загруженный в ресурс, открыт в SILworX. При отсутствии проекта в SIlworX для ресурса возможен только переход в режим STOP!

HIMA рекомендует после каждой загрузки прикладной программы в систему управления, в том числе и через перезагрузку, сохранять данные проекта, например, на внешнем носителе.

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.

11.2.6 Перезагрузка

Если в прикладную программу вносились изменения, то во время работы их можно перенести в ПЭС. Тогда после проверок операционной системой активируется измененная прикладная программа и берет на себя задачу системы управления.

i **При перезагрузке цепочек шагов учитывайте 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 не остается ни одного шага в состоянии *active.*
- Переименование начального шага, когда активен другой шаг.
  В результате образуется цепочка шагов с двумя активными шагами!

i **При перезагрузке действий учитывайте следующее:**

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

Примеры:

- Удаление таймера — определителя действия 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 определителя действия *P0*, имеющего значение TRUE, запускает триггер.

Перед выполнением перезагрузки операционная система проверяет, не увеличивается ли время цикла текущей прикладной программы за счет необходимых дополнительных задач настолько, что будет превышено установленное время сторожевого устройства. В случае превышения перезагрузка прерывается и появляется сообщение об ошибке, а система управления продолжает работать, используя предыдущую конфигурацию проекта.

Управление может прервать перезагрузку.

Чтобы перезагрузка была успешной, при установке времени сторожевого устройства нужно запланировать резервное время для перезагрузки или ненадолго увеличить время сторожевого устройства системы управления, добавив к нему резервное время.

Временное увеличение времени сторожевого устройства необходимо согласовать с полномочным отделом контроля.

Превышение заданного времени цикла также может привести к обрыву перезагрузки.

Перезагрузка возможна только, если системный параметр *Reload Allowed* установлен на ON, а системная переменная *Reload Deactivation* - на OFF.

В сферу ответственности пользователя входит учет резерва при измерении времени сторожевого устройства. Это должно помочь справиться со следующими ситуациями:

- Колебания времени цикла прикладной программы
- Внезапные сильные нагрузки цикла, напр., в результате коммуникации
- Истечение временных пределов при коммуникации.

Подробнее о времени сторожевого устройства см. в главе 3.2.2.

11.2.7 Online Test

В логике прикладных программ разрешается использовать поля онлайн-теста (поля OLT) для индикации переменных во время работы управления.

Более подробную информацию по использованию полей OLT вы найдете по ключевому слову *OLT Field* в онлайн-справке SILworX и в руководстве Первые шаги (SILworX First Steps Manual HI 801 301 RU).

11.2.8 Режим тестирования

Для поиска ошибок прикладная программа в режиме тестирования может выполняться в пошаговом режиме, т. е. цикл за циклом. Каждый цикл инициируется командой PADT. В промежуток времени между двумя циклами глобальные переменные, описанные в данной прикладной программе, «заморожены». Из-за этого назначенные физические выходы и данные коммуникации перестают реагировать на изменения в процессе!

Данную функцию можно использовать только в случае, когда системный параметр **Test Mode Allowed** для соответствующей прикладной программы имеет значение ON.

Состояние	Значение
OFF	Режим тестирования не доступен (по умолчанию).
ON	Режим тестирования доступен.

Таблица 16: Флажок прикладной программы **Test Mode Allowed**

УКАЗАНИЕ

Возможен сбой безопасной работы!

Если прикладная программа остановлена в режиме тестирования, она не может безопасно реагировать на входы и управлять выходами! Значения выходов в этом состоянии не могут изменяться.

Поэтому режим тестирования не допускается для безопасной эксплуатации!

Параметр Test Mode Allowed **для работы в безопасном режиме должен иметь значение OFF!**

11.2.9 Изменение системных параметров в режиме онлайн

Системные параметры, которые представляет Таблица 17, могут быть изменены в управлении в режиме онлайн.
Типичным случаем применения является увеличение времени сторожевого устройства на период проведения перезагрузки.

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

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!

Система управления не позволяет установить для времени сторожевого устройства значение меньше, чем значение времени сторожевого устройства, используемое в конфигурации, загруженной в ПЭС.

Параметр	Значения, изменяемые в данном состоянии ПЭС
System ID	STOP
Watchdog Time (Время сторожевого устройства ресурса)	RUN, STOP/VALID CONFIGURATION
Safety Time	RUN, STOP/VALID CONFIGURATION
Target Cycle Time	RUN, STOP/VALID CONFIGURATION
Target Cycle Time Mode	RUN, STOP/VALID CONFIGURATION
Allow Online Settings	ON->OFF: все OFF->ON: STOP
Autostart	все
Start Allowed	все
Load Allowed	все
Reload Allowed	все
Global Forcing Allowed	все
Global Force Timeout Reaction	все

Таблица 17: Параметры, изменяемые онлайн

Изменить системные параметры во время работы возможно также и с помощью перезагрузки.

11.2.10 Документация программы для безопасных случаев применения

Система программирования SILworX 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

Документация является составляющей частью функциональной приемки установки отделом контроля, требующей разрешения (напр., TÜV).

11.2.11 Multitasking

Многозадачностью называется способность системы HIMax обрабатывать с помощью процессорного модуля до 32 прикладных программ.

Отдельные прикладные программы можно запускать и останавливать независимо друг от друга.

Цикл прикладной программы может длиться в течение нескольких циклов процессорного модуля. Это регулируется параметрами ресурса и прикладной программы. На основе этих параметров SILworX рассчитывает время сторожевого устройства прикладной программы:
Watchdog time$_{\text{user program}}$ = *watchdog time*$_{\text{processor module}}$ * *maximum number of cycles* (Время сторожевого устройства прикладной программы = Время сторожевого устройства процессорного модуля * Максимальное количество циклов)

Отдельные прикладные программы выполняются в общем и целом без обратного воздействия. Однако возможно и взаимное влияние, связанное со следующими причинами:

- Применение одной глобальной переменной в нескольких прикладных программах.
- Незапланированно длинные сроки протекания отдельных прикладных программ, если ограничение не было задано 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 как минимум на один цикл процессорного модуля. В крайнем случае это может произойти через 32 цикла процессорного модуля. Поэтому время реакции на изменения таких глобальных переменных соответственно увеличивается!

УКАЗАНИЕ

Возможно взаимное влияние прикладных программ!

Из-за применения одной глобальной переменной в нескольких прикладных программах может возникнуть взаимное влияние прикладных программ, приводящее к различным последствиям.

- **Поэтому необходимо точно планировать использование одной глобальной переменной в нескольких прикладных программах.**
- **Используйте функцию Cross-Reference in Column редактора глобальных переменных SILworX Editor, чтобы проверять использование 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 системе (HIMax System Manual HI 801 060 RU)

11.2.12 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.

11.3 Контрольный перечень по созданию прикладной программы

HIMA рекомендует использовать имеющийся контрольный перечень для соблюдения аспектов безопасности в ходе программирования, перед загрузкой новой или измененной программы, а также после нее. Контрольные перечни предназначены для использования в качестве документации по планированию, но они также служат для подтверждения добросовестно выполненного планирования.

Контрольные перечни можно найти на веб-сайте компании HIMA в формате Microsoft® Word®.

12 Конфигурацию связи

Наряду с физическими входными и выходными переменными возможен также обмен значениями переменных с другой системой через канал передачи данных. Для этого переменные описываются посредством системы программирования SILworX в области протоколов соответствующего ресурса.

12.1 Стандартные протоколы

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

⚠ ПРЕДУПРЕЖДЕНИЕ

Использование ненадежных данных импорта может привести к телесным повреждениям!

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

Предлагаются следующие стандартные протоколы:

- Для интерфейсов Ethernet модуля связи:
  - Modbus TCP (ведущее/ведомое устройство)
  - Modbus резервный (ведомое устройство).
  - SNTP
  - Send/Receive TCP
  - PROFINET-IO (контроллер, устройство).
- К интерфейсам полевой шины (RS485) модуля связи в зависимости от исполнения устройства
  - Modbus (ведущее/ведомое устройство).
  - Modbus резервный (ведомое устройство).
  - PROFIBUS-DP (ведущее/ведомое устройство).

12.2 Безопасный протокол safe**ethernet**

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

Более подробную информацию по safe**ethernet** см. в руководстве по связи (Communication Manual HI 801 162 RU).

УКАЗАНИЕ

Возможен непреднамеренный переход в безопасное состояние!

***Receive Timeout* является безопасным параметром!**

Receive Timeout (время ожидания приема) является временем контроля на ПЭС 1, в течение которого должен быть принят корректный ответ от ПЭС 2.

i Время ожидания приема (Receive Timeout) действительно также в обратном направлении от ПЭС 2 к ПЭС 1.

Если по истечении времени ожидания приема *Receive Timeout* действительный ответ от партнера по коммуникации не поступает, HIMax завершает безопасную коммуникацию. 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**.

i Допускается подстановка в следующих вычислениях максимального времени реакции (Worst Case Reaction Time*)* значения заданного времени цикла вместо времени сторожевого устройства, если выбран режим заданного времени цикла *Fixed* или *Fixed-tolerant*.

12.3 Максимальное время реакции для safeethernet

На следующих примерах формулы для расчета максимальной времени реакции в случае соединения с системами управления HIMatrix действительны только в том случае, если настроено безопасное время = 2 * время сторожевого устройства. Для систем управления HIMax эти формулы действительны всегда.

i Максимально допустимое время реакции зависит от процесса и должно быть согласовано с отделом контроля, ответственным за приемку.

Понятия:

Receive Timeout (Время ожидания приема):	Время контроля в ПЭС 1, в течение которого должен приниматься действительный ответ от ПЭС 2. В противном случае по истечении времени безопасная связь завершается.
Production Rate	Минимальный интервал между двумя передачами данных.
Watchdog Time (Время сторожевого устройства):	Максимально разрешенная продолжительность цикла RUN в системе управления. Продолжительность цикла RUN зависит от степени сложности прикладной программы и количества соединений safeethernet. Время сторожевого устройства (WDT) вводится в диалоговом окне «Свойства ресурса».
Worst Case Reaction Time (Максимальное время реакции)	Максимальное время реакции для передачи изменения сигнала физического входа (In) ПЭС 1 до изменения физического выхода (Out) ПЭС 2.
Delay:	Задержка в канале передачи, например, при соединении через модем или спутник. При прямой связи можно изначально считать задержку равной 2 мс. Фактическая задержка в канале передачи вычисляется ответственным системным администратором.

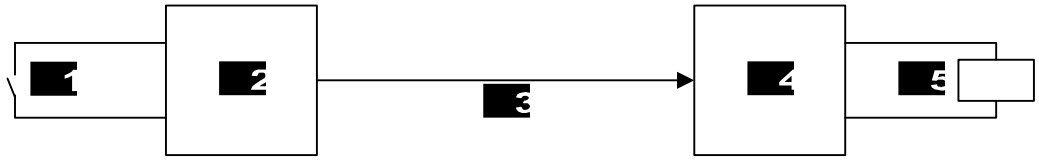
Для следующих расчетов максимально допустимого времени реакции силу имеют следующие условия:

- Сигналы, которые передаются через safe**ethernet,** должны обрабатываться соответствующими системами управления в рамках одного цикла ЦПУ.
- Следует, кроме того, прибавить время реакции датчиков и исполнительных элементов.

Расчеты действительны также для сигналов в противоположном направлении.

12.3.1 Вычисление максимального времени реакции двух систем управления HIMax

Максимальное время реакции T_R (Worst Case) от замены датчика управления 1 (In) до реакции выхода (Out) управления 2 рассчитывается следующим образом:



1 Вход
2 HIMax, система управления 1
3 Безопасный протокол
4 HIMax, система управления 2
5 Выход

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

$T_R = t_1 + t_2 + t_3$

T_R Максимальное время реакции (Worst Case Reaction Time)

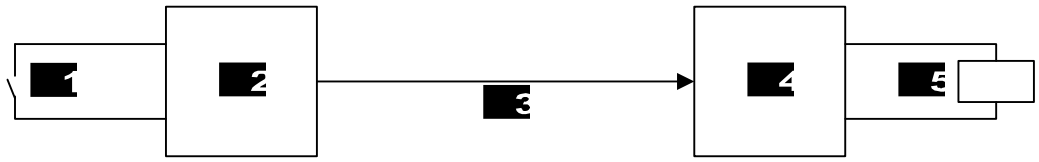
t_1 Безопасное время системы управления 1 HIMax

t_2 *Время ожидания приема (Receive Timeout)*

t_3 Безопасное время Системы управления 2 HIMax

12.3.2 Расчет макс. времени реакции в соединении с ПЭС HIMatrix

Максимальное время реакции T_R (Worst Case) от замены датчика управления 1 (In) в системе управлении HIMax до реакции выхода (Out) управления 2 HIMatrix рассчитывается следующим образом:



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

Рис. 5: Время реакции при соединении системы HIMax с управлением HIMatrix

$T_R = t_1 + t_2 + t_3$

T_R Максимальное время реакции (Worst Case Reaction Time)

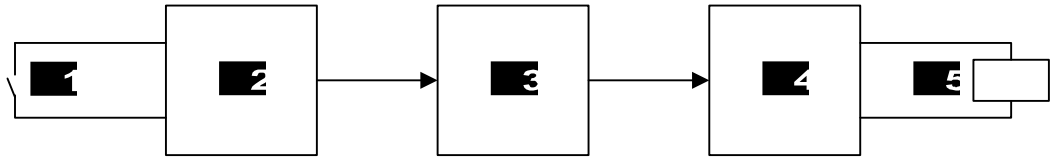
t_1 Безопасное время системы управления HIMax

t_2 *Время ожидания приема (Receive Timeout)*

t_3 2 * Время сторожевого устройства системы управления HIMatrix

12.3.3 Расчет макс. времени реакции с двумя системами управления HIMatrix или удаленными устройствами ввода/вывода

Рассчитайте максимальное время реакции T_R (Worst Case) от смены датчика (In) в первой системе управления HIMatrix или в Remote I/O (удаленном устройстве ввода/вывода) (напр., F3 DIO 20/8 01) до реакции вывода во второй системе управления HIMatrix или в устройстве удаленного ввода/вывода (Out), как показано далее:



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

Рис. 6: Время реакции с двумя системами управления HIMax/устройством удаленного ввода/вывода и одной системой управления HIMatrix

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

T_R Максимальное время реакции (Worst Case Reaction Time)

t_1 2 * Время сторожевого устройства системы управления HIMatrix/устройства удаленного ввода/вывода 1

t_2 *Receive Timeout 1*

t_3 2 * Время сторожевого устройства системы управления HIMatrix

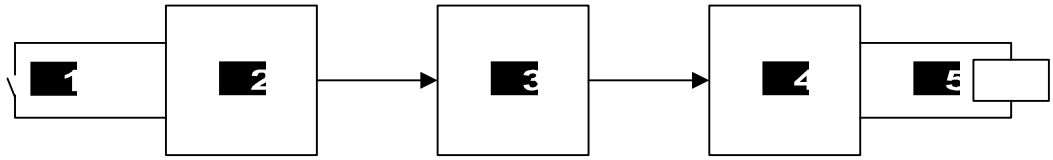
t_4 *Receive Timeout 2*

t_5 2 * Время сторожевого устройства Системы Управления HIMatrix/устройства удаленного ввода/вывода 2

i Оба удаленных устройства 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.

12.3.4 Расчет максимального времени реакции HIMax и одной системы управления HIMatrix

Максимальное время реакции T_R (Worst Case) от замены датчика (In) управления 1 до реакции выхода (Out) системы управления 2 HIMax рассчитывается следующим образом:



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

Рис. 7: Время реакции с двумя системами управления HIMax и одной системой управления HIMatrix

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

T_R Максимальное время реакции (Worst Case Reaction Time)

t_1 Безопасное время системы управления 1 HIMax

t_2 *Receive Timeout 1*

t_3 2 * Время сторожевого устройства системы управления HIMatrix

t_4 *Receive Timeout 2*

t_5 Безопасное время Системы управления 2 HIMax

i Системы управления 1 и 2 HIMax могут быть идентичными.

В качестве системы управления HIMatrix может использоваться и система управления HIMax.

12.4 Безопасный протокол PROFIsafe

Требования по использованию протокола PROFIsafe изложены в руководстве по связи (Communication Manual HI 801 062 RU). Соблюдайте требования.

Формулы для расчета времени реакции см. также в руководстве по связи.

13 Использование в приемно-контрольных приборах пожарной сигнализации

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

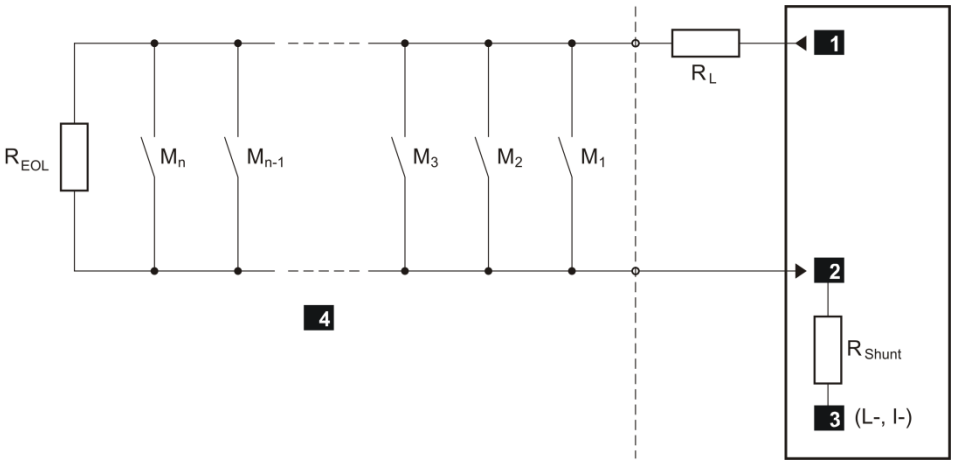
Для этого необходимо, чтобы прикладная программа отвечала функциональным требованиям для приемно-контрольных приборов пожарной сигнализации согласно указанным стандартам.

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 оставаться в состоянии сообщения о неисправности в течение 100 секунд после поступления сообщения о неисправности в систему HIMax.

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 входных модулей с контролем линии
- цифровые и аналоговые выходы выходных модулей с контролем линии



1 Питание датчика
2 Аналоговый вход
3 Минус выходного сигнала
4 Сигнальный контур

M Пожарный извещатель
R_{EOL} Нагрузочное сопротивление на последнем датчике контура
R_L Ограничение максимального тока контура
R_{Shunt} Измерительное сопротивление (см. руководство по модулям)

Рис. 8: 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. Для этого нужно выполнить настройку контроля линии для выходных модулей и обработать в прикладной программе.

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 HIMax на внешнюю систему может быть реализована с помощью имеющегося стандарта связи Ethernet (OPC). О сбое связи необходимо сообщить.

Системы HIMax, 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 переменные, определенные в прикладной программе. Это позволяет программировать сигнализацию неисправностей на распознаваемые системой ошибки. В случае сбоя система HIMax отключает безопасные входы и выходы, что приводит к следующему:

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

Приложение

Глоссарий

Обозначение	Описание
ARP	Address resolution protocol, сетевой протокол для распределения сетевых адресов по адресам аппаратного обеспечения
AI	Analog input, аналоговый вход
AO	Analog output, аналоговый выход
Плата сопряжения	Плата сопряжения для модуля HIMax
COM	Коммуникационный модуль
CRC	Cyclic redundancy check, контрольная сумма
DI	Digital input, цифровой вход
DO	Digital output, цифровой выход
EMC, ЭМС	Electromagnetic compatibility, электромагнитная совместимость
EN	Европейские нормы
ESD	Electrostatic discharge, электростатическая разгрузка
FB	Fieldbus, полевая шина
FBD	Function block diagrams, Функциональные Блоковые Диаграммы
FTT	Fault tolerance time, время допустимой погрешности
ICMP	Internet control message protocol, сетевой протокол для сообщений о статусе и неисправностях
IEC	Международные нормы по электротехнике
Адрес MAC	Адрес аппаратного обеспечения сетевого подключения (media access control)
PADT	Programming and debugging tool, инструмент программирования и отладки (согласно IEC 61131-3), PC с SILworX
PE	Protective earth, защитное заземление
PELV, ЗСНН	Protective extra low voltage, функциональное пониженное напряжение с безопасным размыканием
PES, ПЭС	Programmable electronic system, программируемая электронная система
R	Read
Rack ID	Идентификация основного носителя (номер)
однонаправленный	Если к одному и тому же источнику (напр., трансмиттеру) подключены два входных контура. В этом случае входной контур обозначается как контур «без реактивного воздействия», если он не искажает сигналы другого входного контуры.
R/W	Read/Write
SB	Модуль системной шины
SELV, БСНН	Safety extra low voltage, защитное пониженное напряжение
SFF	Safe failure fraction, доля безопасных сбоев
SIL	Safety integrity level, уровень совокупной безопасности (согл. IEC 61508)
SILworX	Инструмент программирования для HIMax
SNTP	Simple network time protocol, простой сетевой протокол времени (RFC 1769)
SRS	System rack slot, адресация модуля
SP	Software, программное обеспечение
TMO	Timeout, время ожидания
W	Write
w_S	Максимальное значение общих составляющих переменного напряжения
Watchdog (WD)	Контроль времени для модулей или программ. При превышении показателя контрольного времени модуль или программа выполняют контрольный останов.
WDT	Watchdog time, время сторожевого устройства

Перечень изображений

Перечень таблиц

Индекс

HI 801 061 RU

Albert-Bassermann-Str. 28
68782 Brühl, Deutschland
Тел. +49 6202 709 0
Факс +49 6202 709 107
HIMax-info@hima.com
www.hima.com

HIMA

SAFETY
NONSTOP