HIQuad

Безопасная система управления

Руководство по безопасности

HIQuad

SAFETY
NONSTOP

HIMA

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 непосредственно в компанию HIMA. Фирма HIMA с благодарностью принимает предложения по внесению в руководство необходимой дополнительной информации.

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

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

Контакты

Адрес компании HIMA:

HIMA Paul Hildebrandt GmbH

Postfach 1261

68777 Brühl, Germany

Тел.: +49-6202-709-0

Факс: +49-6202-709-107

Эл. почта: info@hima.com

Оригинал на немецком языке	Описание
HI 800 012 D, Rev. 1.01 (1547)	Перевод на русский язык с немецкого оригинала

Содержание

1 Введение

Данное руководство содержит информацию по использованию безопасных устройств автоматизации HIMA H41q и H51q по назначению.

Чтобы обеспечить безопасность установки, ввода в эксплуатацию, а также эксплуатации и текущего ремонта устройств автоматизации H41q/H51q, 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 системе неквалифицированных сотрудников.
- При отключении функций безопасности или при их обходе (функция «байпас»).
- При несоблюдении указаний данного руководства.

Компания HIMA разрабатывает, производит и проверяет устройства автоматизации H41q/H51q при соблюдении соответствующих норм безопасности. Использование системы допускается только при выполнении всех следующих условий:

- применение относится к случаям, предусмотренным в описаниях
- условия окружающей среды соответствуют указанным в руководстве
- подключены только допущенные внешние устройства

Из соображений наглядности данное руководство не содержит полной информации по всем вариантам исполнения устройств автоматизации H41q/H51q.

1.1 Действительность и актуальность

Новейшее издание руководства по безопасности имеет силу также и для более ранних версий операционной системы. Особенности отдельных версий упомянуты в тексте.

Новейшее издание доступно на веб-сайтах www.hima.de и www.hima.com.

Обширные изменения руководства обозначены новым статусом состояния на момент правки, менее обширные — новым статусом издания. Статус состояния указан на передней стороне, за номером документа, статус издания — на задней стороне.

1.2 Целевая аудитория

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

1.3 Оформление текста

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

Полужирный шрифт	Выделение важных частей текста Маркировка кнопок управления, пунктов меню и вкладок в SILworX, по которым можно щелкнуть мышкой.
Курсив	Параметры и системные переменные
`Шрифт Courier`	Текст, вводимый пользователем
RUN	Обозначения режимов работы заглавными буквами
Гл. 1.2.3	Сноски оформлены как гиперссылки, хотя могут и не иметь особой маркировки. При наведении на них указателя мыши его форма меняется. При щелчке по ссылке происходит переход к соответствующему месту в документе.

Указания по безопасности и применению выделены особым образом.

1.3.1 Указания по безопасности

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

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

⚠ СИГНАЛЬНОЕ СЛОВО

Вид и источник риска!

Последствия несоблюдения указаний

Избежание риска

Значение сигнальных слов

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

ПРИМЕЧАНИЯ

Вид и источник ущерба!

Избежание ущерба

1.3.2 Указания по применению

Дополнительная информация представлена следующим образом:

i В этом месте приводится дополнительная информация.

Полезные советы и рекомендации представлены в следующей форме:

РЕКОМЕНДАЦИЯ В этом месте расположен текст рекомендации.

1.4 Остаточный риск

Непосредственно сама система H41q/H51q опасности не представляет.

Остаточный риск может возникать в результате:

- Ошибок при проектировании
- Ошибок в прикладной программе
- Ошибок подключения

2 Указания по использованию систем H41q/H51q

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

2.1 Применение по назначению

2.1.1 Область применения

Безопасные устройства автоматизации H41q и H51q используются до уровня совокупной безопасности 3 (IEC 61508), либо для категории безопасности 4 и уровня производительности Pl e (ISO 13849-1).

Все модули ввода/вывода могут использоваться как для резервного, так и для одноканального исполнения центральных модулей.

При использовании безопасной коммуникации между различными системами необходимо следить за тем, чтобы общее время реакции системы не превышалось. Необходимо использовать приведенные в руководство по безопасности (HIQuad Safety Manual HI 803 077 RU) основы расчета

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

Системы H41q/H51q имеют соответствующие сертификаты для систем управления процессом, систем защиты, камер сгорания и систем управления машинами.

2.1.1.1 Применение в соответствии с принципом тока покоя

Устройства автоматизации созданы для применения по принципу тока покоя.

Система, работающая по принципу тока покоя, не нуждается в энергии для выполнения функции безопасности (**de-energize-to-trip**).

Таким образом, в качестве безопасного состояния в случае ошибки для входных и выходных сигналов принимается обесточенное состояние или состояние без напряжения.

2.1.1.2 Применение в соответствии с принципом рабочего тока

Системы управления H41q/H51q могут использоваться согласно принципу рабочего тока.

Система, работающая по принципу рабочего тока, нуждается в энергии, например, электрической или пневматической, для выполнения функции обеспечения безопасности (**energize-to-trip**).

Для этого системы управления H41q/H51q прошли проверку и имеют сертификаты согласно EN 54 и NFPA 72 для использования в установках пожарной сигнализации и системах пожаротушения. В этих системах требуется, чтобы по требованию для устранения опасности принималось активное состояние.

2.1.1.3 Взрывозащита

Безопасные устройства автоматизации H41q и H51q подходят для установки в зоне 2. Соответствующие декларации о соответствии содержатся в технических паспортах.

Следует соблюдать нижеприведенные условия использования!

2.1.1.4 Использование в приемно-контрольных приборах пожарной сигнализации

Все системы H41q/H51q с аналоговыми входами могут использоваться для приемно-контрольных приборов пожарной сигнализации согласно DIN EN 54-2 и NFPA 72.

Следует соблюдать нижеприведенные условия использования!

2.1.2 Ненадлежащее использование

Передача релевантных для безопасности данных через открытые сети (напр., интернет) не допускается без принятия дополнительных мер для повышения уровня безопасности (напр., туннель VPN, сетевое устройство защиты, и т.д.).

С помощью интерфейсов полевых шин невозможно создать безопасную связь без безопасных протоколов полевых шин.

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 H41q/H51q в автоматических установках и комплексах.

Правильное программирование систем H41q/H51q должно быть соответствующим образом утверждено изготовителями машин и установок.

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.

ПРИМЕЧАНИЯ

Электростатический разряд!

Несоблюдение указаний может привести к повреждению электронных деталей.

- **Перед работой с компонентами HIMA следует дотронуться до заземленного объекта.**
- **Следует использовать рабочие места с антистатическим оснащением и носить заземляющую ленту.**
- **При неиспользовании следует хранить систему с обеспечением антистатической защиты, например в упаковке.**

Изменения или расширения в проводке системы могут выполняться только персоналом, ознакомленным с мерами защиты от электростатического разряда.

3 Концепция безопасности для применения ПЭС

3.1 Безопасность и готовность

Благодаря микропроцессорной структуре 1oo2D на центральном модуле серии систем H41q и H51q даже в виде моносистем рассчитаны на уровень совокупной безопасности до SIL 3.

В зависимости от требуемого уровня готовности автоматизированные системы HIMA в центральной области и области вводов/выводов могут быть оснащены резервными модулями. Резервные модули повышают готовность, так как в случае неисправности одного модуля он автоматически выводится из эксплуатации, а резервный модуль поддерживает работу без разрыва.

3.1.1 Безопасность

Для безопасных систем H41q и H51q согласно IEC 61508 были выполнены расчеты PFD (Probability of Failure on Demand) и PFH (Probability of Failure per Hour).

IEC 61508-1 задает для уровня совокупной безопасности 3 следующие диапазоны:

- PFD 10^{-4}...10^{-3}
- PFH 10^{-8}...10^{-7} в час

Для системы управления принимаются 15% предельного значения от стандарта для PFD и PFH. Отсюда получаются как предельные значения для доли системы управления

- PFD = 1,5 10^{-4}
- PFH = 1,5 10^{-8} в час

Интервал повторной проверки для безопасных систем H41q и H51q составляет 10 лет1.

Функции безопасности, состоящие из безопасного контура (вход, обрабатывающее устройство и выход), во всех комбинациях соответствуют требованиям.

Более подробная информация предоставляется по запросу.

3.1.2 Обзор

В следующей таблице представлен обзор наименований систем, безопасности, готовности и конфигураций системы

Наименование системы	H41q-MS H51q MS	H41q-HS H51q HS	H41q-HRS H51q HRS
SIL / Категория	SIL 3 / Кат. 4	SIL 3 / Кат. 4	SIL 3 / Кат. 4
Безотказность	В норме	Высокий	Очень высокий
Конфигурация			
Центральный модуль	моно	резервный	резервный
Модули ввода/вывода	моно [1)]	моно [1)]	резервный
Шина ввода/вывода	моно	моно	резервный [2)]

1) Отдельные модули ввода/вывода для повышения готовности можно применять также как резервные или в схеме выбора 2oo3 (например, см. главу 7.8.3)

2) Компания HIMA рекомендует для резервной шины ввода/вывода по возможности использовать в качестве резервных не только модули ввода/вывода, но и периферийное оборудование (датчики и исполнительные механизмы в установке). Данные конструкции в целом имеют более высокую интенсивность отказа, чем модули ПЭС.

Таблица 1: Наименования систем, безопасность, готовность и конфигурации систем

[1] Ограничения для релейного модуля F 3430, см. главу 6.5

Для повышения готовности посредством резервных модулей имеют значение три пункта:

- Неисправные модули необходимо распознавать и отключать, чтобы они не блокировали систему.
- Оператор в случае ошибки должен получать сообщение для замены модулей.
- После замены модуля его необходимо автоматически вводить в эксплуатацию.

Автоматизированные системы HIMA в соответствующих конфигурациях выполняют данные требования.

Для программирования систем используется PADT (программирующее устройство, ПК) с инструментом программирования **ELOP II** согласно IEC 61131-3. Этот инструмент помогает при создании безопасных программ и в управлении устройствами автоматизации.

3.2 Безопасное время

Отдельные неисправности, которые могут привести к опасному рабочему состоянию, распознаются устройствами самодиагностики в течение безопасного времени (≥ 1 с).

- Безопасное время процесса

  Техническая характеристика, которая в директивах для пользователя часто обозначается как безопасное время.
- Безопасное время (в ПЭС)

  Величина, зависящая от возможностей системы

  Отказы, которые могут оказать критическое для безопасности воздействие только в комбинации с дополнительными ошибками, распознаются с помощью проверок.

  В отношении проверок различают:
  - Проверки в течение безопасного времени

    Проводятся в течение безопасного времени (приоритетные проверки);

    Время реакции: немедленно, не позднее, чем в течение безопасного времени.
  - Фоновые проверки

    Разделены на несколько циклов,

    Реакция при распознавании ошибки следует немедленно, не позднее, чем в течение времени, в 3600 раз превышающего значение безопасного времени.

  Пример времени реакции: максимум двукратное время цикла. Если для процесса требуется безопасное время 1 с, время цикла не должно превышать 500 мс.
- Время реакции на ошибку

  Время реакции на ошибку устройства автоматизации соответствует безопасному времени (≥ 1 с), которое задается в свойствах ресурса. При этом необходимо учитывать, чтобы время цикла составляло не больше половины безопасного времени, так как реакция на ошибки в модулях ввода происходит в течение макс. 2 циклов. На время цикла оказывает влияние безопасное время, определяющее промежуток времени, в котором выполняются все приоритетные проверки.

  Короткое безопасное время увеличивает время цикла, и наоборот. При продолжительном безопасном времени некоторые проверки распределяются на несколько циклов.
  - Пример 1: безопасное время = 1 с

    Время цикла в прикладной программе = 450 мс

    Требуемое время для проверок = 100 мс

    в течение безопасного времени возможно 2 цикла

    100 мс/2 = 50 мс/время цикла, требуемое для проверок

    Общее время цикла = **500 мс**

- Пример 2: безопасное время = 2 с
  Время цикла в прикладной программе = 450 мс
  Требуемое время для проверок = 100 мс
  в течение безопасного времени возможно 4 цикла
  100 мс/4 = 25 мс/время цикла, требуемое для проверок
  Общее время цикла = **475 мс**

i Для выходных сигналов операционной системы до (07.14) значение 255 с для безопасного времени **не** разрешено! Допустим только диапазон значений 1…254 с!

3.3 Повторная проверка

Повторные проверки распознают скрытые опасные ошибки, которые иначе могли бы отрицательно сказываться на безопасности работы установки.

Системы безопасности HIMA должны подвергаться повторной **проверке с интервалом в 10 лет**[2]. Интервал этот нередко можно и продлить, если анализировать реализованные цепи безопасности с использованием инструмента расчета.

Повторную проверку реле в релейных модулях необходимо осуществлять через интервалы времени, определенные для установки.

3.3.1 Выполнение повторной проверки

Выполнение повторной проверки зависит от следующих моментов:

- Состояние установки (EUC = equipment under control)
- Потенциал опасности установки
- стандарты, применяемые для эксплуатации установки и используемые уполномоченным отделом технического контроля в качестве основания для выдачи разрешения

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

3.3.2 Частота повторных проверок

ПЭС HIMA 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 HIMA. Если пользователь проверяет всю цепь безопасности из-за полевого устройства, то система управления HIMA автоматически включается в эту проверку. В этом случае для системы управления HIMA не требуется никаких дополнительных повторных проверок.

Если повторная проверка полевых устройств не включает в себя систему управления HIMA, то ее следует проверять не реже одного раза в 10 лет. Этого можно добиться, перезапустив систему управления HIMA.

Дополнительные требования к повторной проверке определенных модулей описаны в техническом паспорте соответствующего модуля.

[2] Исключение: модуль F 3430 для уровня совокупной безопасности 3 следует проверять с интерваffлов в 5 лет

3.4 Требования безопасности

При использовании безопасных систем управления H41q и H51q действуют следующие требования безопасности:

i За безопасность эксплуатации установки в соответствии с действующими стандартами использования ответственность несет эксплуатирующая организация.

3.4.1 Проектирование аппаратного обеспечения: требования, не зависящие от изделия

В целях безопасной эксплуатации должны использоваться только допущенные для этого безопасные модули аппаратного обеспечения и компоненты программного обеспечения. Допущенные модули аппаратного обеспечения и компоненты ПО перечислены в *Revision List of Devices and Firmware of H41q/H51q Systems of HIMA Paul Hildebrandt GmbH*.

Номер сертификата см. в последнем действительном выпуске документа. Соответственно текущие номера версий содержатся в списке версий, составляемом совместно с отделом контроля.

- Необходимо соблюдать указанные условия использования (см. главу 3.5.1) в отношении ЭМС, а также механических, климатических воздействий.
- Небезопасные, но не вызывающие реактивного воздействия модули АО и компоненты ПО могут использоваться для обработки небезопасных сигналов, однако они не должны использоваться для обработки задач с учетом сохранения функции безопасности.

3.4.2 Проектирование аппаратного обеспечения: требования, зависящие от изделия

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

3.4.3 Программирование: требования, не зависящие от изделия

- В безопасных приложениях необходимо следить за правильным параметрированием системных величин, влияющих на безопасность. Возможные варианты параметрирования описаны в следующих главах. Особое внимание следует уделить определению конфигурации системы, максимального времени цикла и безопасного времени.

3.4.4 Программирование: требования, зависящие от изделия

- Реакция системы на ошибку в безопасных модулях ввода и вывода должна быть определена прикладной программой согласно условиям сохранения функции безопасности для конкретной установки.
- При использовании инструмента программирования ELOP II, начиная с версии 3.5, можно упростить верификацию составленной программы в соответствии с предписаниями настоящего руководства по безопасности.
- Тем не менее, должен производиться достаточный текущий контроль программы.
- Функциональные проверки/верификация после изменения приложения могут ограничиваться измененными разделами программы.
- Необходимо соблюдать описанный в главе 7 порядок действий при составлении программы и ее изменении.

3.4.5 Связь: требования, зависящие от изделия

- При настройке безопасной коммуникации между различными системами необходимо следить за тем, чтобы общее время реакции системы не превышало безопасное время процесса. Необходимо использовать приведенные основы расчета.
- Передача данных, связанных с безопасностью, в сетях общего пользования (например, Интернет) разрешена только при соблюдении дополнительных мер безопасности, таких как использование VPN-канала.
- Если передача данных осуществляется по внутренним сетям организации/предприятия, то следует посредством административных или технических мер обеспечить достаточный уровень защиты от манипулирования (например, отделением части сети, релевантной для безопасности, от других сетей посредством межсетевого экрана).
- К коммуникационным интерфейсам можно подключать только те устройства, которые обеспечивают безопасное электрическое разделение.

3.4.6 Особые режимы работы: требования, не зависящие от изделия

- Перезагрузка в безопасных применениях допускается только после согласования с отделом контроля, ответственным за приемку установки, и с помощью сертифицированного инструмента ELOP II.
- Во время всего процесса перезагрузки ответственное лицо должно обеспечивать контроль процесса с учетом сохранения функции безопасности посредством прочих технических и организационных мер.
- Перед каждой перезагрузкой необходимо с помощью модуля сравнения C-кодов из ELOP II определить изменения версии по сравнению с работающей прикладной программы.
- При перезагрузке моно-ПЭС продолжительность всего изменения, включая двойное время цикла, не должна превышать безопасное время процесса.
- С помощью ELOP II возможна статическая проверка логики в режиме офлайн. Офлайн-моделирование не подвергалось проверке безопасности. Поэтому моделирование не может заменить функциональную проверку.
- В случае необходимости эксплуатирующее предприятие по согласованию с приемочным органом, ответственным за применение, должно определить административные меры для защиты системы управления от доступа.

3.4.7 Информационная безопасность систем HIQuad

Промышленные системы управления должны 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 HIQuad состоит из следующих компонентов, подлежащих защите:

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

Даже с настройками по умолчанию HIQuad уже является системой, соответствующей требованиям информационной безопасности (безопасности информационных технологий).

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.
- В ПЭС системные параметры регулируются таким образом, что изменение программы возможно только посредством перезагрузки.
- 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.

  Для технического обслуживания или диагностики PADT можно подсоединять на короткое время.

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.

⚠ 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!**

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

- Целесообразная классификация 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

Рекомендуется регулярно (например, раз в год) проверять меры безопасности.

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

Безопасные устройства автоматизации (ПЭС = программируемая электронная система) серий систем H41q и H51q сертифицированы следующим образом:

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

Сертификат и отчет об испытаниях

Безопасные устройства автоматизации

H41q-MS, H41q-HS, H41q-HRS

H51q MS, H51q HS, H51q HRS

Функциональная безопасность безопасных устройств автоматизации серий систем H41q и H51q проверена и сертифицирована в соответствии с перечисленными важными стандартами:

IEC 61508, Parts 1-7: 2010	до SIL 3
IEC 61511, Parts 1-3: 2015	до SIL 3
EN/ISO 13849-1: 2008 + AC: 2015	Кате. 4, уровень производительности e (PL e)
EN 50156-1: 2005	
EN 12067-2: 2004, EN 298: 2012	
NFPA 85: 2015, NFPA 86: 2015	
EN 61131-2: 2007	
EN 61000-6-2: 2005, EN 61000-6-4: 2007	
EN 54-2:1997, A1: 2007, NFPA 72: 2016	
EN 50130-4: 2011 + A1: 2014	

Глава 2.3 содержит подробный список всех проведенных испытаний на воздействие внешних условий и проверок электромагнитной совместимости.

3.5.1 Условия испытаний

3.5.1.1 Условия окружающей среды и технические характеристики

При использовании безопасных систем управления H41q/H51q необходимо соблюдать следующие общие условия:

Условия	Содержание условия
Класс защиты	Класс защиты II согл. IEC/EN 61131-2
Рабочая температура	Рабочая температура: 0...+60 °C
Температура хранения	Температура хранения: от -40...+80 °C (с батареей только -30...+75 °C)
Степень загрязнения	Степень загрязнения II
Высота установки	< 2000 м
Корпус	Стандарт: IP20 Если того требуют соответствующие стандарты применения (напр., EN 60204), систему необходимо встраивать в корпус с необходимой степенью защиты (напр., IP54).
Входное напряжение блока питания	24 В пост. тока

Таблица 2: Условия окружающей среды

Различные отклонения см. в соответствующем техническом паспорте.

Безопасные системы управления H41q/H51q были разработаны в соответствии со следующими нормами ЭМС, климатическими и экологическими требованиями.

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

Таблица 3: Стандарты

3.5.1.2 Климатические испытания

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

IEC/EN 61131-2	Климатические испытания
	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 4: Климатические условия

3.5.1.3 Механические испытания

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

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

Таблица 5: Механические испытания

3.5.1.4 Испытания по электромагнитной совместимости

Соблюдаемые условия проверки см. в декларации ЕС о соответствии.

Все модули систем H41q и H51q отвечают директиве EMC Европейского союза и имеют маркировку CE.

При воздействии помех выше указанных границ системы безопасно реагируют.

3.5.1.5 Электропитание

Наиболее важные испытания и предельные значения для условий электропитания перечислены в таблице ниже.

IEC/EN 61131-2:	Дополнительная проверка характеристик подачи постоянного напряжения
	Блок питания должен соответствовать одному из следующих стандартов: ▪ IEC 61131-2 или ▪ БСНН (защитное пониженное напряжение, EN 60950) или ▪ ЗСНН (пониженное напряжение с безопасным размыканием, EN 60742)
	Защита систем H41q/H51q предохранителем должна осуществляться согласно данным, содержащимся в технических паспортах
	Проверка диапазона напряжений: 24 В пост. тока, -20...+25 % (19,2...30,0 В пост. тока)
	Испытание на устойчивость к кратковременным прерываниям внешнего электропитания: DC, PS 2: 10 мс
	Изменение полярности питающего напряжения: См. указание в соответствующей главе каталога или в техническом паспорте модуля блока питания
	Буферная батарея, испытания на стойкость Испытание B, 1000 ч, литиевая батарея в качестве буферной батареи

Таблица 6: Дополнительная проверка характеристик подачи постоянного напряжения

4 Центральные модули

Необходимые центральные компоненты для различных исполнений устройств автоматизации объединены в блоки. Соответствующий блок работоспособного центрального устройства состоит из следующих элементов:

- Каркас для центральных модулей
- Центральные модули
- Блоки питания
- Принадлежности

Точный объем, а также подключение питающего напряжения и присоединение уровня ввода/вывода см. в технических паспортах в каталоге программируемые системы(HIQuad Product Catalog, HI 800 263 E)

4.1 Центральные модули и блоки для систем H41q

Модуль/блок	Обозначение	Безопасный	без обратного воздействия на источник
F 8652X	Центральный модуль, сдвоенный процессор 1oo2	•	•
B 4235	Блок центрального устройства H41q-MS	•	•
B 4237-1	Блок центрального устройства H41q-HS	•	•
B 4237-2	Блок центрального устройства H41q-HRS	•	•

Таблица 7: Центральные модули и блоки для системы H41q

4.2 Центральные модули и блоки для системы H51q

Модуль/блок	Обозначение	Безопасный	без обратного воздействия на источник
F 8650X	Центральный модуль, сдвоенный процессор 1oo2	•	•
B 5231	Блок центрального устройства H51q MS	•	•
B 5233-1	Блок центрального устройства H51q HS	•	•
B 5233-2	Блок центрального устройства H51q HRS	•	•
B 9302	Несущая стойка входов/выходов	•	•

Таблица 8: Центральные модули и блоки для систем H51q

4.3 Прочие центральные модули для систем H41q и H51q

Модуль/блок	Обозначение	Безопасный	без обратного воздействия на источник
Модули распределителя тока			
F 7133	4-кратный распределитель тока с контролем предохранителей		•
Дополнительные модули			
F 7126	Модуль электропитания		•
F 7130A	Модуль электропитания		•
F 7131	Контроль блоков питания с буферными батареями для H51q		•
F 8621A	Модуль сопроцессора для H51q		•
F 8627X	Ethernet		•
F 8628X	Модуль связи для PROFIBUS-DP (ведомое устройство)		•
Шинные соединения			
F 7553	Соединительный модуль шины ввода/вывода для H51q		•
Модули подключения шины к конструкции HIPRO			
H 7505	Преобразователь интерфейсов RS 485, V.24/20 мА 2-проводной/4-проводной (HIPRO)		•
H 7506	Соединительная клемма для конструкции 2-проводных шин		•

Таблица 9: Центральные модули и блоки для систем H51q

4.4 Общие сведения по безопасности и готовности безопасных центральных модулей

К расположению контактов центральных модулей и модулей блоков питания, а также компонентов шины в модульных стойках серий систем H41q/H51q действуют следующие требования.

Системы H41q	Система H51q
В стойке для системных модулей H41q могут применяться: ▪ 2 центральных модуля ▪ 12 модулей ввода/вывода ▪ 2 модуля электропитания ▪ 2 модуля безопасности	В каркас для центральных модулей могут вставляться: ▪ 2 центральных модуля ▪ на каждый центральный модуль 3 модуля сопроцессора F 8621/A или 5 модулей связи F 8627X, F 8628X

Таблица 10: Различия H41q и H51q

4.4.1 Блоки питания

В безопасных приложениях следует всегда применять на один блок питания 24 В пост. тока/5 В пост. тока больше, чем необходимо с точки зрения потребления тока. Это относится к центральной модульной стойке и к дополнительному энергоснабжению. Блоки питания разъединены с помощью диодов и контролируются центральными устройствами.

4.4.2 Описание функций безопасных центральных модулей F 8652X/F 8650X

Каждый центральный модуль типа F 8652X или F 8650X состоит из следующих функциональных блоков:

- Два микропроцессора с тактовой синхронизацией
- Каждый микропроцессор имеет собственную память
- Блоки памяти одного процессора содержат программу и данные в неинвертированной форме, блоки памяти другого процессора, напротив, содержат программу и данные в инвертированной форме
- Тестируемое сравнивающее устройство аппаратного обеспечения для всех внешних доступов обоих микропроцессоров
- При обнаружении неисправности сторожевое устройство переводится в безопасное состояние, и сообщается статус процессора
- Flash-EPROM как память операционной системы и прикладной программы рассчитана на выполнение мин. 100 000 циклов обращения к памяти
- Память данных в SRAM (статическое ОЗУ)
- Многоканальный коммутатор для подключения шины ввода/вывода, двухпортового ОЗУ (DPR) и резервного модуля
- Буферизация SRAM (ОЗУ) через батареи в центральном модуле
- 2 интерфейса RS485 с гальванической развязкой, скорость передачи макс. 57 600 бит/м; настройка каждого переключателя на 9600 бит/с и 57 600 бит/с или настройка (также других значений скорости передачи) через ПО, при этом ПО имеет приоритет
- Индикация диагностики и 2 светодиода для отображения информации системы, зоны ввода/вывода и прикладной программы
- Двухпортовое ОЗУ для быстрого, взаимного доступа к памяти второго центрального модуля
- Часы аппаратного обеспечения с аварийным питанием от батарей
- Логика шины ввода/вывода для соединения с модулями ввода вывода
- Надежное сторожевое устройство
- Контроль блока питания, тестируемый (напряжение системы 5 В)
- Контроль батарей

4.5 Принцип работы безопасных центральных модулей

Безопасные центральные модули состоят из двух микропроцессоров с ОЗУ, которые одновременно обрабатывают одни и те же программы, операционную систему и прикладную программу. Сравнивающее устройство выполняет постоянное сравнение данных с шин, расположенных между микропроцессорами и их блоками памяти.

В операционной системе содержатся стандартные программы самопроверки, которые постоянно выполняются. Сторожевое устройство осуществляет контроль за выполнением программы.

4.5.1 Стандартные программы самотестирования

In der Таблица 11 sind die Selbsttestroutinen der sicherheitsgerichteten Zentralbaugruppen F 8650X und F 8652X und der Ankopplung an die E/A-Ebene erläutert

Test	Описание
Проверка ЦПУ	Проверяется: ▪ Типы команд и адресации ▪ Возможность записи флагов и обусловленных ими команд ▪ Возможность записи и взаимодействие регистров ▪ Арифметическое устройство (ALU)
Тест областей памяти	Операционная система, прикладная программа, константы и параметры, а также переменные данные хранятся в каждом центральном модуле напрямую и инверсно и проверяются сравнивающим устройством аппаратного обеспечения на неравнозначность.
Фиксированные области памяти	Операционная система, прикладная программа и область параметров хранятся каждая в своей флеш-памяти EPROM и защищаются проверкой CRC.
Тест ОЗУ	Области ОЗУ проверяются на взаимное влияние, в частности, путем проведения тестов записи и чтения.
Тестирование сторожевого устройства	Сигнал сторожевого устройства отключается, если он не запущен в установленный промежуток времени обоими ЦПУ с неравнозначными битовыми комбинациями или если сравнивающим устройством аппаратного обеспечения была обнаружена разница в содержании памяти между двумя источниками (напрямую и инверсно). При помощи других тестов проверяется возможность отключения сигнала сторожевого устройства.
Тест на наличие соединения с зоной ввода/вывода в пределах центрального модуля	Для резервных центральных модулей в системах H41q-HS и H51q-HS с одноканальной шиной ввода/вывода обеспечена двусторонняя блокировка доступа ввода/вывода центральных модулей. Служащая для этого схема блокировки проверяется с помощью самодиагностики. Для двухканального уровня ввода/вывода (система HR или HRS) считывается и проверяется право доступа ввода/вывода. Для одноканального уровня ввода/вывода (система M или MS, одноканальные модули ввода/вывода и одноканальное ЦПУ) считывается и проверяется право доступа ввода/вывода.
Проверка соединительного модуля в несущей стойке входов/выходов	Адресация проверяется циклично после каждой обработки безопасного модуля ввода/вывода. Считываются и проверяются адреса всех оговоренных позиций модулей ввода/вывода. Для модуля F 7553 проверяются ключи безопасности.

Таблица 11: Стандартные программы самотестирования

4.5.2 Реакция на установленные ошибки в центральных модулях

С помощью тестовых программ распознаются ошибки и выполняется отключение неисправного центрального модуля. Одновременно с помощью индикации диагностики ошибка отображается и вносится в диагностику систем.

В центральном модуле (система MS) это означает общее отключение контроллера.

В резервных модулях (системы HS и HRS) выполняется отключение неисправного центрального модуля. Второй центральный модуль продолжает поддерживать бесперебойный режим эксплуатации.

Если в резервных системах выполняется замена неисправного модуля на функционально пригодный модуль с такой же прикладной программой, то новый центральный модуль получает от данного модуля актуальные данные, и система продолжает работу в резервном режиме.

При определенных условиях (в частности, при одинаковой версии операционной системы, не ниже V7.0-8 (05.34)) сама прикладная программа также загружается еще работающим центральным модулем в новый, «пустой» центральный модуль (self-education). Более подробную информацию см. руководство по операционной системе (HIQuad Operating System Manual HI 803 078 RU).

4.5.3 Индикация диагностики

Индикация диагностики является составной частью центрального модуля. Она состоит из следующих элементов:

- 4-значной алфавитно-цифровой индикации для отображения текстов и значений
- светодиода *CPU* для индикации ошибок в центральных модулях
- светодиода *IO* для общей индикации ошибок в безопасных модулях ввода/вывода.

Кроме того, имеется кнопка квитирования (*ACK*) и две кнопки для вызова дополнительной информации о системе.

При наличии ошибок в центральном модуле горит светодиод центрального процессора *CPU*. На 4-значном индикаторе отображается индикация STOP. С помощью действия управления возможно отобразить код ошибки. Перечень кодов ошибок представлен в руководство по операционной системе (HIQuad Operating System Manual HI 803 078 RU).

При наличии ошибок в безопасных модулях в зоне ввода/вывода горит светодиод *IO*. 4-значный индикатор отображает положение модуля и (при наличии) поврежденный канал.

Система диагностики предоставляет все коды ошибок для визуализации в системе управления процессом. В системе диагностики ведется контроль протокола ошибок. Он отображается в PADT и поддерживает функцию обнаружения проблем в приложении.

4.6 Реакция на установленные ошибки в зоне шины ввода/вывода

При наличии ошибок в зоне шины ввода/вывода между центральным модулем и соединительными модулями выполняется отключение всех несущих стоек ввода/вывода, на которые распространяется данная ошибка.

При наличии ошибки в зоне шины ввода/вывода только в пределах несущей стойки ввода/вывода соединительный модуль выполняет отключение выходных модулей в той несущей стойке ввода/вывода, на которую распространяется данная ошибка.

4.7 Указание по замене центральных модулей

Замена неисправных модулей как в центральной зоне, так и в зоне ввода/вывода, может выполняться во время эксплуатации, при этом отключение контроллера не требуется.

i Возможно прерывание работы!

Рекомендуется срочная замена неисправных центральных модулей.

В случае ошибки или необходимости технического обслуживания при замене следует придерживаться следующего порядка работы:

- Центральные модули для контроллеров без резервирования, со встроенной буферной батареей, должны размещаться без прикладной программы, если данная прикладная программа содержит переменные Retain. При пуске системы они не устанавливаются на начальное значение.
- Центральные модули для контроллеров с резервированием, со встроенной буферной батареей, могут размещаться и с прикладной программой, даже если данная прикладная программа содержит переменные Retain. При пуске системы выполняется их перенос из действующего центрального модуля.

Индикация диагностики центрального модуля сигнализирует о разрядке внутренней батареи центрального модуля, отображая текст *BATI*.

Рекомендация по замене батарей модулей содержится в техническом паспорте.

i При выходе батареи из строя и одновременном отключении напряжения переменные RETAIN теряют свои сохраненные значения. В данном случае система инициализирует значения при пуске.

5 Модули ввода

5.1 Общий обзор модулей ввода для систем H41q и H51q

Модуль	Обозначение	Безопасный	без обратного воздействия на источник	(Ex)i	Соответствующий функциональный блок
Модули цифрового ввода					
F 3221	Модуль ввода, 16 каналов		•		
F 3222	Модуль ввода, 8 каналов		•		
F 3223	Модуль ввода, 4 канала		•	•	
F 3224A	Модуль ввода, 4 канала		•	•	
F 3236	Модуль ввода, 16 каналов	•	•		
F 3237	Модуль ввода, 8 каналов	•	•		HB-RTE-3
F 3238	Модуль ввода, 8 каналов	•	•	•	HB-RTE-3
F 3240	Модуль ввода, 8 каналов	•	•		
F 3248	Модуль ввода, 16 каналов	•	•		
F 5220	Модуль счетчика, 2 канала	•	•		HF-CNT-3, -4
Модули аналогового ввода					
F 6213[1)]	Модуль аналогового ввода, 4 канала	•	•		HA-RTE-3
F 6214[1)]	Модуль аналогового ввода, 4 канала	•	•		HA-RTE-3
F 6215	Модуль аналогового ввода, 8 каналов		•		
F 6217	Модуль аналогового ввода, 8 каналов	•	•		
F 6220	Модуль ввода термоэлемента, 8 каналов	•	•	•	HF-TMP-3
F 6221	Модуль аналогового ввода, 8 каналов	•	•	•	HF-AIX-3
[1)] отмененный модуль, больше не поставляется					

Таблица 12: Модули ввода для систем H41q и H51q

5.2 Безопасность и готовность безопасных модулей ввода

Некоторые типы модулей аналогового и цифрового ввода в связи со своей повышенной сложностью имеют собственную микропроцессорную систему 1oo2, которая автоматически выполняет безопасные проверки во время эксплуатации и предоставляет безопасные данные для безопасного обрабатывающего устройства.

Безопасные модули ввода делают возможной индикацию данных диагностики, а таким образом — также и обнаружение и локализацию неисправностей.

В безопасных системах можно применять как безопасные модули ввода, так и модули ввода без обратного воздействия в смешанном оснащении.

Безопасные модули ввода в системах H41q и H51q во время работы автоматически подвергаются качественной циклической самодиагностике. В модулях ввода име.ься элементы переключения, позволяющие выполнять проверку функции модулей ввода с помощью специальных тестовых программ, встроенных в операционную систему. Эти тестовые программы проверены TÜV и обеспечивают правильную работу соответствующего модуля. Для каждой распознанной ошибки создаются сообщения об ошибках. Распознанные ошибки автоматически приводят к безопасной реакции системы. Сообщения об ошибках являются диагностической информацией для оператора. При проектировании и реализации установки можно гибко разрабатывать систему диагностики.

Для повышения уровня готовности можно также применять резервные безопасные модули ввода.

Использование резервных модулей ввода не снижает уровень безопасности системы.

Безопасные модули ввода могут использоваться как для безопасных, так и для небезопасных сигналов.

Для допустимых слотов для модулей ввода в системных несущих стойках и стойках ввода/вывода для систем H41q и H51q необходимо учитывать следующие инструкции:

Система H41q	Система H51q
Модули ввода вставляются в системную несущую стойку. Доступны блоки с 12 слотами (H41q) для модулей ввода/вывода.	Модули ввода вставляются в модульные стойки ввода/вывода с 16 слотами для модулей ввода/вывода. Необходимые базовые компоненты для модульных стоек ввода/вывода объединены в блоках.

Таблица 13: Допустимые слоты

5.2.1 Безопасность датчиков и трансмиттеров

Безопасные сигналы передаются только в случае, если внешние датчики или трансмиттеры имеют подтверждение безопасности. Если у них нет подтверждения безопасности, то безопасность внешних датчиков или трансмиттеров также также можно обеспечить с помощью специального подключения, см. руководство *(*HIQuad Operating System Manual HI 803 078 RU).

В этом случае необходимо подключить несколько датчиков по схеме 1oo2, 2oo3 или NooM. (Примечание: 1oo2 означает «1 out of 2», т. е. 1 из 2.)

Безопасность и готовность чувствительных элементов может повышаться с помощью подключения датчиков. Различные возможности подключения датчиков с точки зрения безопасности и готовности подробно описаны в главе 7.8. Прикладная программа должна быть настроена соответствующим образом.

На основе стандарта IEC 61508 можно задавать интервалы проверочных тестов в режиме офлайн, что обеспечивает возможность соответствующих безопасных подтверждений. Подробные настройки следует задавать в зависимости от приложения.

5.3 Безопасные модули цифрового ввода F 3236, F 3237, F 3238, F 3240 и F 3248

5.3.1 Тестовые программы

Тестовые онлайн-программы проверяют, в состоянии ли входные каналы последовательно подключать оба уровня сигналов (уровень LOW и HIGH) независимо от имеющихся входных сигналов. Данный тест функциональности выполняется при каждом считывании входных сигналов. Каждый раз при ошибке в модуле ввода прикладная программа обрабатывает низкий уровень напряжения (безопасное состояние).

Модули для инициаторов и контактных датчиков с контролем линии дополнительно проверяют линию до датчика. К данным модулям можно подключать безопасный инициатор. Благодаря самодиагностике выполняются все требования по распознаванию пороговых значений безопасных инициаторов.

Контроль тока контактного датчика требует подключения с двумя сопротивлениями согласно техническому паспорту.

5.3.2 Реакция на установленные ошибки для F 3236, F 3237, F 3238, F 3240 и F 3248

Характер неисправности	Реакция системы	Примечание
Неисправность модуля (модуль ввода)	Передача FALSE прикладной программе для всех каналов	Благодаря этому обеспечивается безопасное функционирование системы по принципу тока покоя.
Обрыв линии в цепи датчика	Считывание FALSE на соответствующем канале	Для модулей с контролем линии сигнализируется неисправность линии. В безопасных входах для того, чтобы обеспечить возможность безопасной реакции системы, данный сигнал следует оценивать с помощью модуля программного обеспечения HB-RTE-3 (см. приложение).
Замыкание линии в цепи датчика	Считывание TRUE в соответствующем канале	Для модулей с контролем линии сигнализируется неисправность линии. В безопасных входах для того, чтобы обеспечить возможность безопасной реакции системы, данный сигнал следует оценивать с помощью модуля программного обеспечения HB-RTE-3 (см. приложение).
Общая информация	Индикаторная панель отображает положение неисправных модулей. Для модуля F 3238, занимающего два слота в модульной стойке, отображается положение правого слота. При использовании модулей ввода с контролем обрыва провода и короткого замыкания цепи датчика индикаторная панель наряду с положением модуля показывает также неисправный канал модуля.	

Таблица 14: Реакция на ошибку в безопасных модулях цифрового ввода

5.4 Безопасный модуль счетчика F 5220

Двухканальный модуль счетчика имеет собственную двухпроцессорную систему с безопасным выходом для каждого канала. Он может применяться для счета импульсов, измерения частоты или определения числа оборотов через регулируемое время стробирования, а также для контроля направления вращения.

При изменениях времени стробирования корректное измеренное значение доступно на выходе только через три цикла времени стробирования!

5.4.1 Тестовые программы

Модуль имеет собственную микропроцессорную систему 1oo2, которая автоматически выполняет безопасные проверки в режиме онлайн и предоставляет безопасные данные для безопасной обработки сигналов на модуле программного обеспечения HF-CNT-3 или HF-CNT-4.

5.4.2 Реакция на обнаруженные ошибки

Характер неисправности	Реакция системы в случае ошибки	Примечание
Ошибки модуля	Отключение безопасных выходов	При обнаружении ошибки реакция только в безопасном направлении
Неисправность канала	Отключение заданного безопасного выхода	При обнаружении ошибки реакция только в безопасном направлении
Обрыв или замыкание линии в цепи инициатора или прочие ошибки	Отключение заданного безопасного выхода	После устранения ошибки требуется сигнал сброса на входе модуля HF-CNT-3/4

Таблица 15: Реакция на ошибки в безопасном модуле счетчика F 5220

5.5 Безопасные модули аналогового ввода F 6213, F 6214 и F 6217

При резервировании безопасных модулей аналогового ввода для работоспособных модулей обрабатывается среднее значение (только в пределах допустимых отклонений!). Среднее значение для F 6213 и F 6214 вырабатывает соответствующий модуль, для F 6217 — прикладная программа. В случае ошибки обрабатывается только значение работоспособного модуля.

5.5.1 Тестовые программы

Модули через тестовый цифро-аналоговый преобразователь подключают тестовые значения и проверяют их через аналого-цифровой преобразователь, с помощью которого также оцифровывается входной сигнал.

5.5.2 Реакции на обнаруженные ошибки в F 6213 и F 6214

Характер неисправности	Реакция системы в случае ошибки	Примечание
Ошибки модулей или каналов при одноканальных аналоговых входах	Обработка сконфигурированного значения на модуле программного обеспечения HA-RTE-3 (см. приложение)	В случае ошибки реакция может производиться только в безопасном направлении
Ошибки модулей или каналов при резервных модулях аналогового ввода и резервных трансмиттерах	В случае ошибки модуля ввода обрабатывается значение резервного модуля или сконфигурированное значение ошибки	По выбору создание минимального, максимального или среднего значения через модуль программного обеспечения HA-RTE-3 (см. приложение)
Короткое замыкание в цепи трансмиттера	Индикация положения модуля и неисправного канала на индикаторной панели	только при использовании 4...20 мА

Таблица 16: Реакция на ошибки для безопасных модулей аналогового ввода F 6213, F 6214

5.5.3 Реакции на обнаруженные ошибки для F 6217

Характер неисправности	Реакция системы в случае ошибки	Примечание
Неисправность канала	Аналоговое значение = 0000 Бит ошибки канала = TRUE	Бит ошибки канала подлежит безопасной обработке в прикладной программе
Ошибки модуля	Все аналоговые значения = 0000 Все биты ошибки канала = TRUE	См. ошибки канала, касается всех битов ошибки канала
Превышение диапазона измерения (22 мА)	Макс. аналоговое значение = 4095 Бит ошибки канала = TRUE	Макс. допустимое значение должно определяться в прикладной программе.

Таблица 17: Реакция на ошибку для безопасных модулей аналогового ввода F 6217

Модуль имеет собственную микропроцессорную систему 1oo2, которая автоматически выполняет безопасные проверки в режиме онлайн и предоставляет безопасные данные для безопасного обрабатывающего устройства. Для каждого канала имеется аналоговое значение и относящийся к нему бит ошибки канала.

⚠ ПРЕДУПРЕЖДЕНИЕ

Предупреждение! Опасность травмирования из-за неверного измеренного значения!

Для каждого безопасного аналогового входа следует запрограммировать безопасную реакцию при установленном бите ошибки канала.

5.6 Искробезопасный модуль аналогового ввода термоэлемента F 6220

Модуль термоэлемента имеет восемь каналов для подключения термоэлементов различных типов (в зависимости от параметрирования на модулях HF-TMP-3) и один вход для подключения термометра сопротивления Pt 100 в качестве входа температуры сравнения. Он имеет собственную двухпроцессорную систему, параметрирование производится через модуль программного обеспечения HF-TMP-3 (см. главу 9.2.9 и онлайновую справку ELOP II) для каждого занятого канала.

Входы также могут использоваться для измерения низких напряжений, см. технический паспорт.

5.6.1 Тестовые программы

Модуль имеет собственную микропроцессорную систему 1oo2, которая автоматически выполняет безопасные проверки в режиме онлайн и предоставляет безопасные данные для безопасной обработки сигналов в модуле программного обеспечения HF-TMP-3. Каждый из 8+1 каналов поставляет безопасные входные значения и безопасный статус ошибки.

5.6.2 Реакции на обнаруженные ошибки в F 6220

Состояние	Реакция системы	Примечание
Ошибки модуля	Выход *Channel Fault* на модуле HF-TMP-3 переключает на TRUE.	Реакцию следует реализовывать в прикладной программе с использованием выходного сигнала *Channel Fault*.
Неисправность канала	Выход *Channel Fault* на модуле HF-TMP-3 переключает на TRUE.	Реакцию следует реализовывать в прикладной программе.
Underflow	Выход *Underflow* на модуле HF-TMP-3 переключает на TRUE.	Реакцию следует реализовывать в прикладной программе.
Переполнение	Выход *Underflow* на модуле HF-TMP-3 переключает на TRUE.	Реакцию следует реализовывать в прикладной программе.

Таблица 18: Реакция на ошибку для безопасного модуля термоэлемента F 6220

Предельные значения для антипереполнения или переполнения определяются на входах *Underflow Threshold* либо *Overflow Threshold* модуля HF-TMP-3. Если измеренное значение не достигает этих параметрированных пороговых значений или превышает их, выдается соответствующий сигнал TRUE без наличия ошибки в модуле.

5.6.3 Рекомендации по проектированию

- Неиспользованные входы следует закоротить.
- При уровне совокупной безопасности 3 следует брать значение эталонной температуры из прикладной программы или определять его путем сравнения эталонных температур двух модулей.
- Следует рассматривать все возможные отклонения и учитывать их при интерпретации измеренных значений.
- Для SIL 3 следует определить температуру термоэлементов в качестве сравнения двух термоэлементов.

5.7 Искробезопасный модуль аналогового ввода F 6221

Модуль аналогового ввода имеет восемь каналов для прямого подключения аналоговых трансмиттеров из взрывоопасной зоны. Подача напряжения питания трансмиттеров может производиться через модуль вывода F 3325 или другой подвод напряжения в соответствии с данными технического паспорта. Данное питающее напряжение трансмиттера следует подключать к контролю через модуль F 6221.

Каждый занятый канал параметрируется через собственный модуль программного обеспечения HF-AIX-3.

5.7.1 Тестовые программы

Модуль имеет собственную микропроцессорную систему 1oo2, которая автоматически выполняет проверки в режиме онлайн и предоставляет безопасные данные для безопасной обработки сигналов на модуле программного обеспечения HF-AIX-3. Каждый из восьми каналов поставляет безопасные входные значения и безопасный статус ошибки.

5.7.2 Реакции на обнаруженные ошибки в F 6221

Состояние	Реакция системы	Примечание
Module fault	Выход *Value* (INT) на модуле HF-AIX-3 выдает числовое значение 0. Выход *Channel Fault* на модуле HF-AIX-3 переключает на TRUE.	В прикладной программе значение ошибки должно определяться с использованием входного сигнала модуля *Error Value*
Channel fault	Выход *Channel Fault* на модуле HF-AIX-3 переключает на TRUE.	
Underflow	Выход *Underflow* на модуле HF-AIX-3 переключает на TRUE.	
Overflow	Выход *Underflow* на модуле HF-AIX-3 переключает на TRUE.	

Таблица 19: Реакция на ошибку для безопасного модуля аналогового входа F 6221

Предельные значения для недостижения или превышения определяются на входах *Underflow Threshold* или *Overflow Threshold* модуля HF-AIX-3. Если измеренное значение не достигает этих параметрированных пороговых значений или превышает их, выдается соответствующий сигнал TRUE без наличия ошибки в модуле.

5.7.3 Прочие рекомендации по проектированию

- Незадействованные потенциальные входы 0...1 В следует закоротить на клеммной колодке.
- Незадействованные токовые входы подключаются через шунт в кабельном штекере.
- Допустимо применение только согласно техническому паспорту F 6221.
- Следует соблюдать положения о взрывозащите и условия взрывобезопасного подключения.

5.8 Указание по замене модулей ввода

В случае ошибки или необходимости технического обслуживания при замене следует соблюдать следующие этапы работы:

Замена модуля ввода

1. Открутите кабельный штекер или извлеките модуль ввода со вставленным кабельным штекером.
2. Вставьте новый модуль ввода без кабельного штекера и привинтите его.
3. Вставьте и привинтите кабельный штекер.
4. Задействуйте кнопку квитирования (кнопка *ACK* на центральном модуле).

► Модуль ввода заменен

i Возможно прерывание работы!

Рекомендуется срочная замена неисправных модулей ввода.

5.9 Контрольные перечни для проектирования, программирования и ввода в эксплуатацию безопасных модулей ввода

Для каждого отдельного используемого в системе безопасного модуля ввода в рамках проектирования либо ввода в эксплуатацию следует заполнять собственный контрольный перечень для контроля учитываемых требований. Только в таком случае можно обеспечить полную и наглядную регистрацию требований. Контрольные перечни одновременно служат и документами, подтверждающими тщательность выполнения проектирования.

Контрольные перечни данного руководства по безопасности доступны в виде файлов MS Word на DVD-диске HIMA и в интернете по адресу www.hima.com и www.hima.com:

SDIGE-F3236	для безопасных цифровых модулей
SDIGE-F3237	для безопасных цифровых модулей
SDIGE-F3238	для безопасных цифровых модулей
SDIGE-F3240	для безопасных цифровых модулей
SDIGE-F3248	для безопасных цифровых модулей
SDIGE-F5220	для безопасных модулей счетчика
SANAE-F6213 / F6214	для безопасных аналоговых модулей
SANAE-F6217	для безопасных аналоговых модулей
SANAE-F6220	для безопасных аналоговых модулей
SANAE-F6221	для безопасных аналоговых модулей

6 Модули вывода

6.1 Общий обзор модулей вывода для систем H41q и H51q

Модуль	Обозначение	Безопасный	без обратного воздействия на источник	Нагрузочная способность	Соответствующий функциональный блок
Цифровые модули вывода					
F 3322	Модуль цифрового вывода, 16 каналов		•	≤ 0,5 A	
F 3325	Модуль питания (Ex), 6 каналов		•	22 В ≤ 0,02 A	
F 3330	Модуль цифрового вывода, 8 каналов	•	•	≤ 0,5 A	
F 3331	Модуль цифрового вывода, 8 каналов	•	•	≤ 0,5 A	HB-BLD-3[1], HB-BLD-4[1]
F 3333	Модуль цифрового вывода, 4 канала	•	•	≤ 2 A	
F 3334	Модуль цифрового вывода, 4 канала	•	•	≤ 2 A	HB-BLD-3[1], HB-BLD-4[1]
F 3335	Модуль цифрового вывода (Ex), 4 канала	•	•	22 В ≤ 0,053 A	
F 3348	Модуль цифрового вывода, 8 каналов	•	•	≤ 0,5 A	
F 3349	Модуль цифрового вывода, 8 каналов	•	•	≤ 0,5 A ≤ 48 В	HB-BLD-3[1], HB-BLD-4[1]
F 3422	Цифровой релейный модуль, 8 каналов		•	≤ 2 A ≤ 60 В	
F 3430[2]	Цифровой релейный модуль	•	•	≤ 4 A ≤ 250 В	
Модули аналогового вывода					
F 6705	Модуль аналогового вывода, 2 канала	•	•	0...20 мА	HZ-FAN-3[3]
F 6706	Модуль аналогового вывода, 2 канала		•	0...20 мА	

[1] Для индикации неисправности и параметрирования рабочих режимов (ток покоя, рабочий ток)

[2] Модуль F 3430 не сертифицирован согласно EN/ISO 13849-1.

[3] Требуется в режиме токового выхода для анализа неисправности

Таблица 20: Модули вывода для систем H41q и H51q

6.2 Общие сведения по безопасности и готовности безопасных модулей вывода

Безопасные модули вывода описываются в каждом цикле, выполняется обратное считывание выходных сигналов и сравнение с рассчитанными прикладной программой выходными данными.

Дополнительно на заднем плане выполняется проверка Walking-Bit через все выходы. При этом выходит тестовый сигнал продолжительностью макс. 200 мкс. Благодаря этому проверяется переключаемость выходов без воздействия на функцию подключенных исполнительных элементов. Распознается замерзание каждого выхода, даже если выходной сигнал является статическим.

Безопасные модулы вывода с контролем линии могут определять ошибку на подающей линии к потребителю. Контроль линии выполняет требования безопасности до уровня совокупной безопасности 1. Это имеет значение только при использовании контроля линии в безопасных электроцепях. Исходный сигнал может использоваться во всех применениях для требований безопасности до SIL 3.

Система H41q	Система H51q
Модули вывода вставляются в стойку системных модулей. Доступны блоки с 12 слотами (H41q) для модулей ввода/вывода.	Модули вывода вставляются в предусмотренные для этого несущие стойки ввода/вывода (EABT) макс. с 16 слотами для модулей ввода/вывода. Необходимые базовые компоненты для EABT обобщены в блоках (см. главу 4 на стр. 21).
Слоты для модулей вывода в системах H41q и H51q	Слоты для модулей вывода в системах H41q и H51q

Таблица 21: Слоты для модулей вывода в системах H41q и H51q

6.2.1 Безопасные модули цифрового вывода

Тестовые программы определяют ошибку путем сравнения считываемых выходных сигналов со внутренними выходными данными. Операционная система переводит в безопасное состояние модуль на позиции модуля, которая была распознана как дефектная, и сообщает об этом на индикаторную панель.

У модулей с контролем выходной цепи распознанный обрыв линии сигнализируется путем индикации неисправного канала модуля на индикаторной панели. Неисправный модуль вывода безопасно отключается встроенным блоком предохранительного отключения.

Дополнительно с помощью модуля программного обеспечения H8-STA-3 определяются одна или несколько групп отключения. Неисправность модуля вывода приводит к отключению всех модулей вывода, относящихся к группе отключения.

В зависимости от требований безопасности установки можно также в настройках для ресурсов с помощью параметров ввода/вывода задавать конфигурацию общего отключения системы управления.

6.2.2 Безопасные модули аналогового вывода

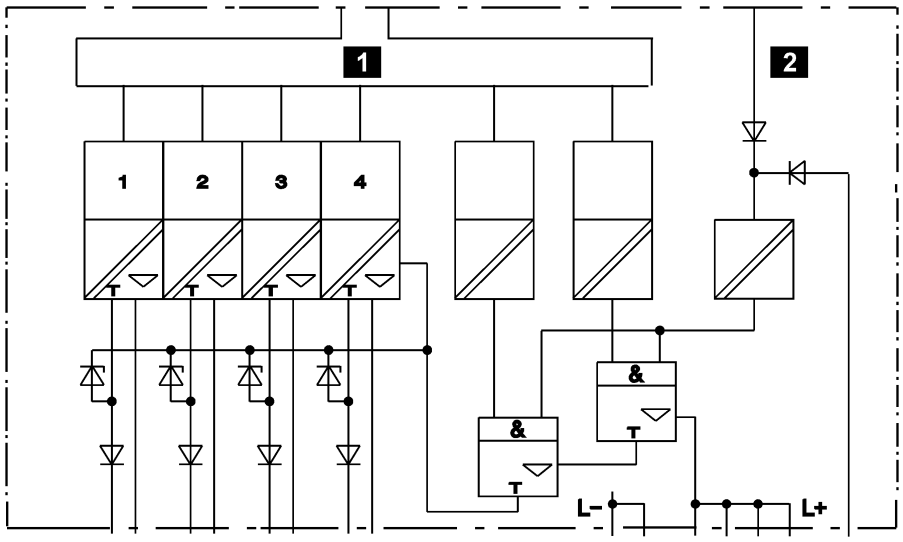
Безопасные модули аналогового вывода могут применяться в режиме источника тока или токового выхода.

В режиме источника тока встроенное предохранительное отключение в случае ошибки приводит в безопасное состояние (выходной ток 0 мА).

В режиме снижения тока безопасное состояние достигается только с помощью дополнительных мероприятий. Прикладная программа должна безопасно отключить питающее напряжение для токовой петли. Для анализа ошибки следует использовать модуль программного обеспечения HZ-FAN-3.

6.3 Основной принцип работы безопасных модулей вывода

В безопасных модулях вывода последовательно включены три тестируемых полупроводниковых переключателя. Таким образом, в модуль вывода интегрирован необходимый для обеспечения функции безопасности второй независимый способ отключения. Этот встроенный блок предохранительного отключения в случае ошибки отключает все каналы неисправного модуля вывода (обесточенное состояние).



1 Шина ввода/вывода 2 Сигнал сторожевого устройства (WD)

Рис. 1: Принципиальная схема модулей вывода со встроенным предохранительным отключением (здесь с 4 выходными каналами)

6.4 Безопасные модули цифрового вывода F 3330, F 3331, F 3333, F 3334, F 3335, F 3349

6.4.1 Тестовые программы

Модули автоматически тестируются во время работы. Основные тестовые функции:

1. Считывание выходного сигнала коммутирующего усилителя. Порог переключения для обратно считываемого низкого уровня: ≤ 6,5 В.
2. Считывание диагностики линии включенных каналов (только для F 3331, F 3334 и F 3349).
3. Подключение тестовых образцов и проверка на перекрестные помехи (Walking-Bit-Test) в рамках фоновых проверок.
4. Считывание диагностики линии всех каналов (только для F 3331, F 3334 и F 3349).
5. проверка встроенного предохранительного отключения.

6.4.2 Реакция на обнаруженные ошибки для F 3330, F 3331, F 3333, F 3334, F 3335, F 3349

- Все обнаруженные на модуле ошибки приводят к тому, что модуль переводится в безопасное, обесточенное состояние, т. е. отключается.
- Внешние короткие замыкания, не отличающиеся от внутренних ошибок, приводят к отключению модуля.
- В связи с неисправностями линии только выводится соответствующее сообщение, к отключению они не приводят.

6.4.3 Указание по проектированию

Перед удалением модулей F 3330, F 3331, F 3333, F 3334 из конфигурации проекта необходимо вернуть выходы в исходное состояние! Например, для выходов, инициализированных на сигнал 1, следует завершить инициализацию.

6.5 Безопасный модуль цифрового вывода F 3430

6.5.1 Тестовые программы

Модуль автоматически тестируется во время работы. Основные тестовые функции:

1. Считывание выходного сигнала коммутирующего усилителя для разнообразных релейных переключателей на три положения.
2. Подключение тестовых образцов и проверка на перекрестные помехи (Walking-Bit-Test) в рамках фоновых проверок.
3. проверка встроенного предохранительного отключения.

6.5.2 Реакция на обнаруженные ошибки в безопасных цифровых релейных модулях

- При всех обнаруженных в модуле ошибках модуль переводится в безопасное, обесточенное состояние, т. е. модуль отключается.
- При внешних коротких замыканиях срабатывает предохранитель для соответствующего канала. Сообщение о неисправности не выдается.

6.5.3 Указание по проектированию

Реле являются электромеханическими элементами и в силу конструктивных особенностей имеют ограниченный срок службы. Срок службы реле зависит от коммутационной способности контактов (ток/напряжение) и количества циклов переключения.

Срок службы в условиях номинального режима составляет 300 000 циклов переключения при 30 В пост. тока и 4 А.

Для соблюдения требований согласно IEC 61508 (PFD/PFH, см. главу 3.1.1) действует интервал повторной проверки в режиме офлайн 5 лет при использовании с уровнем совокупной безопасности 3 и 20 лет при использовании с уровнем совокупной безопасности SIL 2.

Необходимые проверки выполняются изготовителем (HIMA).

6.6 Безопасный модуль аналогового вывода F 6705

6.6.1 Тестовые программы

Модуль автоматически тестируется во время работы. Основные тестовые функции:

1. Обратное считывание выходного сигнала.
2. Проверка цифро-аналогового преобразователя на линейность.
3. Проверка на перекрестные помехи между выходами.
4. проверка встроенного предохранительного отключения.

6.6.2 Реакции на обнаруженные ошибки для F 6705

В режиме источника тока модуль при любых распознанных в модуле ошибках переводится в безопасное, обесточенное состояние, т. е. модуль отключается с помощью встроенного предохранительного отключения.

Внешний обрыв линии не отличается от внутренних ошибок и приводит к отключению модуля.

В режиме токового выхода безопасное, обесточенное состояние достигается только с помощью внешнего отключения. Прикладная программа должна безопасно отключать

источник напряжения для токовой петли. Поэтому для анализа ошибок следует использовать модуль программного обеспечения HZ-FAN-3.

6.7 Указание по замене модулей вывода

В случае ошибки или необходимости технического обслуживания при замене следует соблюдать следующие этапы работы:

Замена модуля вывода

1. Отвинтите кабельный штекер или извлеките модуль вывода со вставленным кабельным штекером.
2. Установите новый модуль вывода без кабельного штекера и привинтите его.
3. Вставьте и привинтите кабельный штекер.
4. Задействуйте кнопку квитирования (кнопка *ACK* на центральном модуле).

► Модуль вывода заменен..

i Возможно прерывание работы!

Рекомендуется срочно заменять неисправные модули вывода.

6.8 Контрольные перечни для проектирования, программирования и ввода в эксплуатацию безопасных модулей вывода

Для каждого отдельного используемого в системе безопасного модуля вывода в рамках проектирования либо ввода в эксплуатацию следует заполнять собственный контрольный перечень для контроля учитываемых требований. Только в таком случае можно обеспечить полную и наглядную регистрацию требований. Контрольные перечни одновременно служат и документами, подтверждающими тщательность выполнения проектирования.

Контрольные перечни данного руководства по безопасности доступны в виде файлов MS Word на DVD-диске HIMA и в интернете по адресу http://www.hima.de/ и www.hima.com.

SDIGA-F3330	для безопасных цифровых модулей
SDIGA-F3331	для безопасных цифровых модулей
SDIGA-F3333	для безопасных цифровых модулей
SDIGA-F3334	для безопасных цифровых модулей
SDIGA-F3335	для безопасных цифровых модулей
SDIGA-F3348	для безопасных цифровых модулей
SDIGA-F3349	для безопасных цифровых модулей
SDIGA-F3430	для безопасных цифровых модулей
SANAA-F6705	для безопасных аналоговых модулей

7 Software, программное обеспечение

Программное обеспечение для безопасных устройств автоматизации HIMA серий систем H41q и H51q подразделяется на три блока:

- Операционная система
- Прикладная программа
- Инструмент программирования согласно IEC 61131-3 (ELOP II со встроенным безопасным инструментом).

Операционная система должна использоваться в действительной форме, сертифицированной TÜV для безопасного применения. Действительную версию см. в общем документе Version List of Modules and Firmware of H41q/H51q Systems. Этот документ составляется общей службой технической документации TÜV Rheinland Industrie Service GmbH и компании HIMA.

Прикладная программа составляется с помощью инструмента программирования ELOP II и включает в себя те зависящие от конкретной установки функции, которые должно выполнять устройство автоматизации. Для параметрирования функций операционной системы также используется ELOP II. Генератор кода переводит прикладную программу в машинный код. ELOP II через последовательный интерфейс или Ethernet передает этот машинный код и прочие данные проектной конфигурации во флеш-память в центральном модуле.

Основные функции операционной системы и связанные с ними установки для прикладной программы описаны в руководстве по операционной системе (HIQuad Operating System Manual HI 803 078 RU).

7.1 Аспекты безопасности для операционной системы

В этой главе описываются сигнатуры и основной принцип работы операционной системы.

7.1.1 Обозначение актуально утвержденной версии для безопасного применения (сигнатура CRC)

Каждая новая операционная система имеет свое обозначение со статусом издания. Для дополнительного обозначения служит сигнатура операционной системы, отображаемая в режиме эксплуатации устройства автоматизации на индикаторной панели.

Действительные, допущенные TÜV для безопасных устройств автоматизации версии операционной системы и соответствующие сигнатуры (CRCs) см. в *Revision List of Devices and Firmware of H41q/H51q Systems*.

7.1.2 Принцип работы и функции операционной системы

Операционная система циклически выполняет прикладную программу.
Последовательность в сильно упрощенной форме:

1. Считывание входных данных (входы аппаратного обеспечения)
2. Обработка логических функций согласно IEC 61131-3, раздел 4.1.3
3. Запись выходных данных (выходы аппаратного обеспечения)

Также выполняются следующие основные функции:

- Обширная самодиагностика
- Тестирования модулей ввода/вывода во время работы
- Передача и сравнение данных.

Цикл выполняется за семь фаз. Эти фазы подробно описаны в руководстве по операционной системе (HIQuad Operating System Manual HI 803 078 RU).

7.2 Безопасные аспекты прикладной программы

Общая последовательность программирования устройств автоматизации серий H41q/H51q для безопасного применения:

1. Спецификация функции управления
2. Запись прикладной программы
3. Верификация прикладной программы с помощью моделирования в режиме офлайн
4. Компиляция прикладной программы при помощи генератора C-кода
5. Надежный генератор C-кода (GNU-CC) дважды переводит C-код и создает целевой код и код сравнения.
6. Сравнивающее устройство сравнивает целевой код и код сравнения. Сравнивающее устройство целевого кода распознает ошибки, вызванные небезопасным ПК, и передает соответствующее сообщение.
7. Не имеющая ошибок и готовая к выполнению программа загружается в систему H41q или H51q. Здесь программа может быть проверена.
8. После успешного завершения проверки ПЭС начинает безопасную эксплуатацию.

Понятия:

Load (загрузка)	Под этим понятием понимается, что программа загружается в систему управления либо с помощью загрузки, либо с помощью перезагрузки.
Download (загрузка)	При загрузке программы в систему управления все выходы системы управления сбрасываются, а система управления останавливается.
Reload (перезагрузка)	При перезагрузке прикладной программы в резервную систему управления измененная прикладная программа загружается поочередно в центральные модули. Центральный модуль при этом всегда в монорежиме. Отключения не происходит. При ПЭС только с одним центральным модулем выходы останавливаются на время передачи. Перезагрузка возможна только в случае, если создан способный к перезагрузке код.

7.2.1 Предустановки и правила для использования в безопасных применениях (требования из экспертизы типового образца и т. д.)

Прикладная программа составляется с помощью инструмента программирования ELOP II. ПК необходимо дополнительно оснастить модулем жесткой блокировки HIMA.

Инструмент программирования ELOP II содержит следующие основные функции:

- Ввод (редактор функциональных блоков), контроль и документацию
- Переменные с символическими именами и типом переменных (BOOL, UINT и т. д.)
- Присвоение ресурса (автоматизированные системы HIMA H41q/H51q)
- Генератор кода (компиляция прикладной программы в машинный код) с генератором C-кода и компилятором GNU-C.

7.2.1.1 Основы программирования

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

- Комбинаторная логическая схема:
  - Схема причина/действие
  - 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 согласно DIN EN 60848
  - Матричная или табличная форма условий поэтапного переключения и управляемых исполнительных элементов
  - Определение краевых условий, напр. режимов работы, EMERGENCY STOP и т. д.

Концепция автоматизации 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 резервирования, необходимого с учетом сохранения функции безопасности (1oo2, 2oo3)
  - 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:

- Простота для понимания
- Возможность отслеживания
- Удобство внесения изменений.

7.2.2 Аспекты безопасности для программирования с ELOP II

Для составления прикладных программ используется инструмент программирования ELOP II.

Условия применения, например поддерживаемая версия Windows, см. в документации к соответствующей версии ELOP II.

Концепция безопасности ELOP II Factory гарантирует следующее:

- Инструмент программирования работает корректно, т. е. ошибки инструмента программирования обнаруживаются.
- Пользователь правильно применяет инструмент программирования, т. е. обнаруживаются ошибки пользователя.

При первом вводе в эксплуатацию безопасной системы управления проверяется безопасность всей системы путем выполнения полного теста функциональности. После изменения прикладной программы для гарантии безопасности необходимо еще раз выполнить полный тест функциональности.

Безопасный инструмент в ELOP II согласно IEC 61131-3 спроектирован таким образом, что после изменения прикладной программы необходимо проверять только изменения. Данный безопасный инструмент служит для обнаружения ошибок пользователя и ошибок инструмента программирования.

Безопасный инструмент ELOP II состоит из трех модулей, имеющих значение для безопасности:

- Сравнивающее устройство C-кода
- Сравнивающее устройство целевого кода
- Надежный компилятор GNU-C.

Сравнивающее устройство С-кода идентифицирует изменения в прикладной программе. Сравнивающее устройство целевого кода сравнивает два целевых кода, поочередно созданных компилятором GNU-C (GNU-CC). Благодаря этому предотвращаются ошибки, которые могут быть вызваны небезопасным ПК.

Небезопасные вспомогательные средства:

- Встроенное в ELOP II управление изменениями. Используется для однозначной идентификации релевантных версий проекта.
- Моделирование в режиме офлайн, представленное на блок-схеме, Рис. 2. Моделирование в режиме офлайн верифицирует прикладную программу в отношении спецификации, не воздействуя на процесс.

7.2.2.1 Применение безопасного инструмента ELOP II при составлении программы

На блок-схеме Рис. 2 указаны пункты, на которые дается ссылка в следующем тексте.

1. Составление прикладной программы по обязательной спецификации (например, согласно IEC 61508, DIN V VDE 0801 или соответствующему прикладному стандарту), на блок-схеме пункты с (1) по (4).
2. Генератор С-кода компилирует прикладную программу в С-код и создает дополнительно файл сравнения, пункт (5) на блок-схеме.

⚠ ПРЕДУПРЕЖДЕНИЕ

Опасность травмирования из-за нарушения функционирования!

Для прикладной программы необходимо создать таблицу ссылок и проверить на правильное использование переменных! Необходимо проверить, что все переменные используются только там, где они предусмотрены согласно спецификации.

3. Надежный С-компилятор переводит С-код и файл сравнения, пункт (6) и (13). Компилятор создает целевой код и код сравнения.

⚠ ПРЕДУПРЕЖДЕНИЕ

Опасность травмирования из-за нарушения функционирования!

Необходимо активировать сравнивающее устройство целевого кода, пункт (14). Оно сравнивает целевой код и код сравнения. Сравнивающее устройство распознает ошибки, вызванные небезопасным ПК, и сообщает о них.

4. Загрузите созданную таким образом, готовую к выполнению программу в систему H41q/H51q (пункт (7)). Здесь программу необходимо полностью проверить и принять (пункт (8)).
5. Выполните резервное копирование целевого кода.
6. ПЭС начинает безопасную эксплуатацию.

7.2.2.2 Применение безопасного инструмента ELOP II при изменении программы

1. Модификация прикладной программы по обязательной спецификации (например, согласно IEC 61508 или соответствующему прикладному стандарту), на блок-схеме пункты с (1) по (4).

   Основой для изменения является резервная копия текущей прикладной программы. Данная резервная копия содержит:

   - Файл сравнения
   - Целевой код
   - Входные данные.
2. Генератор С-кода компилирует измененную прикладную программу в С-код (новый), пункт (5).

3. Необходимо активировать сравнивающее устройство C-кода, пункт (12). Оно сравнивает C-код (новый) с C-кодом (старым) предыдущей версии программы, пункт (11). В качестве файла сравнения (C-код (старый)) необходимо указать резервную копию.
4. Документируется результат сравнения, пункт (15).
5. Проверьте, отображает ли сравнивающее устройство C-кода изменения, выполненные в прикладной программе. Отображаются только релевантные для кода изменения.
6. Результат сравнивающего устройства C-кода:
   a Сообщает об изменениях, которые пользователь не опознает, причины этого могут заключаться в следующем:
   - Выполненное пользователем изменение имеет следствием дальнейшие непредвиденные изменения
   - Имеет место внутренняя ошибка.

   b Не сообщает о выполненных пользователем изменениях, причина может заключаться в следующем:
   - Изменения, которые не распознаются сравнивающим устройством C-кода, например, графические изменения или изменения начальных значений.
   - Изменения, которые были некорректно приняты.
7. C-компилятор переводит C-код (новый) и файл сравнения (новый), пункты (6) и (13). Он создает целевой код и код сравнения.
8. Необходимо активировать сравнивающее устройство целевого кода, пункт (14). Оно сравнивает целевой код и код сравнения. Распознаются ошибки, вызванные небезопасным ПК, и выводится соответствующее сообщение.
9. Составленная таким образом, готовая к выполнению программа загружается в систему H41q/H51q. Здесь необходимо проверить все разделы программы, подлежащие изменению. Тест изменения проверяет правильность целевого кода.
10. Если нарушения функционирования нет, необходимо создать резервную копию новой, актуальной программы. ПЭС может перейти в безопасный режим работы.

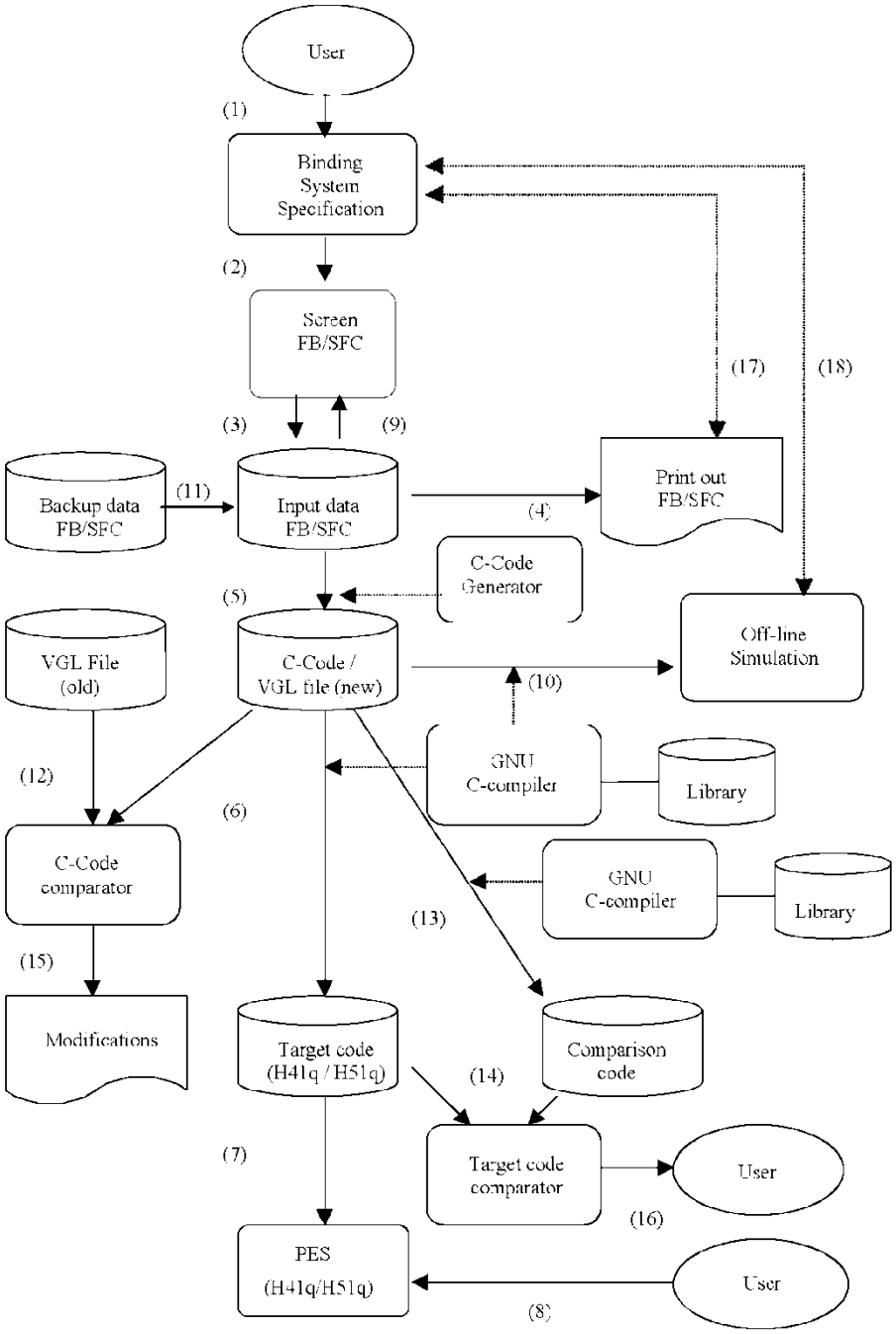


Рис. 2: Блок-схема, функция безопасного инструмента

7.2.3 Использование переменных и имен PCS

С помощью редактора описания переменных определяются имена переменных и их типы данных. Всем переменным прикладной программы присваиваются символические имена. Символические имена могут состоять макс. из 256 знаков.

Для физических входов и выходов используются символические имена PLT, они также могут состоять макс. из 256 знаков.

Использование символических имен вместо физического адреса имеет для пользователя два существенных преимущества:

- В прикладной программе используются обозначения установки для входов и выходов.
- Изменения в присвоении сигналов во входных и выходных каналах не оказывают влияния на прикладную программу.

7.2.3.1 Присвоение имен PCS именам переменных

В качестве основы для присвоения имен PLT именам переменных должен служить список точек измерения или список датчиков и исполнительных механизмов.

Присвоение имени переменной используемому аппаратному обеспечению производится в диалоговом окне для ресурсов, в *Edit Cabinet*. При этом необходимо внести следующие данные:

- Позиция модульной стойки (от 1-1 до 1-8 или от 2-1 до 2-8)
- Тип модульной стойки
- Слот и тип требуемого модуля
- Имена PLT, присваиваемые именам переменных

РЕКОМЕНДАЦИЯ Имя переменной и имя PLT должны быть практически одинаковыми.

Количество каналов (имен) на модуль зависит от используемого типа модуля. Необходимые тестовые программы для безопасных модулей ввода/вывода автоматически выполняются операционной системой.

Компания HIMA рекомендует объединять модули ввода и вывода в модульных стойках ввода/вывода в функциональные группы.

Основаниями для группировки могут быть:

- Группировка по компонентам установки
- Аналогичное расположение модулей в группах, напр.
  - цифровые/аналоговые компоненты установки
  - безопасные/небезопасные модули ввода/вывода
- резервные группировки в различных модульных стойках ввода/вывода в одинаковой последовательности
- Резервные модули или резервные каналы для последующей перезагрузки (перезагружаемый код)

7.2.3.2 Виды переменных

В зависимости от организационного блока программы (POU) — функциональных блоков или функции — можно определять различные виды переменных. В таблице ниже предлагается обзор:

Вид переменной	Прикладная программа PROG	Функциональный блок FB	Функция FUN	Использование
VAR	X (CONST[1)], RETAIN[2)])	X (CONST, RETAIN)	X (CONST)	Локальные переменные
VAR_INPUT	-	X	X	Входная переменная
VAR_OUTPUT	-	X (RETAIN)	X	Выходная переменная
VAR_EXTERNAL	-	X (CONST)	-	Внешне с/на другой POU
VAR_GLOBAL	X (CONST, RETAIN)	-	-	Глобально с другого POU
VAR_ACTION	X	X	X	В блоке действия языка последовательных функциональных схем

1) CONST: изменяемая во время проверки в режиме онлайн постоянная — без нового перевода прикладной программы. Она не может быть описана прикладной программой.

2) RETAIN: переменная со сцепляемостью, т. е. значение не теряется после отключения напряжения и его восстановления.

Таблица 22: Виды переменных в ELOP II

Неинициализированные переменные после холодного пуска установлены на значение 0 или FALSE.

7.2.3.3 Цифровые входы и выходы для булевских переменных

При определении ресурса проводится различие между цифровыми входами и выходами и цифровыми безопасными входами и выходами. Для безопасных функций должны использоваться только безопасные модули ввода/вывода. Для большинства безопасных модулей ввода/вывода в прикладной программе необходимо предусматривать стандартные модули HIMA, см. приложение.

Небезопасные модули ввода/вывода только читаются или описываются операционной системой и не подвергаются никакому дальнейшему тестированию. Вследствие этого неисправность не распознается операционной системой, сообщение о неисправности не появляется. Компания HIMA рекомендует для расширенной диагностики использовать только безопасные модули ввода/вывода.

7.2.3.4 Модули аналогового ввода/вывода

Модули аналогового ввода преобразуют аналоговые значения (напряжение, ток) в цифровые значения с 12-разрядным разрешением.

Модули аналогового вывода преобразуют 12-разрядные цифровые значения в ток 0...20 мА или 4...20 мА.

Для большинства аналоговых безопасных и небезопасных модулей ввода/вывода в прикладной программе следует использоваь модули HIMA, см. приложение.

7.2.3.5 Импортируемые или экспортируемые переменные

Данные импортируемых или экспортируемых переменных через интерфейсы передаются либо системе связи HIMA через HIPRO (ведущее устройство ПЭС), либо сторонним системам. Доступные протоколы для сторонних систем: Modbus, Modbus TCP, PROFIBUS-DP и 3964R. Данные можно передавать также через протокол Ethernet на сервер OPC. Переменные для импорта и экспорта обрабатываются в прикладной

программе как обычные входные и выходные переменные. Они определяются в описании переменных программной инстанции.

Булевские переменные можно снабдить атрибутом Event. События являются изменениями сигнала булевских переменных с дополнительной информацией о моменте (дата и время). Метка времени события с точностью до миллионной доли секунды соответствует времени устройства автоматизации.

7.2.4 Сигнатуры прикладной программы

Непреднамеренные или неавторизованные изменения в прикладной программе могут распознаваться несколькими сигнатурами CRC. Эти сигнатуры называются номерами версий. В ELOP II имеются следующие номера версий:

- Номер версии кода
- Номер версии RUN
- Номер версии данных
- Номер версии диапазона

7.2.4.1 Номер версии кода

Номер версии кода создается с помощью функций программируемой логики. Только если версия кода программы в системе управления и в инструменте программирования совпадают, через ПК можно наблюдать функцию системы управления.

На номер версии кода не оказывают влияние:

- Запись или удаление комментариев
- Установка или удаление полей онлайн-теста (поля OLT), т. е. информации инициализации
- Перемещение линий или модулей, если последовательность обработки не меняется
- Изменение параметров SIO, а не активация/деактивация параметров SIO
- Параметры шины.

Изменения базовых адресов для подсоединения стороннего устройства/Modbus могут привести к изменению номера версии кода. При всех других изменениях меняется также номер версии кода.

7.2.4.2 Номер версии RUN

Система управления создает номер версии Run во время эксплуатации. Сравнением с действительным до этого и документированным номером версии Run устанавливается, оказывалось ли за это время воздействие на программу в системе управления (видно при вызове индикаторной панели).

Номер версии Run изменяется при:

- другом номере версии кода (не для всех типов изменений)
- вставке или удалении модулей
- других системных параметрах
- вставке или удалении VAR_CONST
- изменении значений VAR_CONST
- изменении типа ресурса
- изменении настроек в режиме онлайн
- инициализации переменных входа/выхода в поле онлайн-теста
- изменении положения главного выключателя инициализации

7.2.4.3 Номер версии данных

Номер версии данных касается определения небезопасных импортируемых или экспортируемых переменных и изменяется в следующих случаях:

- Если изменяется имя переменной с атрибутами для HIPRO-N (не безопасно).
- Если такие переменные сжимаются при генерации неперезагружаемого кода (если имеются пробелы в области памяти).

7.2.4.4 Номер версии диапазона

Номер версии диапазона охватывает все установленные в проекте переменные и изменяется в следующих случаях:

- Удаление или добавление модулей в шкафу.
- Если установлено генерирование перезагружаемого кода, а атрибутам нижеперечисленных типов присвоено больше переменных в качестве удаленных:
- HIPRO-N, HIPRO-S, BUSCOM, событие, 3964R.
- Если установлено генерирование неперезагружаемого кода, а атрибутам нижеперечисленных типов добавляются или удаляются присвоенные переменные:

  HIPRO-N, HIPRO-S, BUSCOM, событие, 3964R.
- Если требуется новая организация запоминающего устройства, так как достигнут порог ЗУ.

Изменения базовых адресов для соединения стороннего устройства/Modbus могут привести к изменению номера версии диапазона.

7.2.5 Параметрирование устройства автоматизации

Перечисленные ниже параметры определяют поведение устройства автоматизации во время работы и настраиваются в меню **Resource Properties**.

7.2.5.1 Параметры защиты

В **Resource Properties** регулируются параметры защиты:

- Параметры для безопасной эксплуатации устройства автоматизации
- Операции, которые допустимы с помощью программирующего устройства при безопасной эксплуатации

Безопасные параметры		Рекомендуемая настройка
Возможна корректировка параметров в режиме онлайн		Reset, в зависимости от проекта
Параметры защиты		
	Safety Time in ms	В зависимости от процесса
	Watchdog Time in ms	макс. половина безопасного времени
	Requirement Class	6, соответствует уровню совокупной безопасности 3, в зависимости от проекта
Возможна корректировка значений		
	Constants	Reset
	Variables	Reset
	I/O Forcing	Reset
Допустимые операции		
	Test Mode	Reset
	Start	Reset
	Reload	в зависимости от проекта

Таблица 23: Безопасные параметры

i Для выходных сигналов операционной системы до (07.14) значение 255 с для безопасного времени **не** разрешено!

Допустим только диапазон значений **1…254 с**!

Настройки, которые могут задаваться во время безопасного режима, не привязаны к определенному требованию безопасности (SIL), для каждого применения устройства автоматизации они должны согласовываться с полномочным отделом контроля.

Изменение параметров защиты в режиме онлайн

В панели управления включается диалоговое окно *Change System Parameters*. Вкладка **Safety** служит для изменения параметров защиты в режиме онлайн. Если *Parameter Online Change* устанавливается на неизменяемые и передается в систему управления, то ни один из этих параметров нельзя изменить в режиме онлайн.

Однако это не видно из содержания вкладки. Поэтому можно менять параметры и передавать в систему управления в режиме онлайн. Однако система управления игнорирует последующие изменения в режиме онлайн, если *Parameter Online Change* установлена на неизменяемые.

Последующие изменения в режиме онлайн снова возможны только, если *Parameter Online Change* в прикладной программе установить на изменяемые и загрузить с помощью загрузки в систему управления.

7.2.5.2 Поведение при ошибках в безопасных выходных каналах

В следующей таблице представлены возможности настройки параметра *Behavior in Case of Output Faults*. Он находится во вкладке **I/O Parameters** диалогового окна *Properties* ресурса.

Настройка	Описание
Display only	Отключение посредством встроенного устройства предохранительного отключения выходного усилителя. Если это невозможно, отключение сигнала сторожевого устройства в модульной стойке ввода/вывода с помощью соединительного модуля (только системы H51q). Без отключения сигнала сторожевого устройства соответствующего центрального модуля (без остановки из-за ошибки). Прикладная программа и связь продолжают работать. **Допускается только до уровня совокупной безопасности 1!**
Emergency stop	Отключение сигнала сторожевого устройства соответствующего центрального модуля и вместе с этим отключение выходных каналов (остановка из-за ошибки). Прикладная программа и связь перестают работать.
Normal operation	Реакция, как при параметре *Display only*, дополнительно отключение соответствующей группы, если группа сконфигурирована с помощью модуля H8-STA-3, глава 9.2.1. Отключение сигнала сторожевого устройства соответствующего центрального модуля (остановка из-за ошибки), если группа не сконфигурирована или реле группы неисправно. В этом случае прикладная программа и связь перестают работать. **Требуется начиная с уровня совокупной безопасности 2.** **Обычные и рекомендуемые настройки.**

Таблица 24: Настройка параметра Behavior in Case of Output Faults

7.2.6 Идентификация программы

Прикладная программа однозначно идентифицируется с помощью номера версии кода. Таким образом однозначно определяется и соответствующая резервная копия (версия архива).

Если существует неуверенность, какая резервная копия правильная, компилируют спорную резервную копию с опцией загрузки и затем сравнивают целевой код с версией кода загруженной программы.

При перезагружаемом коде это возможно только, если резервная копия создана следующим образом:

1. Выполнить последнее изменение
2. Создать версию кода A, сгенерировав (скомпилировав) перезагружаемый код
3. Загрузить систему управления с версией кода A
4. Создать версию кода B, сгенерировав перезагружаемый код, который может быть идентичен версии A
5. Загрузить систему управления с версией кода B
6. При каждом последующем генерировании кода без изменения появляется версия кода B.

7.2.7 Проверка созданной прикладной программы на предмет соблюдения специальной функции безопасности

Для проверки создать подходящий набор вариантов проверки, охватывающий спецификацию. При этом не требуется выполнять 2^{20} вариантов теста для одного 20-канального логического элемента И. Как правило, независимого теста каждого входа и важных соединений достаточно. Данной тестовой последовательности достаточно, так как благодаря ELOP II и указанным в настоящем руководстве по безопасности мерам практически невозможно создание семантически и синтаксически корректного кода, который содержит еще не опознанные систематические ошибки процесса создания кода.

При числовом анализе формул также необходимо сгенерировать соответствующую тестовую последовательность. Имеет смысл, например, выполнить тесты класса эквивалентности, т.е. тесты в рамках определенного диапазона значений, при предельных значениях и в недопустимых диапазонах значений. Варианты теста следует выбирать таким образом, чтобы подтверждалась правильность расчета. Необходимое количество вариантов теста зависит от используемой формулы и должно охватывать критические пары значений.

При этом онлайн-тест может применяться в виде поддержки, например, чтобы задать значения и считать промежуточные значения. Требуется активное моделирование с источниками, так как только так можно подтвердить правильность проводки датчиков и исполнительных элементов. Кроме того, только так можно проверить конфигурацию системы.

7.3 Контрольный перечень: мероприятия по созданию прикладной программы

Контрольный перечень MEAP-0001-D доступен в виде файла Word на DVD-диске HIMA и в интернете по www.hima.de и www.hima.com.

7.4 Перезагрузка (перезагружаемый код)

i Перезагрузка допускается только после согласования с отделом контроля, ответственным за приемку установки. Во время всего процесса перезагрузки ответственное лицо должно обеспечивать контроль процесса с учетом сохранения функции безопасности посредством прочих технических и организационных мер.

⚠ ПРЕДУПРЕЖДЕНИЕ

Предупреждение! Опасность травмирования из-за нарушения функционирования!

Перед каждой перезагрузкой необходимо определить изменения в прикладной программе в отношении еще работающей прикладной программы с помощью сравнивающего устройства C-кода в безопасном инструменте ELOP II.

Изменения перезагрузки необходимо тщательно проверять на имитаторах перед передачей в ПЭС.

Если перезагрузка прикладной программы возможна в центральном(ых) модуле(ях), это отображается посредством сообщения Reloadable Code во время процесса перевода генератора кодов.

Для некоторых видов изменений в прикладной программе перезагружаемость пропадает, более подробную информацию и другие ограничения при перезагрузке см. в руководстве по операционной системе (HIQuad Operating System Manual HI 803 078 RU).

7.4.1 Системы с центральным модулем

В течение времени загрузки прикладной программы доступ к уровню ввода/вывода не происходит, т.е. модули ввода/вывода не читаются, не описываются или не тестируются.

Во время загрузки прикладной программы она не обрабатывает интерфейсы системы управления, не происходит передача импортируемых или экспортируемых переменных через интерфейсы.

i **Возможно прерывание работы!**

Если перезагрузка выполняется в системах с центральным модулем, ее необходимо завершить в течение безопасного времени процесса.

7.4.2 Системы с резервными центральными модулями

Для данных систем возможна перезагрузка без вышеуказанных ограничений для одноканальных систем.

Ход перезагрузки:

1. При загрузке первого центрального модуля второй центральный модуль продолжает обработку прикладной программы в монорежиме.
2. После этого вновь загруженный центральный модуль сохраняет актуальные данные еще находящегося в эксплуатации центрального модуля и принимает монорежим с новой прикладной программой.
3. После загрузки второго центрального модуля он сохраняет актуальные данные первого модуля, оба центральных модуля переходят в режим с резервированием.

7.5 Тест в режиме офлайн

Изменения в прикладной программе могут моделироваться с помощью теста в режиме офлайн в ELOP II. Данное моделирование является хорошим вспомогательным средством для анализа влияния изменения. Этого не достаточно, чтобы валидировать выполненные изменения в безопасных системах управления. Для этого требуется проверка в фактической системе управления или имитаторе.

7.6 Инициализация

Ответственность за инициализацию лежит на эксплуатирующей стороне!

Инициализация допускается только после согласования с отделом контроля, ответственным за приемку установки. Во время инициализации ответственное лицо должно обеспечивать контроль процесса с учетом сохранения функции безопасности посредством прочих технических и организационных мер.

Возможности при инициализации:

- Инициализацию можно запретить посредством конфигурации. Тогда ПЭС не принимает никакие значения инициализации, определенные пользователем. В этом случае новые значения инициализации могут устанавливаться только после отключения системы.
- При закрытии панели управления отображается, установлены ли значения инициализации, и в каком количестве.
- Все инициализированные входы или выходы могут сбрасываться двумя отдельными главными выключателями инициализации

Более подробную информацию по процедуре инициализации см. в руководстве по операционной системе (HIQuad Operating System Manual HI 803 078 RU) и онлайновой справке ELOP II.

⚠ ПРЕДУПРЕЖДЕНИЕ

Опасность травмирования персонала из-за непреднамеренной функции!

Перед началом безопасной работы необходимо удалить все маркеры инициализации из прикладной программы.

7.6.1 Удаление инициализированных переменных

Перед удалением переменных следует завершить инициализацию данных переменных!

Обоснование:

- Удаление инициализированной переменной и загрузка таких изменений в систему управления приводит к тому, что редактор инициализациии больше не отображает удаленную переменную. Это распространяется на все версии ELOP II до V5.1 730 IV3 включительно. С более новыми версиями ELOP II инициализация удаленных переменных может быть завершена и после процесса загрузки в редакторе инициализации.
- Объяснение этому заключается в том, что ранее присвоенный данной переменной вход инициализирует свойство и сохраняет значение инициализации.
- Вставка переменной в более поздний момент и ее присвоение инициализированному входу приводит к тому, что после загрузки с перезагрузкой инициализируется новая переменная непосредственно после перезагрузки!

Это может оказать воздействие на безопасность установки!

7.7 Функции прикладной программы

Программирование не ограничивается аппаратным обеспечением. Функции прикладной программы программируются произвольно. При программировании необходимо принимать во внимание, что на входах и выходах должен учитываться принцип тока покоя. Обрыв провода приводит, например, к отключению соответствующего исполнительного механизма.

- В прикладной программе для программируемых логических контроллеров, в отличие от встроенных безопасных систем управления, обрывы проводов учитывать не следует.
- Допускается выполнение произвольных логических операций «Нет».
- Активные сигналы для срабатывания действия (например, смещающий тактовый импульс для сдвигающего регистра) могут использоваться для безопасного применения.

Для аналоговых безопасных модулей ввода в случае ошибки далее обрабатывается заданное значение. Более подробные данные см. в описании модулей программного обеспечения в руководстве ELOP II, тип ресурса.

В цифровом безопасном модуле ввода/вывода в случае ошибки вход устанавливается на безопасное значение 0, а модуль цифрового вывода отключается встроенным безопасным отключением. Более подробные данные см. в описании модулей программного обеспечения в приложении.

По сравнению с интегрированными системами управления, программируемые логические контроллеры имеют более широкий объем функций, в частности, возможность обработки байтов и слов.

7.7.1 Групповое отключение

Безопасные модули вывода, используемые для определенной области установки (например, для горелки), могут объединяться в одну группу. Для этого в расчете на группу необходимо добавлять в прикладную программу модуль программного обеспечения H8-STA-3. На модуле программного обеспечения необходимо устанавливать все позиции относящихся к группе модулей вывода. Ошибка одного модуля вывода приводит к тому, что все относящиеся к этой группе модули вывода отключаются. Однако для безопасности системы достаточно лишь встроенного безопасного отключения модулей вывода.

7.7.2 Программные модули для отдельных безопасных модулей ввода/вывода

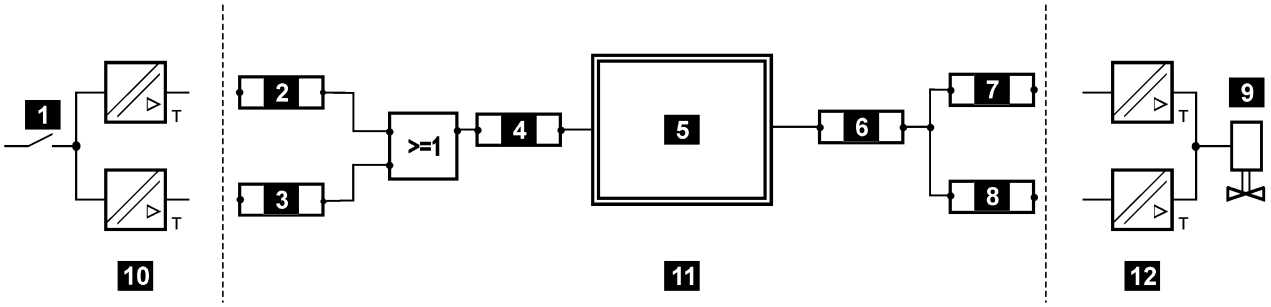
Модуль ввода		Модуль вывода	
Цифровой		Цифровой	
Тип	Программный модуль	Тип	Программный модуль
F 3237	HB-RTE-3	F 3331	HB-BLD-3 / -4
F 3238	HB-RTE-3	F 3334	HB-BLD-3 / -4
F 5220	HF-CNT-3 / -4	F 3349	HB-BLD-3 / -4
Аналоговый		Аналоговый	
F 6213	HA-RTE-3	F 6705	HZ-FAN-3
F 6214	HA-RTE-3		
F 6220	HF-TMP-3		
F 6221	HF-AIX-3		

Таблица 25: Присвоение программных модулей модулям ввода/вывода

Для безопасных модулей ввода/вывода в прикладную программу необходимо добавлять соответствующие программные модули. Более подробные сведения см. в главе 9.2 или в онлайн-справке ELOP II.

7.8 Резервные модули ввода/вывода

Для повышения готовности без ограничения безопасности могут параллельно подключаться безопасные модули ввода или вывода, как показано на следующей схеме. Максимальная готовность достигается, если в этом случае используются также устройства автоматизации с двумя шинами ввода/вывода, а резервные сигналы входа/выхода проводятся также на отдельные модули ввода/вывода.



1 Датчик
2 Сигнал входа 1
3 Сигнал входа 2
4 Входная переменная
5 Логическая схема программы
6 Выходная переменная
7 Выходной сигнал 1
8 Выходной сигнал 2
9 Исполнительный элемент
10 Подсоединение входов (аппаратное обеспечение)
11 Прикладная программа (программное обеспечение)
12 Подсоединение выходов (аппаратное обеспечение)

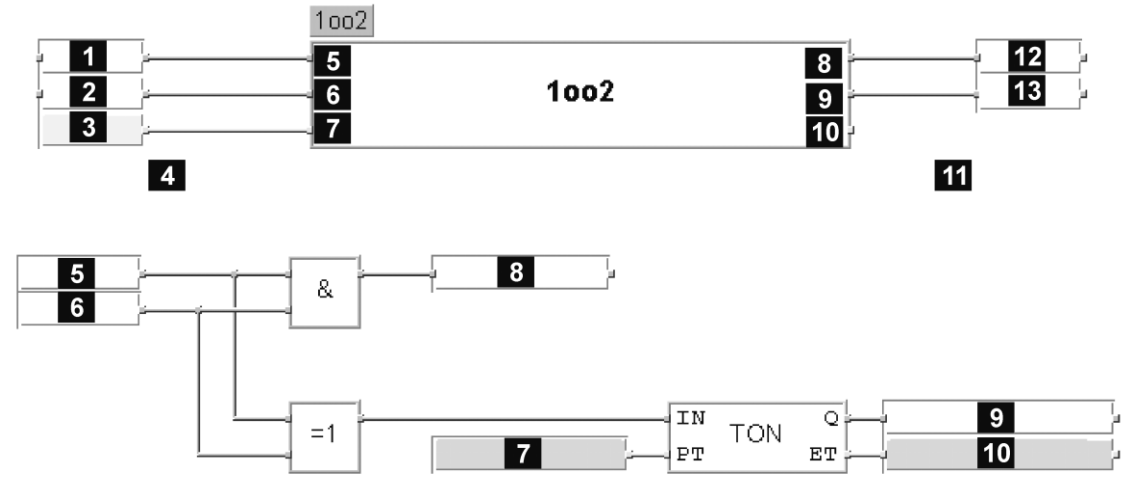
Рис. 3: Резервные модули ввода/вывода для повышения готовности

7.8.1 Резервные, небезопасные датчики

7.8.1.1 Аппаратное обеспечение

В зависимости от управляющего сигнала (механический контакт, инициатор, искробезопасный/неискробезопасный) необходимо использовать модули ввода типа F 3236, F 3237 или F 3238. Оба датчика работают в схеме 1oo2, т. е. при срабатывании датчика сразу же отключается безопасная коммутируемая цепь. По истечении заданного времени выдается сообщение о рассогласовании. Данная функциональность может обобщаться в функциональном модуле для модуля ввода F 3236. Для модулей F 3237 и F 3238 имеется модуль HB—RTE-3 с последующим контролем цепей инициатора.

7.8.1.2 Прикладная программа, модуль ввода F 3236



1 Сигнал датчика 1
2 Сигнал датчика 2
3 Время рассогласования, например 1 с
4 Входные сигналы
5 Вход модуля *Sensor1*
6 Вход модуля *Sensor2*
7 Вход модуля *Discrepancy Time*
8 Выход модуля *Control Signal*
9 Выход модуля *Discrepancy Signal*
10 Выход модуля *Discrepancy Time* Actual *Value*
11 Сигналы к логической схеме или цепи сигнализации
12 Переменная для последующей обработки управляющего сигнала
13 Переменная для последующей обработки сигнала рассогласования

Рис. 4: Пример для функционального модуля 1oo2 и логической схемы модуля

Управляющий сигнал имеет значение TRUE, если оба датчика имеют значение TRUE.

Сигнал рассогласования имеет значение TRUE, если сигналы датчика по истечении времени рассогласования различны.

7.8.1.3 Прикладная программа, модуль ввода F 3237 или F 3238

Использование модуля HB-RTE-3

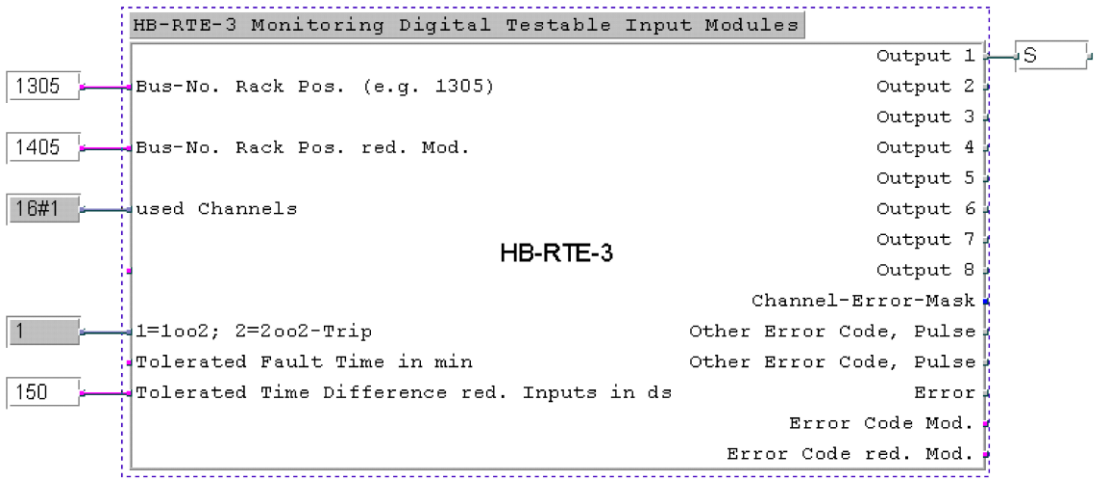


Рис. 5: Использование модуля HB-RTE-3

Сигналы S-1 и S-2 подключены непосредственно на первые каналы модуля F 3237 или F 3238. Другое аппаратное обеспечение не присвоено.

7.8.1.4 Оценка безопасности

При срабатывании одного из двух датчиков или отказе компонента в системе выход отключается.

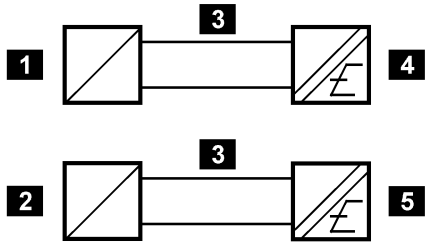
Для применений датчиков необходимо соблюдать соответствующие стандарты, например IEC 61511.

7.8.1.5 Оценка готовности

Готовность отсутствует, так как каждый отказ компонента приводит в отключению.

7.8.2 Аналоговые резервные датчики

7.8.2.1 Подсоединение аппаратного обеспечения

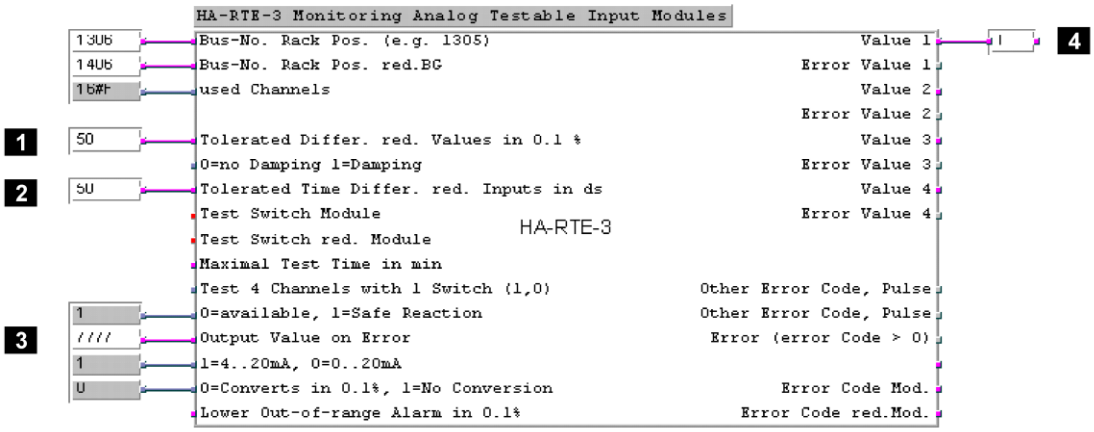


1 Трансмиттер 1
2 Трансмиттер 2
3 4…20 мА
4 T1
5 T2

Рис. 6: Подсоединение резервных датчиков

7.8.2.2 Прикладная программа для модуля ввода F 6213 или F 6214

Использование модуля HA-RTE-3, более подробную информацию по модулю см. в главе 9.2.2 и онлайн-справке ELOP II.



1 Например 50

2 Например 50

3 7777, если физическая величина в случае опасности становится больше (все четыре канала модуля),

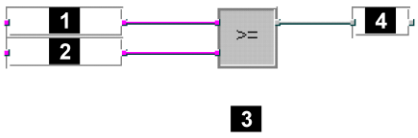
0000, если физическая величина в случае опасности становится меньше (все четыре канала модуля)

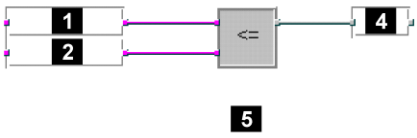
4 Значения 0...1066

Рис. 7: Использование модуля HA-RTE-3 при F 6213 или F 6214

Сигналы T1 и T2 заложены непосредственно на первые каналы модуля F 6213 или F 6214. Дальнейшее присвоение аппаратного обеспечения не производится.

Два примера для элемента сравнивающего устройства для сигнализации или отключения при достижении допустимого предельного значения:





1 Сравниваемая переменная, например измеренное значение

2 Контрольное значение

3 Элемент сравнивающего устройства для сигнализации

4 Результат сравнения

5 Элемент сравнивающего устройства для отключения

Рис. 8: Элементы сравнивающего устройства для сигнализации или отключения при достижении допустимого предельного значения

7.8.2.3 Оценка безопасности

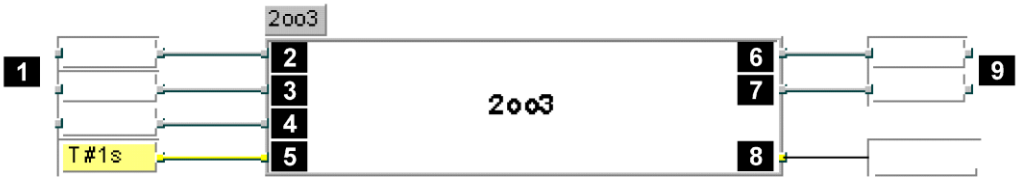
При срабатывании одного из двух датчиков или отказе компонента в системе выход A имеет высокий уровень напряжения.

Для применений датчиков необходимо соблюдать соответствующие стандарты, например IEC 61511.

7.8.2.4 Оценка готовности

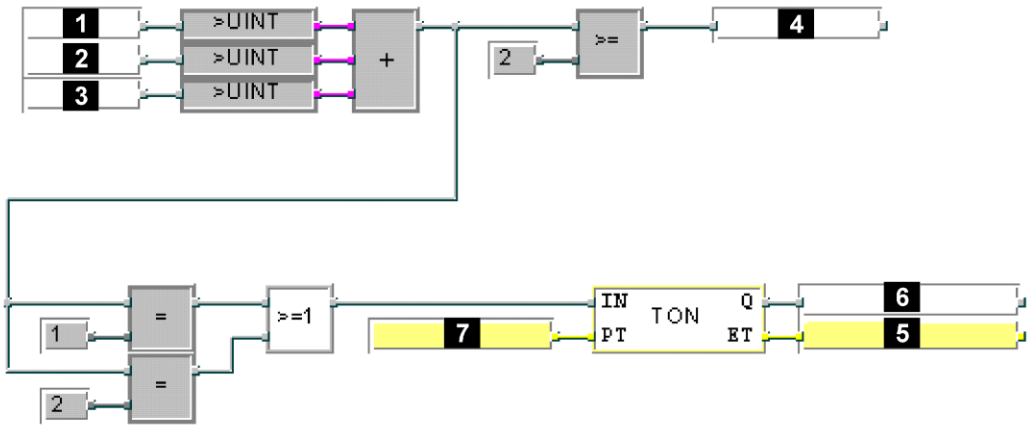
Готовность отсутствует, так как каждый отказ компонента или срабатывание датчика приводит к отключению.

7.8.3 Модули ввода с подключением 2oo3



1. Сигналы от трех различных модулей ввода
2. Вход модуля для датчика 1
3. Вход модуля для датчика 2
4. Вход модуля для датчика 3
5. Вход модуля для времении рассогласования
6. Выход модуля для сигнала результата
7. Выход модуля для сигнала рассогласования
8. Выход модуля для фактического значения времени рассогласования
9. Сигналы к логической схеме или цепи сигнализации

Рис. 9: Функциональный блок 2oo3



1. Датчик 1
2. Датчик 2
3. Датчик 3
4. Сигнал результата
5. Время рассогласования
6. Сигнал рассогласования
7. Фактическое значение времени рассогласования

Рис. 10: Структура функционального блока 2oo3

Представленная схема целесообразно обобщена в функциональном блоке 2oo3.

Управляющий сигнал имеет значение TRUE, если два или три датчика имеют значение TRUE.

Сигнал рассогласования имеет значение TRUE, если один или два датчика по истечении времени рассогласования имеют значение TRUE.

При ПЭС с двумя шинами ввода/вывода сигнал второго датчика разветвляется на два входных канала (соответственно один канал в шине ввода/вывода 1 и один канал в шине ввода/вывода 2) и проводится в прикладной программе через функцию ИЛИ. Также все сигналы датчиков могут подключаться параллельно на выходные каналы на обеих шинах ввода/вывода и связываться с помощью функции ИЛИ.

Для применений датчиков необходимо соблюдать соответствующие стандарты, например IEC 61511.

7.9 Проектная документация для безопасных применений

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

- Описание интерфейсов
- Список переменных
- Логическая схема
- Описание типов данных
- Конфигурации для шкафа, модульных стоек, модулей и параметров системы
- Перекрестная ссылка PLT/переменные
- Информация по генератору кодов

Структура различных типов документов может задаваться в произвольном порядке.

Документация является составляющей частью функциональной приемки установки, требующей разрешения, отделом контроля (напр. TÜV). Приемка касается только функции пользователя, а не безопасных устройств автоматизации HIMA H41q-MS, H51q MS, H41q-HS, H51q HS, H41q-HRS, H51q HRS, которые уже прошли испытание типового образца.

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

7.10 Аспекты безопасности для связи (безопасная передача данных)

Протокол HIPRO-S сертифицирован для уровня совокупной безопасности 3.

7.10.1 Безопасная связь

В диалоговом окне *Properties* для ресурсов (вкладка **HIPRO-S**, **Edit** выделенного ресурса) обмен данными с безопасно назначенными ресурсами может контролироваться через ведущее устройство ПЭС. Для этого время контроля можно указать в качестве параметра *Time Interval,* а также активировать опцию *Reset Imported Variables* при превышении времени контроля.

Устанавливаемое время контроля зависит от процесса, согласование производится с органом, осуществляющим приемку.

Безопасная связь может осуществляться также через сертифицированный TÜV протокол safe**ethernet** с помощью коммуникационных модулей Ethernet F 8627X или F 8628X.

7.10.2 Временные требования

При последовательном соединении компания HIMA рекомендует по причинам постоянного времени передачи предусмотреть собственное ведущее устройство ПЭС и собственную шину для безопасной передачи данных со скоростью 57,6 кбит/с.

Время передачи данных T_T от смены значения датчика на ПЭС до реакции на выходе другого ПЭС:

$T_T = 2*CT_1 + 2*T_D + 2*CT_2$

CT_1 Время цикла ПЭС 1

CT_2 Время цикла ПЭС 2

T_D Время передачи данных между двумя ПЭС, зависит от используемого соединения в сети передачи данных:

- Последовательная передача: здесь необходимо принимать значение времени цикла шины. Информацию о времени цикла шины см. руководство по операционной системе (HIQuad Operating System Manual HI 803 078 RU).
- Передача через Ethernet: в этом случае принимать максимальное время передачи (T_{max}), см. технический паспорт модуля F 8627X, (HIQuad F 8627X Manual HI 803 129 RU).

7.10.3 Указания по созданию прикладной программы

Задание конфигурации сети Ethernet в ELOP II для HIPRO-S производится автоматически. При составлении прикладной программы следует, однако, учитывать следующие указания:

- Имя ресурса в ELOP II должно состоять из восьми знаков, при этом последние два знака должны быть цифрами. Допускаются цифры в диапазоне от 1 до 99. Цифры должны быть однозначными, чтобы исключались конфликты при их использовании для определения IP-адреса коммуникационного модуля.
- Безопасную связь с HIPRO-S в нормальном режиме работы следует устанавливать таким образом, чтобы каждое устройство автоматизации конфигурировало безопасный обмен данными (т.е. обмен эквивалентными данными, если не производится обмен данными пользователя) с каждым другим устройством.
- При использовании режима HIPRO-S-DIRECT обмен эквивалентными данными не требуется. Подробности см. в техническом паспорте F 8627X, (HIQuad F 8627X Manual HI 803 129 RU).
- Для контроля конфигурации HIPRO-S следует компилировать программу ведущего устройства ПЭС. Затем следует исправить возникшие ошибки.
- При безопасной связи для данных передачи следует использовать нуль в качестве безопасного значения.

8 Использование для приемно-контрольных приборов пожарной сигнализации согласно

Системы H41q и H51q могут использоваться в приемно-контрольных приборах пожарной сигнализации согласно DIN EN 54-2 и NFPA 72.

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

Система H41q и H51q может легко достигать предписанного DIN EN 54-2 максимального времени цикла приемно-контрольных устройств пожарной сигнализации в 10 секунд, а также требуемого в некоторых случаях безопасного времени в 1 с (время реакции при ошибке), поскольку время цикла в данной системе может находиться в диапазоне < 0,5 с.

Подключение пожарного извещателя осуществляется по принципу рабочего тока с контролем линии на короткое замыкание и обрыв. Для этого могут использоваться модули ввода F 3237/F 3238 для логических подключений или F 6217/F 6221 для аналоговых подключений по следующей схеме:

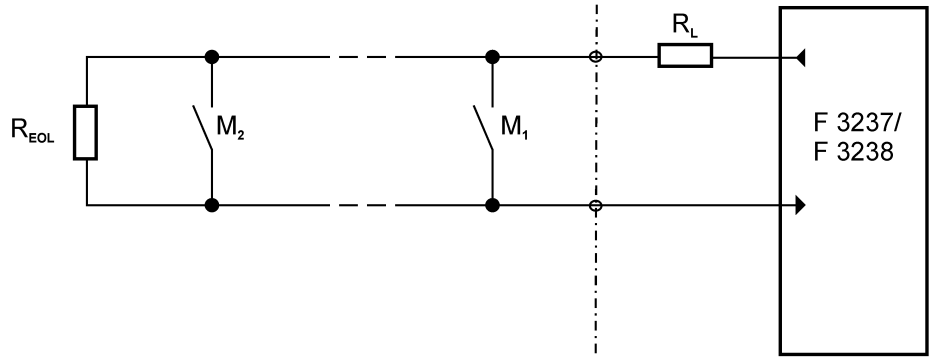
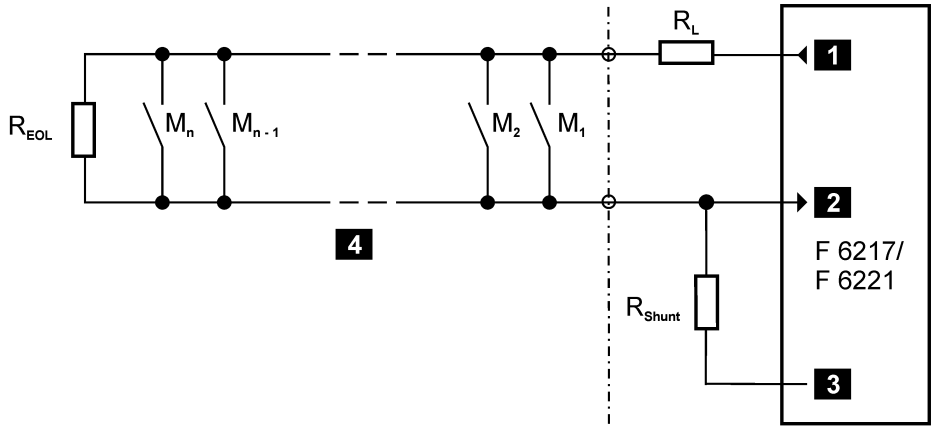


Рис. 11: Подключение пожарных извещателей с цифровыми входами



1 Питание датчика
2 Аналоговый вход
3 Опорный полюс (L-)
4 Сигнальный контур

Рис. 12: Подключение пожарных извещателей с аналоговыми входами

Пояснения к Рис. 11 и Рис. 12:

M	Пожарный извещатель
R_{EOL}	Нагрузочное сопротивление на последнем датчике контура
R_L	Ограничение максимально допустимого тока контура
R_{Shunt}	Измерительное сопротивление

Для применения необходимо рассчитать сопротивление R_{EOL}, R_L и $R_{шунт}$ в зависимости от используемых датчиков и числа датчиков в каждом сигнальном контуре. Для этого необходимо учитывать технические паспорта изготовителей датчиков.

Дополнительно следует обращать внимание на соблюдение специфицированных значений по току модулей F 3237 или F 3238 (см. технические паспорта). В частности это имеет значение, если пожарные извещатели не имеют механических контактов, а только электронные выходы.

Выходы сигнала тревоги для управления лампами, сиренами, акустическими сигналами и т. д. работают по принципу рабочего тока, т. е. необходимо использовать модули вывода с контролем цепей на замыкание и обрыв линии, например типы модулей F 3331 или F 3334.

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

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

Передача сообщений пожарной сигнализации от системы HIMA к системе HIMA может быть реализована с помощью имеющихся стандартов связи, таких как Modbus, HIPRO-S, OPC (Ethernet). Контроль связи является составной частью прикладной программы. Компания HIMA рекомендует выполнять связь с резервированием, чтобы при неисправности компонента отрезка передачи (провод, ошибки аппаратного обеспечения и т.д.) все же обеспечивалась связь. В случае отказа компонента должно выдаваться сообщение, а неисправный компонент необходимо заменить или отремонтировать во время эксплуатации.

Системы H41q или H51q, используемые в качестве приемно-контрольных приборов пожарной сигнализации, должны иметь резервный источник питания. Необходимо также принять меры на случай сбоя в электроснабжении, например, установить акустический сигнал, работающий от аккумулятора. Переключение между электроснабжением от сети и резервным источником питания должно производиться достаточно быстро, чтобы гарантировать бесперебойную эксплуатацию. Допускаются провалы напряжения до 10 мс.

При сбоях системы операционная система описывает системные переменные, анализируемые в прикладной программе. Это позволяет программировать сигнализацию неисправностей на распознаваемые системой ошибки. Безопасные входы и выходы в случае ошибки отключаются, т. е. на всех каналах модуля ввода, содержащего ошибку, обрабатывается низкий уровень и отключаются все каналы модуля вывода, содержащего ошибку.

Для установок пожарной сигнализации согласно EN 54-2 и NFPA 72 следует использовать устройство контроля короткого замыкания на землю.

9 Стандартные функциональные блоки

В таблицах ниже перечислены стандартные функциональные блоки HIMA для безопасного применения. Функциональные описания блоков доступны в онлайн-справке.

В следующем тексте стандартные блоки называются сокращенно «Модули».

9.1 Модули независимо от модулей ввода/вывода

Для функций центральных модулей могут вызываться и задействоваться стандартные программные модули. Подробное описание данных модулей см. в онлайн-справке соответствующего модуля.

Тип	Функция	Испытание TÜV[1)]	
		Безопасный	без обратного воздействия на источник
H8-UHR-3	Дата и время		•
HA-LIN-3	Линеаризация температуры	•	•
HA-PID-3	PID-регулятор	•	•
HA-PMU-3	Параметрируемый измерительный преобразователь	•	•
HK-AGM-3	Контроль ведущего устройства ПЭС		•
HK-COM-3	Контроль коммуникационного модуля		•
HK-LGP-3	Оценка и конфигурирование LGP		•
HK-MMT-3	Ведущее устройство Modbus		•

[1)] В столбце «Испытание TÜV» знаком «•» обозначены модули, для которых имеется подтверждение безопасности TÜV. Для безопасного применения модулей мы отсылаем к документации модулей.

Таблица 26: Стандартные функциональные модули независимо от уровня ввода/вывода

Следующие модули могут использоваться в безопасных применениях, но не для безопасных операций:

- H8-UHR-3
- HK-AGM-3
- HK-LGP-3
- HK-MMT-3

9.1.1 Модуль H8-UHR-3

Модуль позволяет внешнюю установку или изменение даты и времени устройства автоматизации.

Выходы модуля служат только для информации, от них нельзя производить никаких безопасных операций в прикладной программе.

9.1.2 Модуль HA-LIN-3

Модуль служит для линеаризации измерений температуры с термоэлементами и термометрами сопротивления Pt 100. Необходимо проверить правильность параметрирования, если используются значения для отключения безопасных соответствующих цепей (см. онлайн-справку ELOP II).

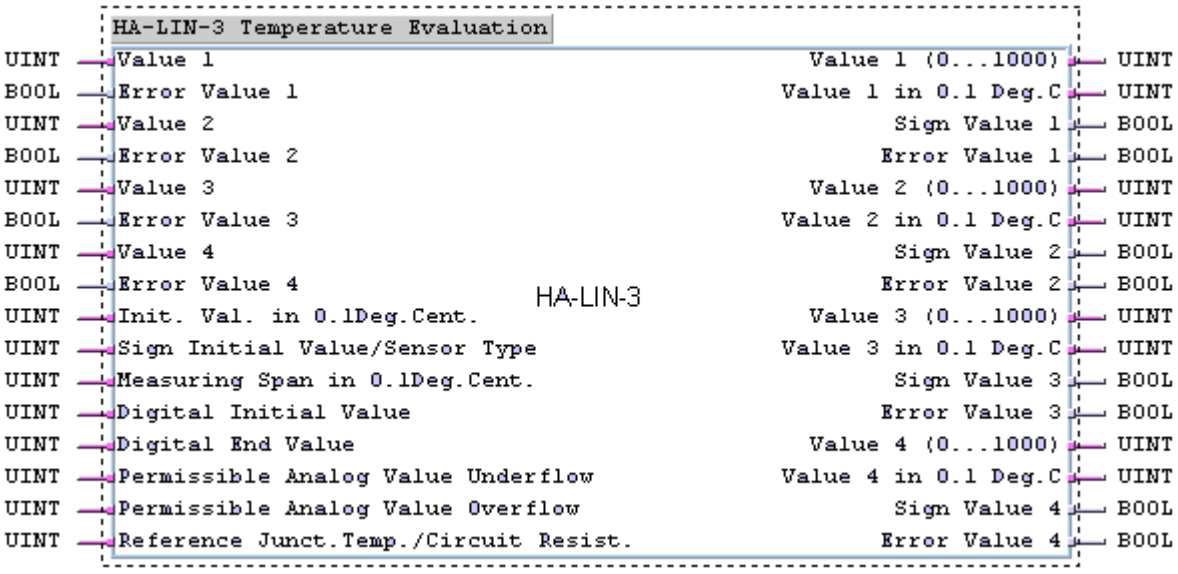


Рис. 13: Подключения модуля HA-LIN-3

9.1.3 Модуль HA-PID-3

Модуль содержит цифровой регулятор, который может эксплуатироваться в устройствах с принципом работы P, I, D, PI, PD и PID.

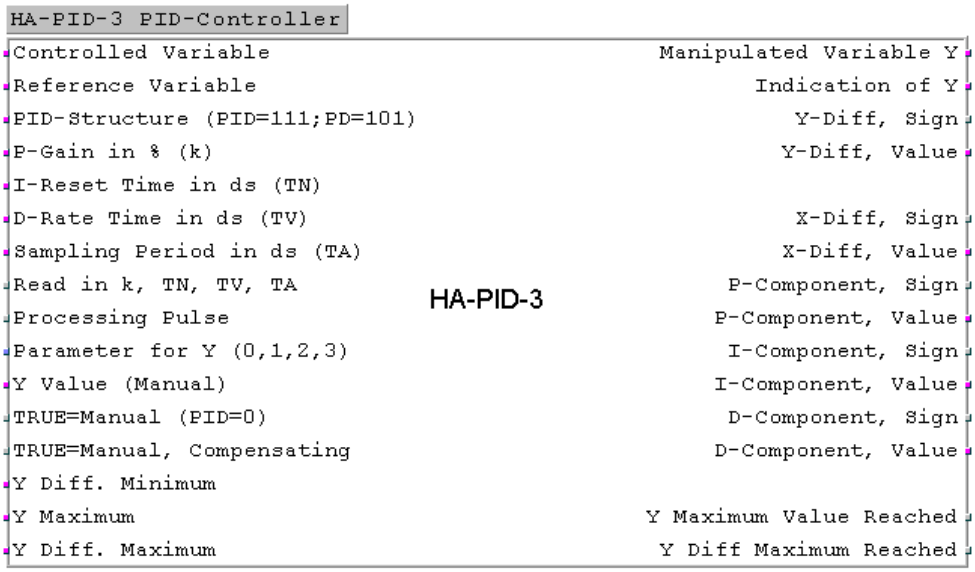


Рис. 14: Подключения модуля HA-PID-3

9.1.3.1 Входы

True=Manual (PID=0), *True=Manual, Compensating*	Для безопасной эксплуатации модуля регулирования данные входы занимать нельзя. Отклонения должны быть утверждены органом, отвечающим за допуск в эксплуатацию. Изменение параметров и констант на входах модулей без остановки системы допускается только с разрешения органа, отвечающего за допуск в эксплуатацию, и в контролируемом режиме. Назначение входов модуля с небезопасными импортируемыми переменными не допускается.

9.1.3.2 Выходы:

Безопасные отключения допускаются только через параметры:

Maximum Value Reached и *Diff Maximum Reached*

Отклонения должны быть утверждены органом, отвечающим за допуск в эксплуатацию.

i Алгоритм регулирования модуля не в каждом случае может обеспечить безопасное состояние установки. В каждом конкретном случае требуются дополнительные мероприятия.

9.1.4 Модуль HA-PMU-3

Модуль служит как для преобразования цифровых измеренных значений в формат представления значений в тысячных, так и для преобразования значений в тысячных в оцифрованные аналоговые значения. Необходимо проверить правильность параметрирования, если используются значения для отключения безопасных соответствующих цепей (см. онлайн-справку ELOP II).

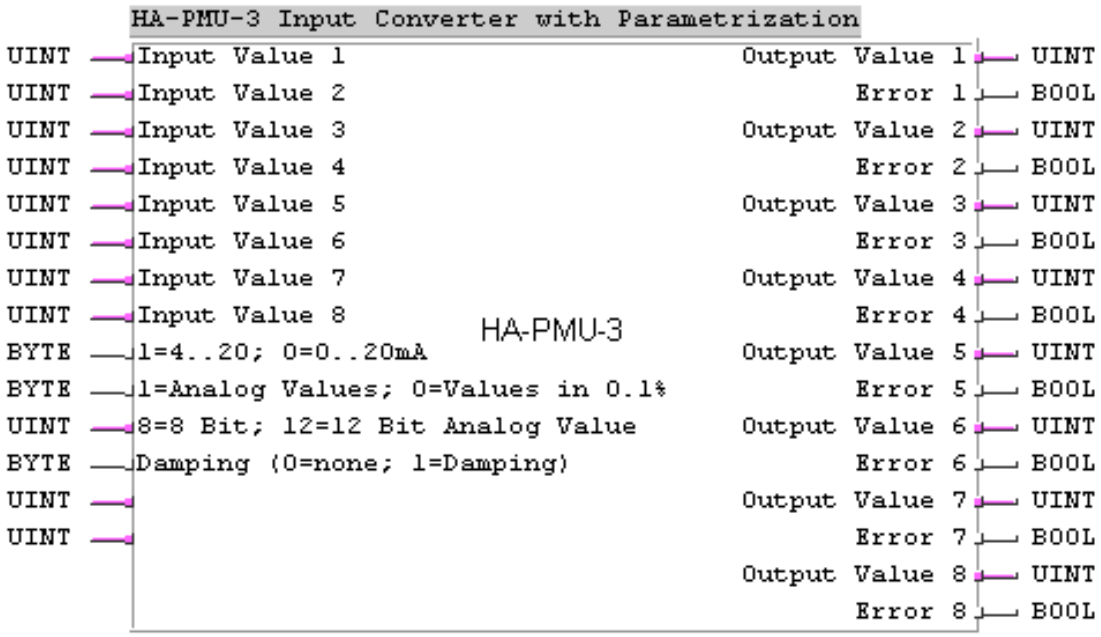


Рис. 15: Подключения модуля HA-PMU-3

9.1.5 Модуль HIMA HK-AGM-3

С помощью данного модуля контролируется функция устройства автоматизации H41qc или H51q в качестве ведущего устройства HIPRO.

Модуль не имеет отношения к безопасности. Выходы модуля служат только для информации, от них нельзя производить никаких безопасных операций в прикладной программе.

9.1.6 Модуль HK-COM-3

С помощью данного модуля контролируется функция коммуникационных модулей в системе H51q.

Модуль не имеет отношения к безопасности. Выходы модуля служат только для информации, от них нельзя производить никаких безопасных операций в прикладной программе.

9.1.7 Модуль HK-LGP-3

Модуль служит для анализа и конфигурации записи события и переключения между Modbus и LCL (logic-plan controlled logging, протоколирование, управляемое планом логической схемы).

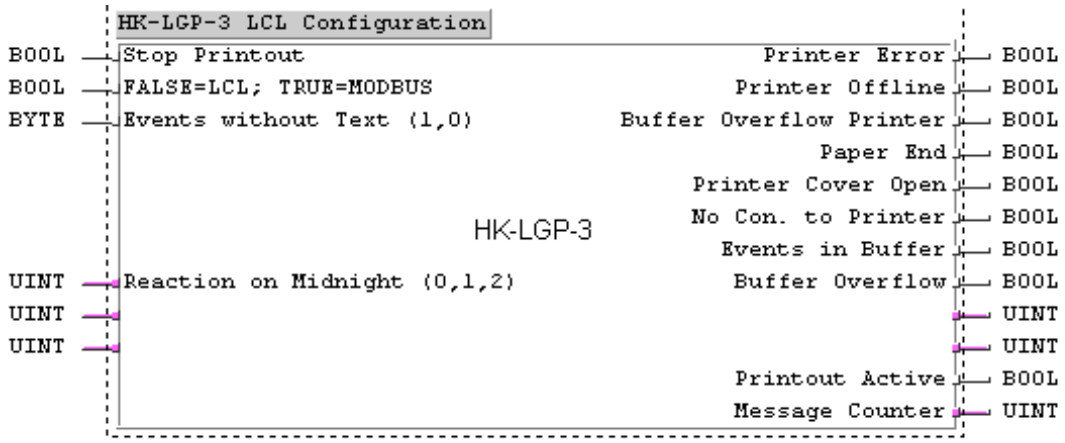


Рис. 16: Подключения модуля HK-LGP-3

Модуль не имеет отношения к безопасности. Выходы модуля служат только для информации. Они не должны использоваться для программирования безопасных реакций в прикладной программе.

9.1.8 Модуль HK-MMT-3

С помощью данного модуля устройство автоматизации H41q или H51q можно использовать в качестве ведущего устройства Modbus.

Модуль не имеет отношения к безопасности. Выходы модуля служат только для информации, от них нельзя производить никаких безопасных операций в прикладной программе.

9.2 Модули в зависимости от модулей ввода/вывода

Все описываемые ниже программные модули допущены для эксплуатации в безопасных устройствах автоматизации.

Тип	Функция	Испытание TÜV[1)]	
		Безопасный	без обратного воздействия на источник
H8-STA-3	Создание группы безопасных тестируемых выходов	•	•
HA-RTE-3	Контроль аналоговых тестируемых модулей ввода F 6213/F 6214	•	•
HB-BLD-3	Диагностика модулей и линий тестируемых выходов	•	•
HB-BLD-4	Диагностика модулей и линий тестируемых выходов	•	•
HB-RTE-3	Контроль двоичных тестируемых модулей ввода	•	•
HF-AIX-3	Контроль аналоговых тестируемых модулей ввода F 6221	•	•
HF-CNT-3	Модуль счетчика для модуля F 5220	•	•
HF-CNT-4	Модуль счетчика для модуля F 5220	•	•
HF-TMP-3	Модуль конфигурации для F 6220	•	•
HZ-DOS-3	Диагностика без безопасности		•
HZ-FAN-3	Индикация ошибок для тестируемых модулей ввода/вывода		•

[1)] В столбце «Испытание TÜV» знаком «•» обозначены модули, для которых имеется подтверждение безопасности TÜV. Для безопасного применения модулей мы отсылаем к документации модулей.

Таблица 27: Стандартные функциональные блоки в зависимости от уровня ввода/вывода

Следующие модули могут использоваться в безопасных применениях, но не для безопасных операций:

- HZ-FAN-3
- HZ-DOS-3

HIMA Необходимо соблюдать описанные в данной главе отдельные указания по программированию.

Для более точной информации о функциях программных модулей и назначении входов и выходов следует использовать онлайн-справку соответствующего модуля.

9.2.1 Модуль H8-STA-3

Модуль используется для конфигурирования группового отключения. Он используется для каждой группы отключения однократно в прикладной программе.

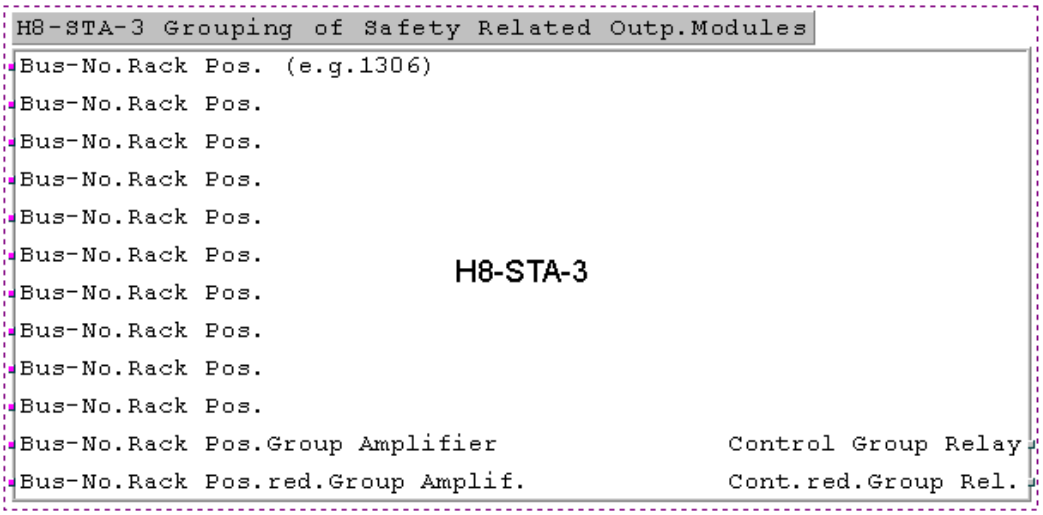


Рис. 17: Подключения модуля H8-STA-3

О порядке действий при возникновении ошибок выходных каналов см. в главе 6.

9.2.1.1 Входы

Позиции относящихся к группе отключения модулей задаются в виде четырехзначного десятичного числа в соответствии с настройками в выбранном ресурсе.

Пример: «1306» означает:

Шкаф 1, модульная стойка 3, позиция модуля 06

При использовании модулей со встроенным предохранительным отключением необходимо занимать один из входов *Bus No. Rack Pos. Group Amplif.* или *Bus No. Rack Pos. red. Group Amplif*. Здесь необходимо внести имеющийся, но не оснащенный слот.

i Модули вывода со встроенным предохранительным отключением не требуют группового отключения. Однако оно может задаваться и для данных модулей. Тогда ошибка модуля вывода приводит к отключению всех модулей, относящихся к группе (в соответствии с данными в модуле H8-STA-3).

9.2.2 Модуль HA-RTE-3

Модуль служит для последующей обработки и индикации ошибок для аналоговых безопасных модулей ввода при одноканальном режиме или режиме с резервированием. Он должен использоваться для каждого безопасного аналогового модуля ввода (F 6213) однократно в прикладной программе. Для случаев, когда используются два резервных модуля ввода/вывода, модуль должен иметься в прикладной программе только однократно.

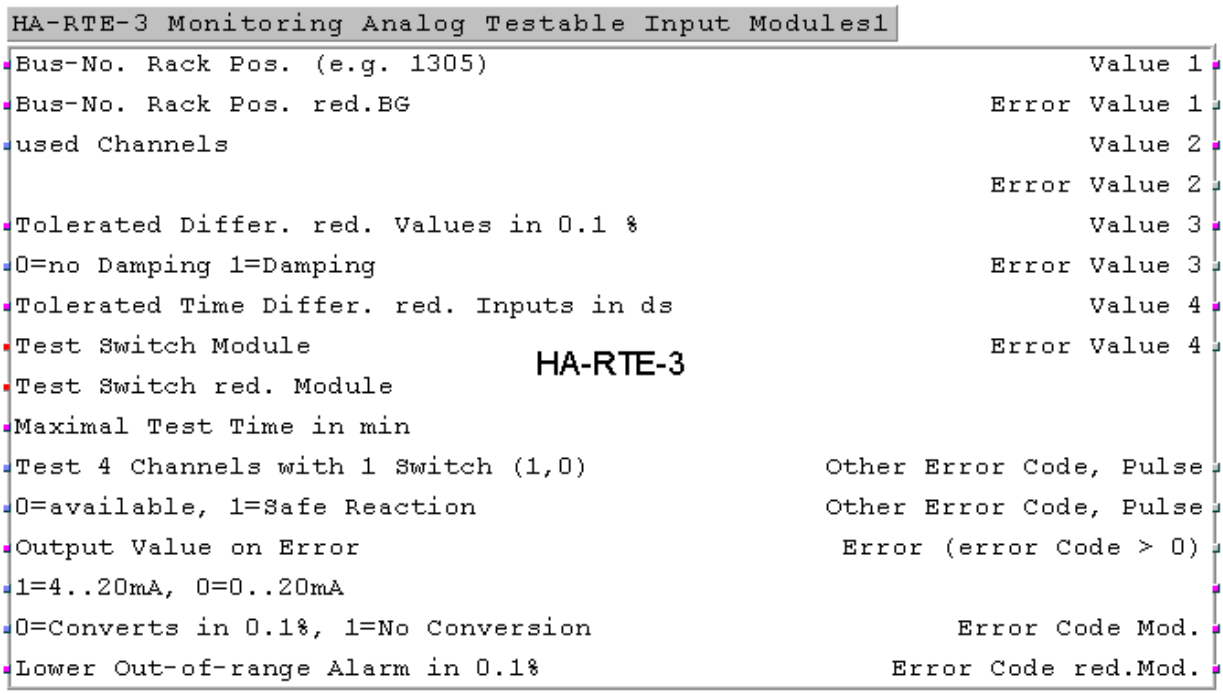


Рис. 18: Подключения модуля HA-RTE-3

9.2.2.1 Входы

Bus No. Rack Pos. (например, 1305) *Bus No. Rack Pos. red. Mod.*	Позиция безопасного аналогового модуля ввода и резервного модуля (при наличии такового) в виде 4-значного десятичного числа: Пример: «1305» означает: Шкаф 1, модульная стойка 3, позиция модуля 05 (в режиме с резервированием резервный модуль должен получать другое положение)
0 = нет; 1 = демпфирование	1 только для режима с резервированием. Разность актуального значения и значения предыдущего цикла прибавляется к допустимой разности в ‰ (допустимая разность резервных значений в тысячных).
Maximum Test Time in min	Ограничение времени проверки в минутах. По истечении времени проверки снова обрабатывается фактическое значение в прикладной логической схеме.

9.2.2.2 Выходы

Value 1...4	Использование значений необходимо проверить, если они используются для отключения безопасных цепей.
Error Value 1...4	Выходы должны быть заняты, чтобы в случае ошибки с булевским сигналом срабатывало отключение.

Другие выходы служат только для информации, из них не должны выводиться безопасные операции в прикладной программе.

9.2.3 Модуль HB-BLD-3

Модуль служит для анализа ошибок и индикации ошибок соответствующих каналов в цифровых безопасных модулях вывода F 3331, F 3334 и F 3349. Для каждого используемого модуля он может использовать только однократно.

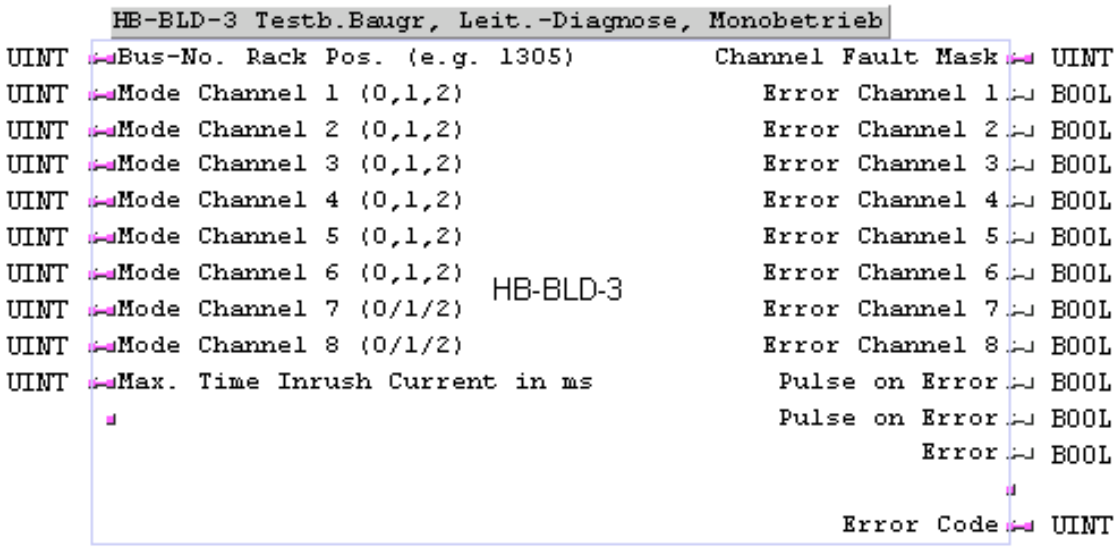


Рис. 19: Подключения модуля HB-BLD-3

Входы

Bus No. Rack Pos. (например, 1305)

Позиция безопасного цифрового модуля вывода в виде 4-значного десятичного числа, пример: «1305» означает:
Шкаф 1, модульная стойка 3, позиция модуля 05

Mode Channel n (0/1/2)

Назначение	Значение
1	Нормальный режим, сообщается об обнаруженной ошибке с высоким уровнем на соответствующем выходе «Ошибка канала n» (Error Channel n), цепь выхода модуля закрыта.
0	Анализ ошибки, сообщения об ошибках блокируются
2	Допускается только для некоторых установок, инверсный режим, т. е. цепь выхода должна быть открыта
> 2	Диапазон значения превышен: канал интерпретируется как неисправный (TRUE на выходе) и выдается сообщение о неисправности соответствующего канала.

В безопасных цепях управления следует использовать принцип тока покоя.

Max. Time Inrush Current in ms

Определение времени ожидания для распознавания обрыва линии или времени для установления допуска ограничения тока. В течение данного времени блокируется индикация неисправностей. Увеличение времени ожидания влечет за собой увеличение времени цикла.

9.2.3.1 Выходы

Выходы *Pulse on Error (2x), Error* и *Error Code* служат только для информации, они не должны использоваться для программирования безопасных реакций в прикладной программе.

Прочие выходы можно использовать для безопасных реакций.

9.2.4 Модуль HB—BLD--4

Модуль служит для анализа ошибок соответствующего модуля и индикации неисправностей для цифровых безопасных модулей вывода F 3331, F 3334 и F 3349 для режима с резервированием. Он может использоваться для резервной пары модулей только однократно.

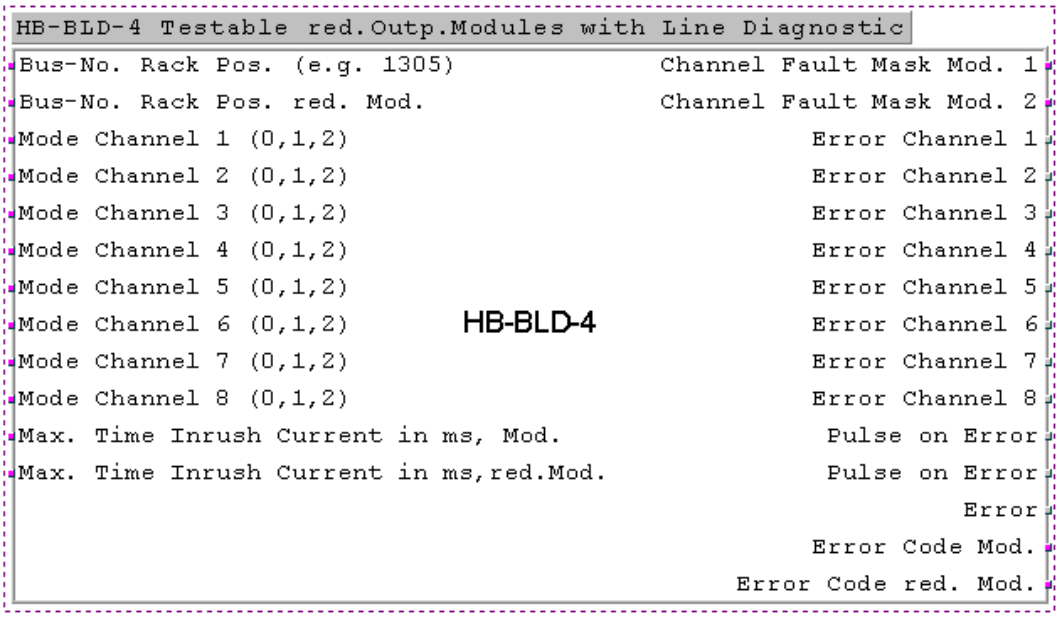


Рис. 20: Подключения модуля HB-BLD-4

9.2.4.1 Входы

Bus No. Rack Pos. (например, 1305)
Bus No. Rack Pos. red. Mod.

Позиция безопасного цифрового модуля вывода и при наличии резервного модуля в виде 4-значного десятичного числа.
Пример: «1305» означает:
Шкаф 1, модульная стойка 3, позиция модуля 05

Mode Channel n (0/1/2)

Назначение	Значение
1	Нормальный режим, сообщается об обнаруженной ошибке с высоким уровнем на соответствующем выходе «Ошибка значения канала n» (Error Channel n), цепь выхода модуля закрыта.
0	Анализ ошибок, сообщения об ошибках блокируются.
2	Допускается только в зависимости от установки, инверсный режим, т. е. цепь выхода должна быть открыта. Об обнаруженной ошибке сообщается высоким уровнем на соответствующем выходе *Error Channel n*,
> 2	Диапазон значения превышен: канал интерпретируется как неисправный (TRUE на выходе) и выдается сообщение о неисправности соответствующего канала.

В безопасных цепях управления следует использовать принцип тока покоя.

Max. Time Inrush Current in ms, Mod.
Max. Time Inrush Current in ms, red. Mod.

Определение времени ожидания для распознавания обрыва линии или времени для установления допуска ограничения тока. В течение данного времени блокируется индикация неисправностей. Увеличение времени ожидания влечет за собой увеличение времени цикла.

9.2.4.2 Выходы

Выходы Pulse on Error (2x), Error, Error Mod. и Error Code red. Mod. служат только для информации, из них нельзя выводить безопасные операции в прикладной программе.

Прочие выходы могут применяться для безопасных операций.

9.2.5 Модуль HB-RTE-3

Модуль служит для анализа и индикации ошибок при цифровых безопасных модулях ввода при одноканальном режиме или режиме с резервированием. Он должен использоваться для каждого модуля ввода типа F 3237 или F 3238 или для двух резервно работающих модулей ввода F 3237 или F 3238 однократно в прикладной программе.

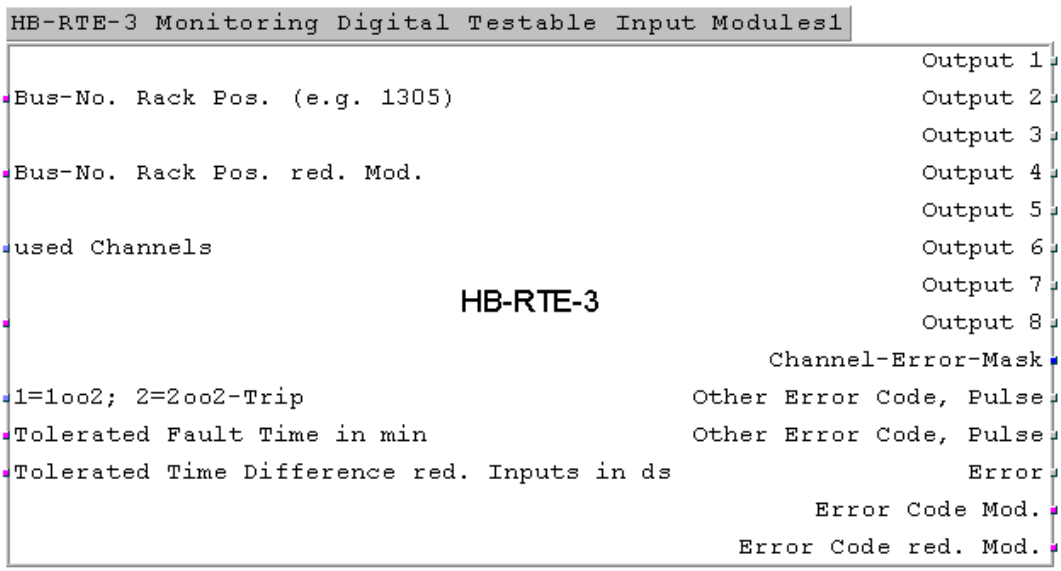


Рис. 21: Подключения модуля HB-RTE-3

9.2.5.1 Входы

Bus No. Rack Pos. (например, 1305)
Bus No. Rack Pos. red. Mod.

Позиция безопасного цифрового модуля вывода и при наличии резервного модуля в виде 4-значного десятичного числа. Пример: «1305» означает:

Шкаф 1, модульная стойка 3, позиция модуля 05

1 = 1oo2; 2 = 2oo2 trip

Назначение	Значение
0	Назначение в одноканальном режиме. Ввод согласно IEC 1131: 16#00 или 2#00000000.
1	Отключение 1 из 2, соответствует соединению И. При отключении 1 из 2 используется резервирование модулей для повышения готовности. Если не возникает ошибок модулей ввода и входных цепей, то входные сигналы каналов 1...8 модулей имеют привязку И к соответствующим выходам модуля. При возникновении ошибки на канале удерживается последнее состояние на соответствующем выходе модуля и по истечении определенного времени ошибки значение сбрасывается на FALSE, если ошибка еще присутствует. При FALSE на другом входе, не содержащем ошибку, или при одновременном возникновении ошибок в обоих каналах (двойная ошибка) выход модуля сразу же устанавливается на FALSE.
2	Отключение 2 из 2, соответствует привязке ИЛИ. При отключении 2 из 2 используется резервирование модулей для повышения готовности. Если нет ошибки модулей ввода или входных цепей, входные сигналы каналов 1...8 модулей передаются на соответствующие выходы модуля с привязкой ИЛИ. При возникновении ошибки на канале входной сигнал другого канала передается на выход модуля. Только при одновременном возникновении ошибок на обоих каналах (двойная ошибка) удерживается последнее состояние на соответствующем выходе модуля и по истечении определенного времени ошибки значение сбрасывается на FALSE, если двойная ошибка сохраняется.

В безопасных цепях управления следует использовать принцип тока покоя.

Tolerated Fault Time in min.

В течение указанного времени после проверки датчиков неисправность элемента или провода не оказывает влияния на отключение

Требуется согласование с органом, осуществляющим приемку.

Tolerated Time Difference red, Inputs in ds

Временная разность точек переключения между двумя резервными датчиками. Время зависит от датчика, требуется согласование с органом, осуществляющим приемку.

9.2.5.2 Выходы

Выходы *Channel Error Mask, Other Error Code, Pulse (2x), Error, Error Code Mod.* и *Error Code red. Mod.* служат только для информации. Они не должны использоваться для программирования безопасных реакций в прикладной программе.

Выходы *Output 1*…*Output 8* могут применяться для безопасных реакций.

9.2.6 Модуль HF-AIX-3

Модуль HF-AIX-3 служит для программирования и анализа канала безопасного аналогового модуля ввода (Ex)i F 6221 с разрешением 0...10 000.

Модуль HF-AIX-3 должен использоваться для каждого канала F 6221 однократно в прикладной программе.

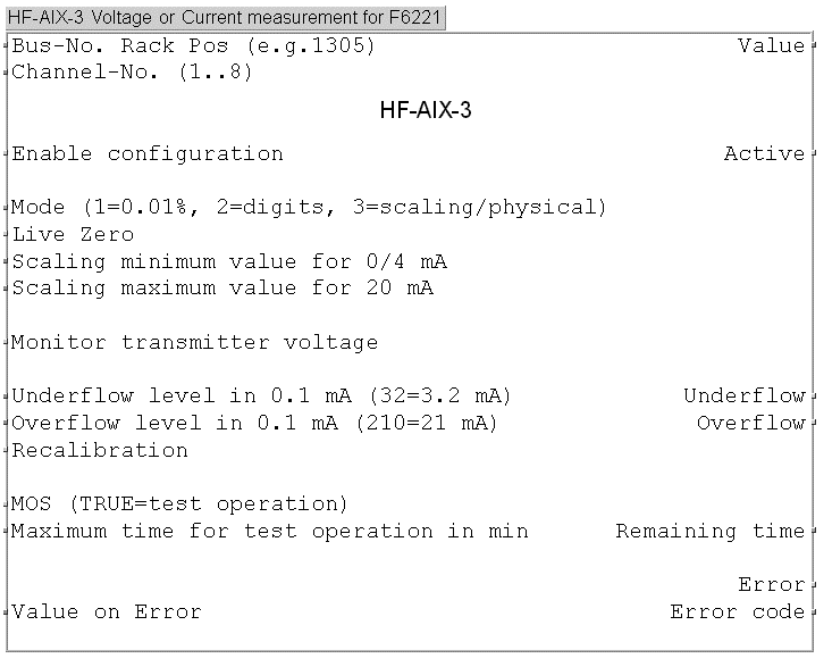


Рис. 22: Подключения модуля HF-AIX-3

Аналоговый модуль ввода имеет на каждый канал безопасный выход, управляемый независимо от цикла центрального модуля. Состояние данного выхода отображается на выходе модуля HF-AIX-3 и доступно для дальнейшей обработки в прикладной программе.

С помощью настроек параметров значение аналогового модуля ввода может преобразовываться и масштабироваться.

Заданное на входе модуля значение *Value on Error* в следующих случаях переключается на выход *Value*:

- при неисправностях канала
- при ошибках модуля
- при превышении максимального или недостижении минимального значения измерений

В данных случаях прикладная программа обрабатывает значение *Value on Error* вместо измеренного значения.

9.2.7 Модуль HF-CNT-3

Модуль HF-CNT-3 служит для параметрирования и анализа обоих каналов безопасного модуля счетчика F 5220 с разрешением 24 бит. Модуль счетчика может использоваться для подсчета импульсов, определения частот или частоты вращения, а также определения направления вращения.

Модуль HF-CNT-3 должен использоваться в прикладной программе однократно для каждого модуля счетчика F 5220.

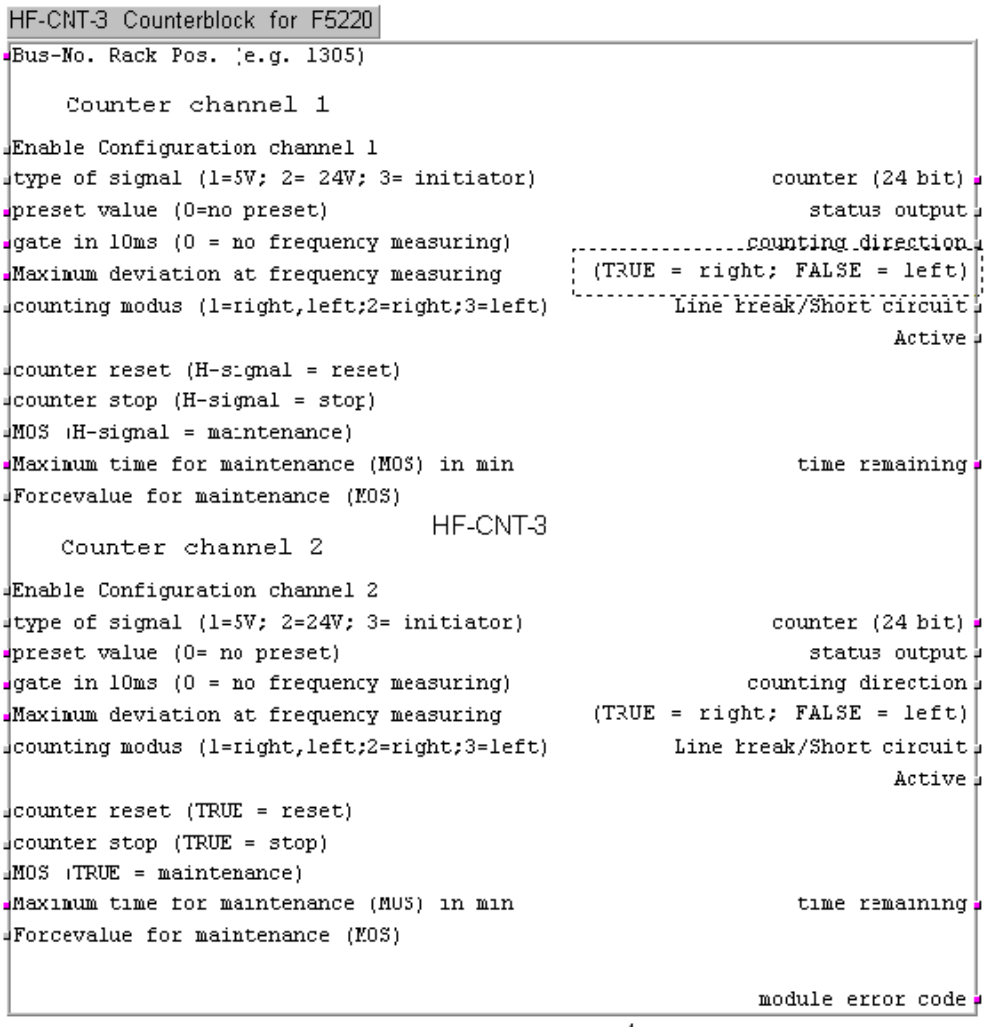


Рис. 23: Подключения модуля HF-CNT-3

Модуль счетчика имеет на каждый канал безопасный выход, управляемый независимо от цикла центрального модуля. Состояние выхода (*Output State*) отображается на выходе модуля счетчика HF-CNT-3 и доступно для дальнейшей обработки в прикладной программе.

С сигналом TRUE на выходе *MOS* (Maintenance Override Switch) выход модуля счетчика для заданного времени тестового режима может управляться напрямую, т. е. выход проводит сигнал, заданный на входе *Force Value for Test Operation*.

i При изменении времени стробирования корректное измеренное значение доступно на выходе только после трех циклов времени стробирования (согласно текущим настройкам)!

9.2.8 Модуль HF-CNT-4

Данный модуль соответствует модулю HF-CNT-3, однако имеет дополнительно по одному выходу *Channel Error*.

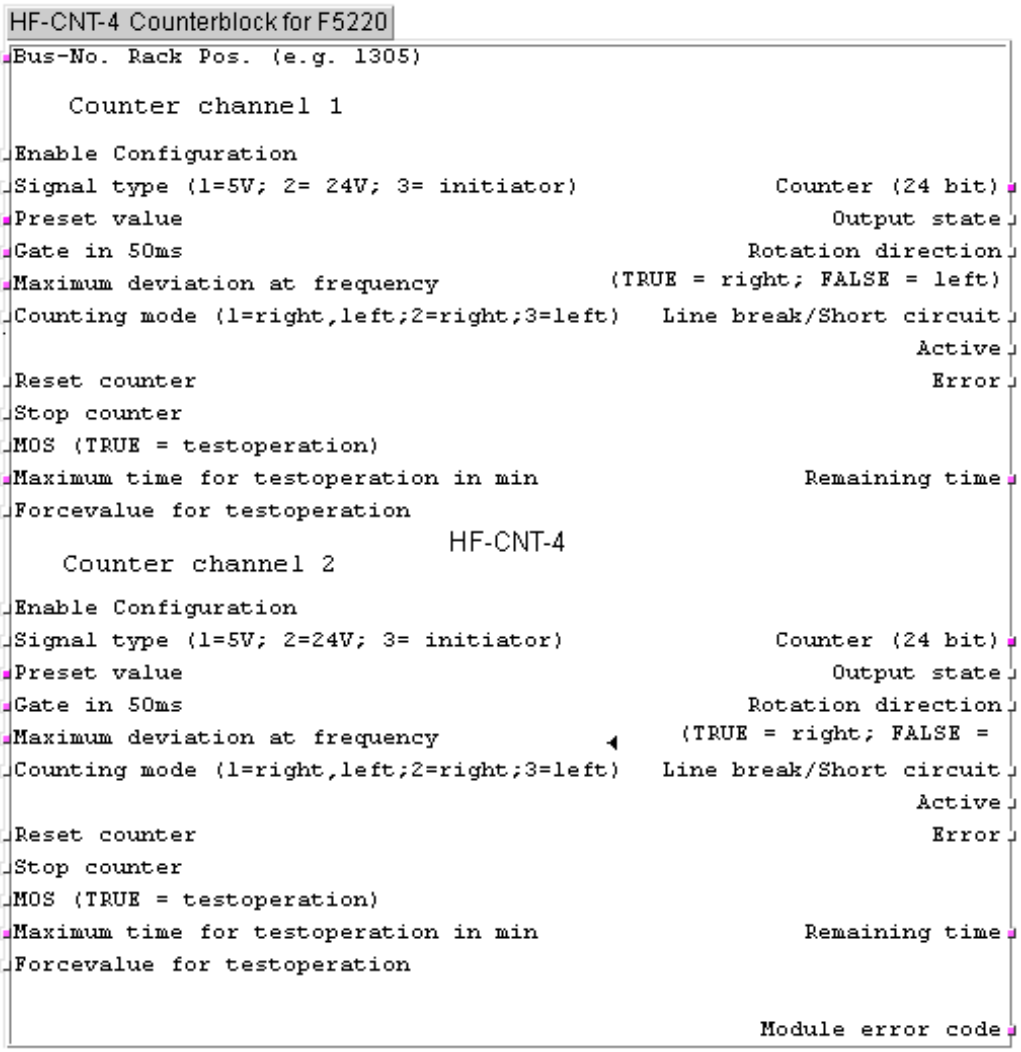


Рис. 24: Подключения модуля HF-CNT-4

Выходы *Channel Error* сообщают об ошибке канала:.

Channel Error =	
TRUE	Имеет место ошибка канала. При ошибке модуля оба выхода *Channel Error* имеют значение TRUE
FALSE	Канал работает правильно или еще не параметрирован.

9.2.9 Модуль HF-TMP-3

Модуль HF-TMP-3 используется для каждого канала модуля термоэлемента F 6220. Без корректного параметрирования канала с помощью модуля HF-TMP-3 канал не работает, т. е. имеет выходные значения 0 или FALSE. Функциональность по умолчанию или настройки по умолчанию отсутствуют. Тип датчика 1 должен задаваться только на канале 9.

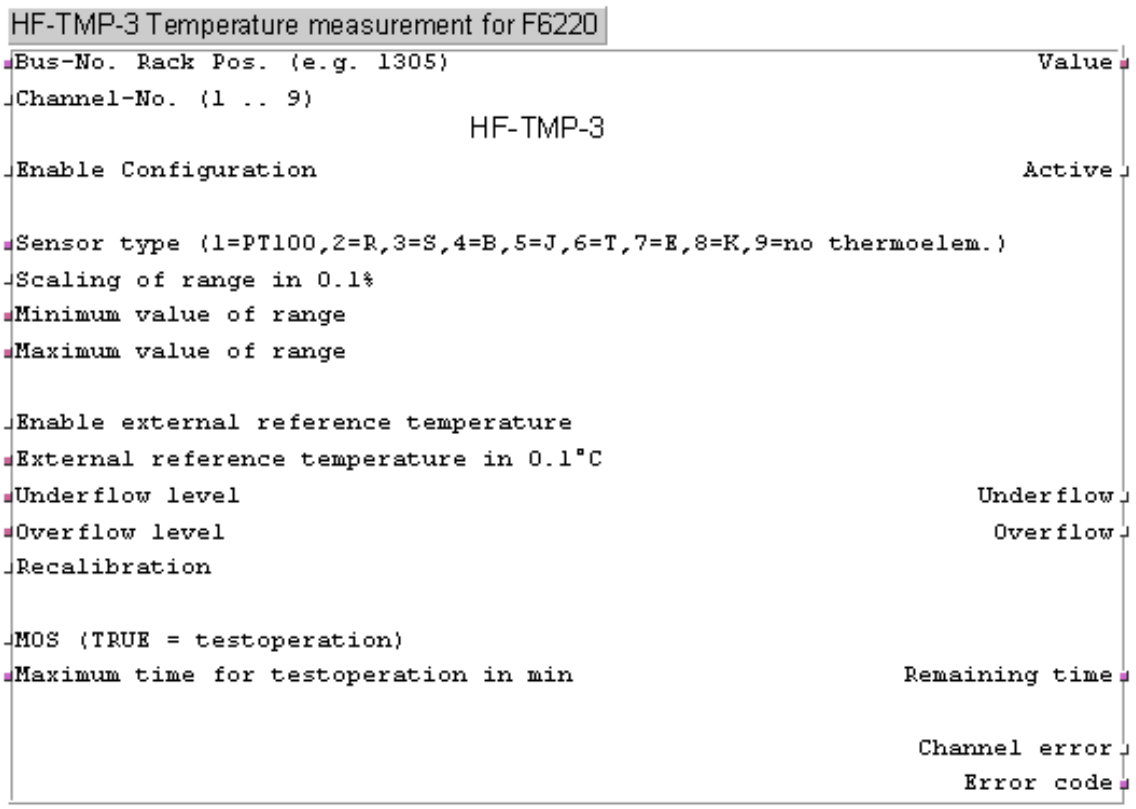


Рис. 25: Подключения модуля HF-TMP-3

Сигнал *Enable External Reference Temperature* анализируется только, если установлен режим работы *Temperature Measurement* (значения от 2 до 8 на входе *Sensor Type*). Если данный вход дает значение TRUE, то температура на входе *External Reference Temperature* используется в качестве сравнительного значения. Если данный вход дает значение FALSE, то в качестве сравнительной температуры обрабатывается значение температуры термометра сопротивления, находящегося на модуле.

Выход модуля *Value* в случае ошибки канала или модуля выдает значение 0. В прикладной программе необходимо анализировать выход модуля *Channel Error*, чтобы обрабатывалось определяемое в прикладной программе значение ошибки.

Для безопасных применений для уровня совокупной безопасности 3 следует анализировать опорную исходную температуру как результат сравнения опорных температур на двух разных модулях, а также температуру двух термоэлементов.

Перекалибровка выполняется автоматически каждые 5 минут для автоматического определения существующих на модуле условий окружающей среды (например, температуры). Перекалибровка может также срабатывать из-за TRUE на входе *Recalibration*. Данный сигнал должен существовать только в течение одного цикла.

С сигналом TRUE на входе *MOS* (*Maintenance Override Switch*) значение на выходах модуля *Value* и *Channel Error* замораживается, если отсчитывается время для тестового режима.

9.2.10 Модуль HZ-DOS-3

Модуль позволяет определять, какие безопасные модули ввода/вывода должны работать только в диагностическом режиме. С помощью модуля можно контролировать до шестнадцати модулей. Модуль может использоваться неоднократно в прикладной программе.

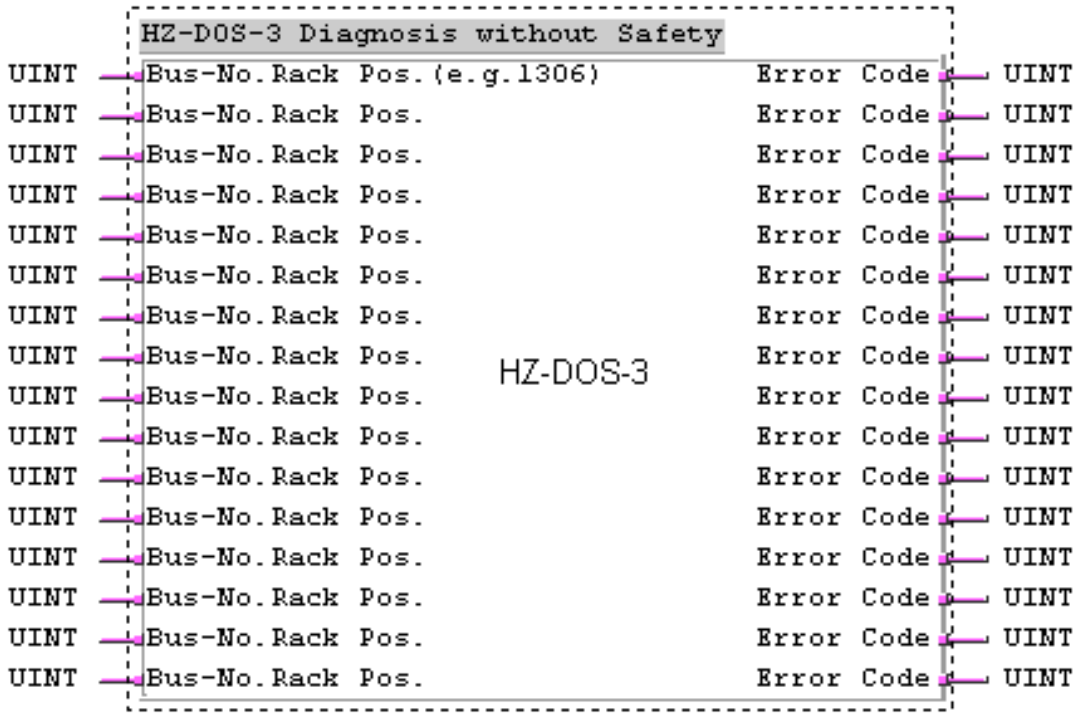


Рис. 26: Подключения модуля HZ-DOS-3

Модуль не имеет отношения к безопасности. Выходы модуля служат только для информации. Они не должны использоваться для программирования безопасных реакций в прикладной программе.

Все безопасные модули ввода/вывода, перечисленные на модуле HZ-DOS-3, не разрешается использоваться для функций безопасности.

9.2.11 Модуль HZ-FAN-3

Модуль служит для анализа и индикации ошибок при безопасных модулях ввода/вывода. С помощью модуля можно контролировать до восьми модулей. Модуль может использоваться неоднократно в прикладной программе.

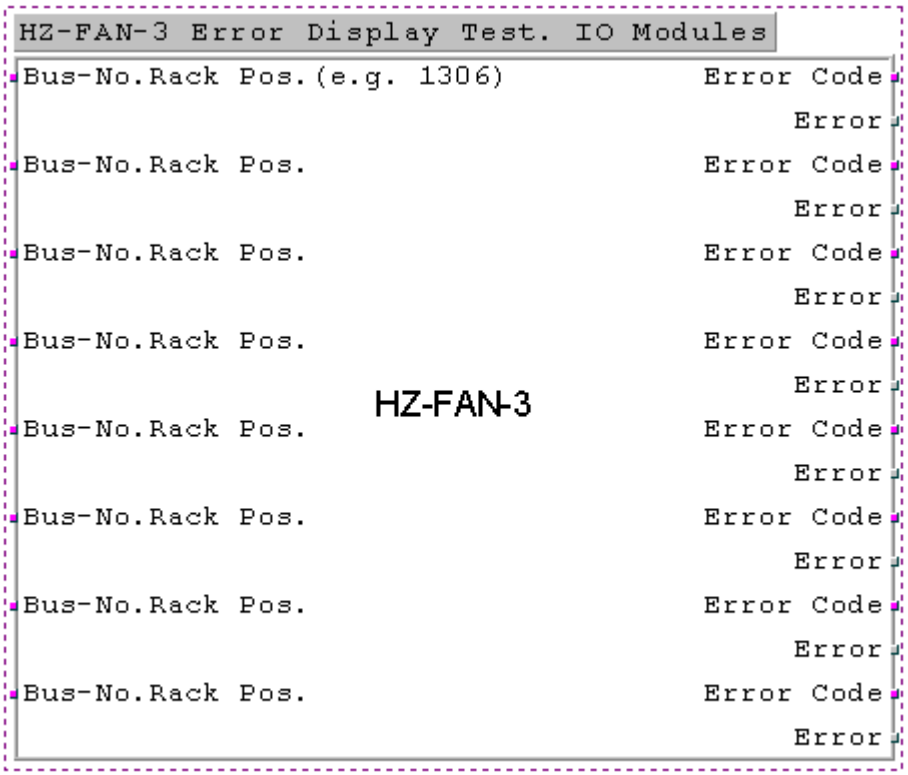


Рис. 27: Подключения модуля HZ-FAN-3

9.2.11.1 Входы

Bus No. Rack Pos. (например, 1306)	Позиции безопасных модулей ввода/вывода вводятся в виде четырехзначного десятичного числа. Пример: «1306» означает: Шкаф 1, модульная стойка 3, позиция модуля 06

9.2.11.2 Выходы

Все выходы модуля служат для информации. Они не должны использоваться для программирования безопасных реакций в прикладной программе.

Приложение

Глоссарий

Обозначение	Описание
AI	Analog input, аналоговый вход
ARP	Address resolution protocol, сетевой протокол для распределения сетевых адресов по адресам аппаратного обеспечения
COM	Коммуникационный модуль
CRC	Cyclic redundancy check, контрольная сумма
DI	Digital input, цифровой вход
DO	Digital output, цифровой выход
ELOP II	Инструмент программирования для H41q/H51q
EMC	Electromagnetic compatibility, электромагнитная совместимость
EN	Европейские нормы
ESD	Electrostatic discharge, электростатическая разгрузка
FB	Fieldbus, полевая шина
FBD	Function block diagrams, язык функциональных модулей
ICMP	Internet control message protocol, сетевой протокол для сообщений о статусе и неисправностях
IEC	Международные нормы по электротехнике
PADT	Programming and Debugging Tool, инструмент программирования и отладки (согласно IEC 61131-3), ПК с ELOP II
PE	Protective earth, защитное заземление
PELV/ЗСНН	Protective extra low voltage, пониженное напряжение с безопасным размыканием
PFD	Probability of failure on demand, вероятность индикации ошибки при требовании обеспечения безопасности
PFH	Probability of failure per hour, вероятность опасного отказа в работе за час
R	Read
R/W	Read/Write
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)
SNTP	Simple network time protocol, простой сетевой протокол времени (RFC 1769)
SRS	System.Rack.Slot, адресация модуля
SW	Software, программное обеспечение
TMO	Timeout, время ожидания
W	Write
Watchdog (WD)	Контроль времени для модулей или программ. При превышении показателя контрольного времени модуль или программа выполняют контрольную остановку.
WDT	Watchdog time, время сторожевого устройства
Адрес MAC	Адрес аппаратного обеспечения сетевого подключения (media access control)
без обратного воздействия на источник	Предположим, к одному и тому же источнику (например, трансмиттеру) подключены два входных контура. В этом случае входной контур обозначается как контур «без обратного воздействия на источник», если он не искажает сигналы другого входного контура.
ПЭС	Programmable electronic system, программируемая электронная система

Перечень изображений

Перечень таблиц

Индекс

HI 803 077 RU

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28 | 68782 Brühl | Germany
Телефон +49 6202 709-0 | Телефакс +49 6202 709-107
info@hima.com | www.hima.de

SAFETY
NONSTOP

Подробный перечень всех филиалов и представительств Вы найдете по адресу: www.hima.com/contact