Руководство на ПЛК безопасности Quantum

33003879 русс

Астана +7(7172)727-132 Волгоград (844)278-03-48 Воронеж (473)204-51-73 Екатеринбург (343)384-55-89 Казань (843)206-01-48 Краснодар (861)203-40-90 Красноярск (391)204-63-61 Москва (495)268-04-70 Нижний Новгород (831)429-08-12 Новосибирск (383)227-86-73 Ростов-на-Дону (863)308-18-15 Самара (846)206-03-16 Санкт-Петербург (812)309-46-40 Саратов (845)249-38-78 Уфа (347)229-48-12
единый адрес: sdn@nt-rt.ru | sensedat.nt-rt.ru

Содержание

Меры предосторожности

Важная информация

ПРИМЕЧАНИЕ Внимательно ознакомьтесь с данным руководством и оборудованием перед проведением работ по установке, эксплуатации или обслуживанию. Приведенные ниже предостережения могут встречаться по всему руководству, а так же присутствовать непосредственно на самом оборудовании. Подобные замечания предостерегают пользователя о потенциальной опасности и требуют повышенного внимания, а так же могут содержать дополнительную информацию пояснительного характера.

Этот символ встречается на шильдиках ОПАСНО или ВНИМАНИЕ и предостерегает о возможности электрического удара и нанесения травм персоналу при несоблюдении должных инструкций.

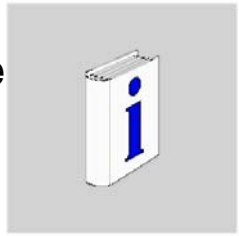
Это символ, требующий повышенного внимания. Он предупреждает пользователя об опасности. Во избежание травм, включая вероятный смертельный исход, уделяйте повышенное внимание подобного рода предупреждениям.

⚠ ОПАСНО
Знак ОПАСНО указывает на наличие опасности, которая **может привести** к серьезным травмам, смертельному исходу или повреждению оборудования.
⚠ ВНИМАНИЕ
Знак ВНИМАНИЕ указывает на наличие опасности, которая если не отнестись к ней с должной осторожностью, **может** привести к серьезным травмам, смертельному исходу или повреждению оборудования.
⚠ ПРЕДУПРЕЖДЕНИЕ
Знак ПРЕДУПРЕЖДЕНИЕ указывает на наличие опасности, которая если не отнестись к ней с должной осторожностью, **может** привести к травмам или повреждению оборудования.

ОБРАТИТЕ ВНИМАНИЕ К установке, эксплуатации, обслуживанию или ремонту электрического оборудования допускается только квалифицированный персонал. Компания не несет какой-либо ответственности за последствия вследствие использования настоящего материала.

© 2007 . Все права сохранены.

Об этом руководстве



Начальные сведения

Краткой обзор руководства

Данное руководство по безопасности содержит описание программируемых логических контроллеров с расширенными функциями безопасности серии Quantum, в частности в области соответствия требованиям безопасности, установленных стандартом безопасности IEC 61508. В данном руководстве представлено подробное описание правил установки, запуска и обслуживания систем, которые необходимо соблюдать для гарантии безопасности людей, предотвращения вредного воздействия на окружающую среду, порчи оборудования или нарушения производственных процессов.

Данная документация предназначена для изучения квалифицированными специалистами, имеющими необходимое представление о функциональной безопасности и инструментальной системе Unity Pro. К пуско-наладочным работам и эксплуатации программируемых логических контроллеров с расширенными функциями безопасности серии Quantum (далее по тексту - ПЛК безопасности Quantum) допускаются только сотрудники, имеющие необходимую квалификацию для проведения пуско-наладочных работ или эксплуатации подобных устройств в соответствии с требованиями действующих стандартов безопасности.

Срок действия

Данные и иллюстрации, представленные в данном документе, не являются обязывающими. Компания сохраняет за собой право вносить изменения в собственные изделия, следуя политике компании и техническим достижениям. Изменения вносятся в данный документ без уведомления и это не считается обязательством компании .

Лист регистрации изменений

Изм. №	Изменение
1	Первоначальный вариант

Используемые документы

Название документа	Номер по каталогу
Модули Ethernet Quantum 140 NOE 771 xx, Руководство пользователя	UNYUSE10410
Правила заземления и электромагнитная совместимость ПЛК, Руководство пользователя	UNYUSE10010
Архитектура связи ПЛК Quantum и Premium, Справочник	UNYUSE10410
Сеть Modbus Plus, Руководство по проектированию и монтажу	890 USE 100 00
Система кабелей дистанционного управления, Руководство по проектированию и монтажу	890 USE 101 00
Дискретные и аналоговые вводы/выводы ПЛК Quantum, Справочник	UNYUSE10010
Инструкции для ПЛК Quantum	33002365
Аппаратные средства ПЛК Quantum, Справочник Горячее резервирование Modicon Quantum при помощи программного обеспечения Unity, Руководство пользователя	35013379 35010533
Правила конфигурирования TCPIP/IP для ПЛК Quantum, Руководство пользователя	UNYUSE10410
ПЛК Quantum и инструментальная система Unity Pro, Справочник по аппаратным средствам	UNYUSE10010
Рабочие режимы инструментальной системы Unity Pro, Руководство	33003101
OSLoader в инструментальной системе Unity Pro, Руководство пользователя	35006156
Структура программы и языки инструментальной системы Unity Pro, Справочник	35006144
Библиотека блоков функций безопасности в инструментальной системе Unity Pro	33003873
Правила работы в инструментальной системе Unity Pro XLS	33003885
Стандарт IEC 61131-2. Программируемые контроллеры. Раздел 2: Методики испытаний и требования к оборудованию, Второе издание 2003-02	–
Стандарт IEC 61508. Функциональная безопасность электрических/электронных/программируемых электронных систем безопасности, Первое издание 2003-01	–
Стандарт IEC 61511. Функциональная безопасность. Инструментальные системы безопасности для перерабатывающей промышленности. Первое издание	–

Примечание: Любые требования относительно электрической безопасности, наружных кабелей и проводки применяются дополнительно к требованиям, установленным в документах из настоящей таблицы и данном руководстве по безопасности.

Предупреждения относительно изделия

Компания не несет ответственности за любые ошибки и неточности, встречающиеся в данном документе. Любые предложения по улучшению и дополнению данного документа или замечания об обнаруженных ошибках направляйте представителям компании. Запрещается полное или частичное воспроизведение данного документа в электронном или бумажном виде, включая ксерокопии, без предварительного разрешения компании в письменном виде.

При установке и эксплуатации данного изделия необходимо соблюдать все действующие государственные, федеральные и местные правила. Исходя из соображений безопасности и соответствия представленным в документах данным, ремонт компонентов изделий осуществляется исключительно производителем.

Соблюдайте все необходимые правила и указания при использовании программируемых логических контроллеров в областях, где действуют требования к технической безопасности.

Несоблюдение требований использования программного обеспечения компании или другого утвержденного программного обеспечения с изделиями компании может привести к травмам персонала, порче оборудования и другим нежелательным последствиям.

Несоблюдение данных предостережений может привести к травмам или порче оборудования.

Общие сведения о ПЛК безопасности Quantum

1

Начальные сведения

Введение

В данной главе представлены общие сведения о ПЛК безопасности серии Quantum.

Что в этой главе?

В этой главе имеются следующие параграфы:

1.1 Общие сведения

Начальные сведения

Введение

В данном параграфе представлены подробные сведения о функциях безопасности, предусмотренных в программируемых логических контроллерах безопасности серии Quantum .

Что в этом параграфе?

В этом параграфе имеются следующие темы:

Стандарт IEC 61508 и уровни безопасности (SIL)

Введение	ПЛК безопасности серии Quantum представляет собой систему безопасности, успешно прошедшую сертификацию организацией TÜV Rheinland Group в соответствии с требованиями стандарта IEC 61508. Данный контроллер построен на базе программируемых логических контроллеров семейства Quantum. Программирование таких контроллеров выполняется при помощи инструментальной системы Unity Pro XLS, разработанной компанией . Имея такой же набор функций, как и инструментальная система версии Unity Pro XL, эта версия дополнительно позволяет программировать ПЛК безопасности серии Quantum. Более подробное описание различий между данными версиями инструментальной системы см. в разделе *Различия между обычными ПЛК Quantum и ПЛК безопасности Quantum, стр. 24*.
Описание стандарта IEC 61508	Стандарт IEC 61508 представляет собой технический документ, содержащий нормы функциональной безопасности электрических, электронных и программируемых электронных систем обеспечения безопасности. Под понятием системы обеспечения безопасности подразумевается система, выполняющая одну или более специальных функций для поддержания степени риска на приемлемом уровне. Такие функции определены как функции безопасности. Система считается функционально безопасной, если произвольные, систематические или наиболее распространенные неисправности не становятся причиной выхода системы из строя, травмирования или смерти людей, причинения вреда окружающей среде, порче оборудования или нарушения производственного процесса.
Описание уровней безопасности (SIL)	Функции безопасности выполняются для обеспечения и поддержания системы в безопасном состоянии. В стандарте IEC 61508 вводятся понятия о четырех уровнях безопасного выполнения функции безопасности. Данные уровни именуются как уровни безопасности (SIL), самый низкий - 1, а самый высокий 4. ПЛК безопасности серии Quantum имеет сертификат соответствия уровню безопасности SIL2 и может применяться в областях, где обесточенное состояние считается безопасным состоянием, например в системах аварийной остановки (ESD). Кроме этого, при помощи устройств безопасности, предлагаемых компанией Schneider, можно применять методику так называемого "горячего резервирования" (HSBY), что в целом повышает отказоустойчивость системы безопасности.

Сертификаты безопасности

Введение

Программируемые логические контроллеры безопасности серии Quantum прошли сертификацию

- в организации TÜV Rheinland Group
- и имеют сертификат соответствия уровню безопасности SIL2 в соответствии со стандартом IEC 61508.

Данный сертификат удостоверяет соответствие контроллеров безопасности серии Quantum требованиям следующих стандартов:

- IEC 61508: Функциональная безопасность электрических/электронных/программируемых электронных систем безопасности. Раздел 1-7. Первое издание, 2003-01.
- IEC 61131: Программируемые контроллеры.
  - Раздел 2: Методики испытаний и требования к оборудованию, Второе издание 2003-02
- Защита бойлеров
  - Европейский стандарт: PR EN 50156
  - Американские стандарты: NFPA 85 и NFPA 86
- EN 54 Системы обнаружения пожара и сигнализации
- EN 298 Системы автоматического контроля газовых горелок и газовых приборов с вентилятором или без него

Примечание: Использование контроллеров безопасности Quantum является необходимым, но не единственным условием сертификации системы безопасности. Система безопасности также обязана удовлетворять требованиям стандартов IEC 61508, IEC 61511, IEC 61131-2 и других соответствующих стандартов. Дополнительно, см. *Требования к аппаратному обеспечению и программированию, стр. 28*, *Требования к программированию и исключения, стр. 71* и *Специальные требования к стандартным областям применения, стр. 127*.

Классификация изделий

В состав ПЛК безопасности Quantum входят модули безопасности, которые выполняют функции безопасности. Также предусмотрена возможность добавления в конфигурацию контроллера так называемых модулей, не влияющих на уровень безопасности, не имеющих отношения к функциям безопасности.

Соответственно, изделия компании делятся на две категории:

- модули безопасности, и
- модули, не влияющие на уровень безопасности.

В отличие от модулей безопасности, модули, не влияющие на уровень безопасности, не выполняют функции безопасности. Они имеют сертификаты в качестве модулей, не влияющих на уровень безопасности, которые можно добавлять в конфигурацию контроллеров безопасности Quantum. Отказ одного из этих модулей не оказывает отрицательного влияния на выполнение функций безопасности.

Номенклатура модулей безопасности

Компания выпускает различные модули безопасности, которые успешно прошли сертификацию и утверждены для применения в системах безопасности. Вместе с модулями безопасности приводятся коэффициенты PFD/PFH для контрольных испытаний (PTI), которые проводятся с разной периодичностью, см. *Вероятности отказов, стр. 20* и *Периодичность контрольных испытаний, стр. 21*. Значения коэффициентов PFD/PFH выражены в процентном отношении модулей, которые были использованы для составления суммарных коэффициентов PFD/PFH для всего контура безопасности (см. *Описание контура безопасности, стр. 20* и *Контур безопасности, стр. 137*). Значения приведены для областей применения с уровнем безопасности SIL2.

В данной таблице приводится список модулей безопасности с коэффициентами PFD/PFH для областей применения с уровнем безопасности **SIL2**:

Тип изделия	**Номер по каталогу**	**Средняя наработка на отказ [ч] при 30 °C**	**PTI = 5 лет**		**PTI = 10 лет**	
			PFD [%]	**PFH [%]**	**PFD [%]**	**PFH [%]**
Модуль ЦП безопасности, без горячего резерва	140 CPU 651 60S	600 000	0,6	0,6	1,1	0,6
Модуль ЦП безопасности, с горячим резервом	140 CPU 671 60S	600 000	0,6	0,6	1,1	0,6
Модуль цифровых вводов	140 SDI 953 00S	900 000	0,1	0,2	0,2	0,2
Модуль цифровых выводов	140 SDO 953 00S	1 000 000	0,1	0,2	0,2	0,2
Модуль аналоговых вводов	140 SAI 940 00S	700 000	0,1	0,2	0,2	0,2
Модуль питания	140 CPS 124 20	–	–	–	–	–

Программирование контроллеров безопасности Quantum осуществляется при помощи инструментальной системы Unity Pro XLS.

Номенклатура модулей, не влияющих на уровень безопасности

Компания выпускает следующие модули, не влияющие на уровень безопасности:

Тип модуля	Номер по каталогу
Головной адаптер удаленного ввода/вывода	140 CRP 932 00
Адаптер устройства удаленного ввода/вывода	140 CRA 932 00
Модуль Ethernet	140 NOE 771 11
Шасси, 16 слотов	140 XBP 016 00
Шасси, 10 слотов	140 XBP 010 00
Шасси, 6 слотов	140 XBP 006 00
Модуль цифрового ввода	140 DDI 353 00
Модуль цифрового вывода	140 DDO 353 00
Модуль аналогового ввода	140 ACI 040 00
Модуль аналогового вывода	140 ACO 020 00
Колодка зажимов	140 XTS 002 00

ОПАСНО

ОПАСНОСТЬ НЕВОЗМОЖНОСТИ СОЗДАНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ

Для создания системы безопасности применяйте только изделия , имеющие сертификат соответствия для применения в системах безопасности. Функции безопасности могут выполнять только модули безопасности. Запрещается использовать вводы или выводы модулей, не влияющих на уровень безопасности, в качестве выходов безопасности. **Несоблюдение этих указаний может привести к смертельному исходу или серьезным травмам.**

Инструментальная система Unity Pro XLS поддерживает возможность разбиения логики на секции. Компания рекомендует создавать секции, которые используются только для нейтральной логики (т.е. не имеющей отношения к функциям безопасности) системы. Данные из модулей, не влияющих на уровень безопасности, обрабатываются только в этих секциях, таким образом, сертифицировать вашу систему будет значительно проще.

Примечание: Для работы контроллеров безопасности Quantum, а также программирования и запуска системы безопасности, Вам потребуется сертифицированная прошивка Quantum, утвержденная для применения в системах безопасности. Подробнее см. *Сертифицированные изделия, стр. 21*.

Вероятности отказа

В стандарте IEC 61508 вводятся следующие значения коэффициентов вероятностей отказов (PFD) и вероятностей отказов в час (PFH) для уровня безопасности SIL2 в зависимости от режима работы:

- PFD ³ 10^{-3} до < 10^{-2} для режима низкой нагрузки
- PFH ³ 10^{-7} до < 10^{-6} для режима высокой нагрузки

Контроллеры безопасности Quantum имеют сертификаты соответствия для применения в системах низкой и высокой нагрузки.

Определение контура безопасности

Контур безопасности, к которому принадлежит контроллер безопасности Quantum, состоит из трех частей:

- датчики
- ПЛК безопасности Quantum
- пускатели

На рисунке ниже приводится пример типичного контура безопасности:

При расчете коэффициентов PFD/PFH приведенной в качестве примера системы, значение коэффициента ПЛК берется не более 15%. Значения коэффициентов PFD/PFH модулей безопасности Quantum см. в *Номенклатуре модулей безопасности, стр. 18*.

Примечание: Инструментальная система Unity Pro XLS не является частью контура безопасности.

Более подробную информацию о стандарте IEC 61508 и уровнях безопасности (SIL) см. в главе *IEC 61508, стр. 131*.

Пример расчета

В таблице ниже приводится 2 примера расчета коэффициентов PFD для контура безопасности с уровнем безопасности SIL2. При расчете периодичность контрольных испытаний берется равным 10 годам:

Если контур безопасности содержит ...	**Тогда коэффициент ПЛК в контуре безопасности составляет...**	**А коэффициентам датчиков и пускателей остается...**
• 1 модуль цифрового ввода, • 1 модуль цифрового вывода, и • модуль ЦП без горячего резерва	0,2 + 1,1 + 0,2 = 1,5%	98,5%
• 2 датчика, • 2 модуля аналогового ввода с резервированием • 2 модуля цифрового вывода с резервированием, и • 2 модуля ЦП с горячим резервом	0,2 + 1,1 + 0,2 = 1,5% **Примечание:** Поскольку методика резервирования применяется для увеличения безотказности системы, при расчете коэффициента каждый модуль с резервированием считается как один. Таким образом, в контуре безопасности активен только один модуль.	98,5%

Определение безопасной продолжительности

Минимальное время цикла контроллера безопасности Quantum составляет 20 мкс. Это время необходимо для обработки сигналов, полученных от модулей ввода/вывода, выполнения пользовательской логики и настройки выходов. При вычислении максимального времени отклика контроллера необходимо располагать данными о максимальном времени отклика датчиков и пускателей. Кроме этого, максимальное время отклика контроллера также зависит от времени безопасной продолжительности конкретного процесса (PST). Правила настройки времени отклика ПЛК приведены в главе *Безопасная продолжительность процесса, стр. 74*.

Периодичность контрольных испытаний

Контрольное испытание представляет собой испытание, которое периодически проводится с целью выявления неисправностей системы, обеспечения безопасности и последующим восстановлением системы в нормальное состояние или состояние, максимально приближенное к нему. Промежуток времени между такими испытаниями называется интервалом контрольных испытаний (т.е. периодичность контрольных испытаний). Периодичность контрольных испытаний для ПЛК безопасности Quantum устанавливается равной 5 или 10 годам. Подробнее см. *Номенклатура модулей безопасности, стр. 18*.

Сертифицированные изделия

Различные модификации устройств безопасности имеют необходимые сертификаты. Разрешается программировать, запускать в эксплуатацию и эксплуатировать только сертифицированные контроллеры безопасности Quantum.

Примечание:	Для контроллеров безопасности Quantum разрешается использовать только прошивку, предназначенную для контроллеров безопасности.

Для загрузки прошивки в контроллеры безопасности Quantum применяется OSLoader. Более подробную информацию о правилах перепрошивки контроллеров см. в руководстве пользователя на Unity Pro OSLoader.

Последние сведения о модификациях изделий, прошедших сертификацию, см. на сайте организации TÜV Rheinland Group *http://www.tuvasi.com/* в разделе *Information* и *List of Type Approved Programmable Electronic Systems*.

Специальные режимы работы

Введение

С точки зрения безопасности особое значение имеют следующие два режима работы контроллеров безопасности Quantum:

- Безопасный режим
- Служебный режим

Определение безопасного режима

По умолчанию контроллер безопасности Quantum работает в безопасном режиме. В данном режиме включены функции безопасности, которые обеспечивают управление процессом. Безопасный режим имеет некоторые ограничения, в частности отсутствует возможность внесения изменений и запрещены работы, связанные с обслуживанием контроллера. Таким образом, среди разрешенных действий остается только включение и выключение контроллера.

Более подробное описание Безопасного режима см. в главе *Безопасный режим, стр. 91.*

.

Описание режима обслуживания

Режим обслуживания контроллера безопасности Quantum - это временный режим, предусмотренный для изменения и отладки программы. Предусмотрена возможность внесения изменений и фиксирования значений

	**ВНИМАНИЕ** **УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ** В Безопасном режиме выполняются все диагностические функции, но результат не оценивается. При выходе из Безопасного режима и перехода в режим обслуживания безопасность Вашей системы будет всецело зависеть от вас. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Более подробное описание режима обслуживания см. в главе *Режим обслуживания, стр. 93*.

Диагностика

Введение

Контроллер безопасности Quantum обеспечивает дополнительные функции внутренней диагностики и проверки системы, таким образом, расширяя диагностические возможности.

Обзор возможностей диагностики

Внутренняя архитектура модулей ЦП безопасности Quantum

- обеспечивает 2 канала выключения и
- позволяет формировать и выполнять двойной код для выявления
  - систематических ошибок в формировании и выполнении кода и
  - случайные неполадки в модуле ЦП и ОЗУ

  Контроль выполнения двойного кода осуществляется при помощи двух 2 разных процессоров, встроенных в модуле ЦП.

Подробнее см. раздел *Модуль ЦП безопасности, без горячего резерва, стр. 34.*

Внутренняя архитектура модулей вводов/выводов безопасности Quantum

- обеспечивает возможность резервирования
- выявляет систематические ошибки при выполнении кода и
- случайные неполадки в модулях ввода/вывода.

Кроме этого, модули вводов/выводов безопасности обеспечивают функции диагностики

- связи между модулями ввода/вывода и модулем ЦП, и
- статуса и состояния модулей ввода/вывода.

Подробнее см. *Общие сведения о модулях вводов/выводов безопасности, стр. 40.*

Различия между обычным ПЛК Quantum и ПЛК безопасности Quantum

Различия между стандартным ПЛК и ПЛК безопасности

Контроллер безопасности Quantum отличается от стандартного ПЛК Quantum тем, что отвечает требованиям стандарта IEC 61508.
В таблице ниже приводятся основные отличия контроллера безопасности Quantum от стандартного контроллера Quantum:

Параметр	**Стандартный ПЛК Quantum**	**ПЛК безопасности Quantum**
Выполнение программы ЦП	прикладной процессор или Intel	прикладной процессор и Intel
Конфигурация	• шасси • локальное шасси • удаленный ввод/вывод • любые модули питания • средства расширения шасси • распределенный ввод/вывод • полевая шина ввода/вывода	• шасси • локальное шасси • удаленный ввод/вывод • специальный модуль питания
Прошивка	обычная	специальная
Программное обеспечение	• Unity Pro XLS • Unity Pro XL • Unity Pro L	• Unity Pro XLS
Пользовательская логика	• язык функциональных блок-схем (FBD) • язык лестничной логики (LD) • язык списка инструкций (IL) • структурированный текст (ST) • язык последовательных функций (SFC)	• язык функциональных блок-схем (FBD) • язык лестничной логики (LD)
Тип данных	• расширенный тип данных (EDT) • динамические инструменты диалогов (DDT)	• расширенный тип данных (EDT) • только простые массивы
Режим	–	• Режим обслуживания • Безопасный режим
Повторный запуск	• без перезапуска • холодный пуск • горячий пуск	• без перезапуска • холодный пуск

Различия между ОС стандартного ПЛК и ПЛК безопасности

Для обеспечения соответствия требованиям стандарта IEC 61508 операционная система контроллера безопасности Quantum отличается от системы стандартного ПЛК Quantum.
В таблице ниже приводятся основные отличия операционной системы контроллера безопасности Quantum от системы стандартного контроллера Quantum:

Параметр	**ОС стандартного ПЛК Quantum**	**ОС ПЛК безопасности Quantum**
Горячий пуск	да	нет
Безопасный режим	нет	да
Минимальное время выполнения главной задачи (MAST) в режиме цикла	3 мс	20 мс
Принудительное включение Безопасного режима блокировкой ключа	нет	да
Отображение символов индикации режима на ЖК-экране	нет	да
Проверка памяти	нет	да
Пароль	нет	да
Модуль аналогового ввода безопасности	нет	да
Модуль цифрового ввода безопасности	нет	да
Модуль цифрового вывода безопасности	нет	да
Значение слов SW12, SW13	другое значение	безопасный режим
Блоки MSTR	да	нет
Подписка глобальных данных (Ethernet)	везде	только в свободном разделе
Чтение сканера ввода/вывода (Ethernet)	везде	только в свободном разделе
Глобальный ввод и специальный ввод (сеть Modbus Plus)	везде	только в свободном разделе
Свободный раздел для %M и %MW	нет	да

Примечания

Контроллеры безопасности Quantum поддерживают только холодный пуск. Таким образом, повторная инициализация приложения выполняется при каждом запуске.
Контроллеры безопасности Quantum могут работать в непрерывном (цикличном) или периодическом режиме. Поэтому, разница в поведении по сравнению с обычными контроллерами Quantum отсутствует. Подробнее периодическую работу и работу в цикле см. в главе "Структура прикладной программы" в справочнике *Языки инструментальной системы Unity Pro и Структура программы*.

Память

Память модулей безопасности ЦП Quantum подразделяется на безопасный раздел и свободный. Безопасный раздел памяти имеет защиту от записи и используется для обработки данных, имеющих отношение к безопасности. Свободный раздел памяти не имеет защиты от записи и используется для доступа к функциям безопасности, когда возникает такая необходимость. Значения из данного раздела памяти нельзя использовать непосредственно. Для этого предусмотрены специальные функциональные блоки, см. *Раздел памяти, стр. 105*.

При установке в слот A в модулях безопасности ЦП Quantum используются карты памяти PCMCIA в тех же целях, что и стандартных модулях ЦП Quantum. Такие карты могут быть стандартного типа, с картами памяти «application and file-type» или «data and file-type». Подробнее см. главу "Высокопроизводительные ЦПУ" в *Quantum с инструментальной системой Unity Pro, Справочник по аппаратным средствам*.

В отличие от них, использование слота B для карт памяти «data and file-type» не допускается, поскольку хранение таких данных не применимо для проектов безопасности.

	**ВНИМАНИЕ** **УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ** Не используйте слот B. Данные, сохраненные на карте памяти в слоте B не обрабатываются в проектах безопасности. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Горячий резерв

Кроме стандартных функций "горячего резерва" стандартных контроллеров Quantum также можно использовать контроллеры безопасности Quantum для формирования безопасных систем "горячего резерва", таким образом, существенно увеличивая отказоустойчивость модуля ЦП в системе безопасности. Для контроля способности резервного контроллера вступать в работу вместо основного ПЛК применяются элементарные функциональные блоки (EFB) при помощи которых программируется автоматическое переключение между основным и резервным контроллерами. Более подробную информацию по данной теме см. в разделе *Модуль ЦП безопасности, с горячим резервом, стр. 36*.

Резервированный ввод/вывод

Для обеспечения высокой отказоустойчивости вводов/выводов безопасности можно применять методику резервирования вводов/выводов безопасности. Более подробную информацию по данной теме см. в разделе *Примеры конфигурации ПЛК безопасности Quantum, стр. 61*.

Обучение

Введение

В соответствии с требованиями в разделе 1, приложение B стандарта IEC 61508 , все сотрудники, принимающие участие в процедурах по обеспечению безопасной службы изделий, обязаны иметь соответствующую квалификацию, обладать необходимыми техническими знаниями и навыками в сфере своих должностных обязанностей. Необходимая степень владения соответствующими знаниями и навыками определяется в зависимости от конкретного применения.

Примечание: Считается обязательным обладать всеми знаниями и навыками, необходимыми для проведения работ по установке, запуску или обслуживанию системы безопасности.

Курс обучения

Кроме традиционных курсов обучения, где преподаются правила пользования изделиями компании, специалисты компании также проводят специальные курсы, в рамках которых преподается материал по системам безопасности, соответствующих стандарту IEC 61508.

1.2 Требования безопасности

Требования к аппаратному обеспечению и программированию

Введение

При эксплуатации контроллеров безопасности Quantum необходимо соблюдать следующие требования безопасности:

Требования к аппаратному обеспечению

- В проекте безопасности необходимо применять один из следующих двух модулей безопасности ЦП Quantum:
  - модель 140 CPU 651 60S для независимых систем
  - модель 140 CPU 671 60S для систем, где требуется высокий показатель отказоустойчивости
- Функции безопасности могут выполнять только модули безопасности Quantum. Нейтральные модули также могут входить в состав контроллера безопасности, поскольку они не препятствуют работе модулей безопасности. Тем не менее, они не способны выполнять функции безопасности. Такие модули применяются только для обработки сигналов, не связанных с безопасностью.
- Безопасным состоянием выводов считается обесточенное состояние.
- Необходимо неукоснительно соблюдать установленные рабочие условия касательно электромагнитной совместимости, механического и климатического воздействия. Подробнее см. главу "Технические характеристики системы" в *Справочнике по аппаратным средствам "Платформа Quantum и инструментальная система Unity Pro".*

Примечание: Средства расширения шасси и распределенный ввод/вывод нельзя вводить в состав контроллеров безопасности Quantum.

Примечание: Все модули безопасности и модули, не влияющие на уровень безопасности, отвечают требованиям, установленным в стандарте IEC 61131-2.

Требования к программированию

- При программировании проекта безопасности необходимо применять сертифицированное "вшитое" программное обеспечение Quantum Safety и инструментальную систему программирования проектов безопасности Unity Pro XLS.
- При конфигурировании и программировании проектов безопасности необходимо в точности соблюдать правила, установленные в стандарте IEC 61508, а так же правила, приведенные в данном руководстве.
- На всех стадия разработки проекта необходимо соблюдать требования, установленные в стандарте IEC 61511 относительно установки, пуско-наладочных работ и утверждения.
- Проверка логики может выполняться в режиме моделирования. Однако полная проверка функций безопасности обязательно выполняется после окончательной установки и с использованием исполняющей системы.

	**ВНИМАНИЕ** **ВЕРОЯТНОСТЬ ОШИБОК В ПРОЕКТЕ** Убедитесь, что проект выполнен в соответствии со спецификацией, выполнив необходимые проверки с использованием исполняющей системы. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Аппаратные средства и конфигурация

2

Начальные сведения

Введение

В данной главе представлена информация об аппаратном обеспечении и конфигурации изделий компании , которые можно применять в проектах безопасности.

Что в этой главе? В этой главе имеются следующие параграфы:

2.1 Модуль ЦП безопасности

Начальные сведения

Введение

В следующем параграфе приводится описание внутренней архитектуры и специальных функций безопасности модулей безопасности ЦП Quantum в зависимости от применения данных модулей - в независимых системах или с горячим резервом.

Что в этом параграфе?

В этом параграфе имеются следующие темы:

Модуль ЦП безопасности, без горячего резерва

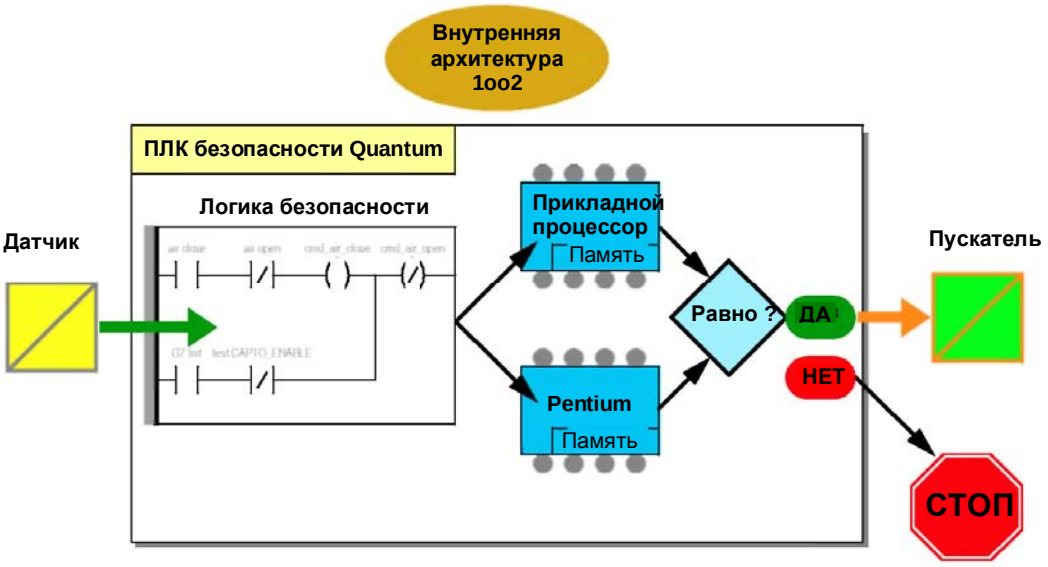
Введение

Следующие модули ЦП безопасности Quantum имеют сертификаты соответствия для применения в системах без горячего резерва:

- 140 CPU 651 60S

Определение внутренней архитектуры ЦП

В состав модуля ЦП безопасности Quantum входит 2 различных процессора - модель Intel Pentium и прикладной процессор. Каждый из этих процессоров обеспечивает выполнение логики безопасности в своем собственном разделе памяти, и затем оба сравнивают результаты выполнения по завершению каждого цикла. Каждый процессор имеет собственный независимый "путь отключения", который позволяет отключить систему, т.е. перевести ее в безопасное состояние, при обнаружении несоответствия по результатам выполнения или обнаружении ошибки. Такая двойная обработка носит название *внутренней архитектуры 1oo2 (1 из 2)*.
На рисунке ниже приведена внутренняя архитектура модуля ЦП безопасности Quantum:



Преимущества формирования и выполнения двойного кода

Два процессора, входящих в состав контроллера безопасности Quantum, обеспечивают формирование и выполнение двойного кода.
Данная особенность дает следующие преимущества при обнаружении отказов:

- формирование двух исполняемых кодов выполняется независимо. Поскольку компиляторы разные,
  можно выявить систематические ошибки при формировании кода.
- Два сформированных кода выполняются двумя разными процессорами. Таким образом, ЦПУ может
  выявить как систематические ошибки в формировании кода, так и случайные ошибки в
  ПЛК.
- Два процессора используют два независимых раздела памяти. Таким образом, ЦПУ
  могут выявить случайные ошибки в ОЗУ, и при этом устраняется необходимость проведения полной проверки ОЗУ
  при каждом сканировании.

Определение таймера Watchdog

Аппаратный и "вшитый" программный таймер "watchdog" осуществляет проверку работы контроллера и времени, необходимого для выполнения пользовательского логики.

Примечание: Необходимо сконфигурировать программный таймер "watchdog" (максимальная продолжительность цикла контроллера) в соответствии со временем выполнения приложения, фильтрацией ошибки связи вводов/выводов, искомой безопасной продолжительностью процесса (PST). Дополнительно см. *Безопасная продолжительность процесса, стр. 74*.

Описание проверки памяти

Проверка всех разделов статической памяти, включая флэш-память и ОЗУ, выполняется при помощи функции циклического контроля избыточности (CRC) и выполнением двойного кода. Защита динамических областей памяти обеспечена выполнением двойного кода и периодической проверкой памяти. При холодном пуске данные проверки проходят повторную инициализацию.

Модуль ЦП безопасности, с горячим резервом

Введение

Следующий модуль ЦП безопасности Quantum имеет сертификат соответствия для применения в системах с горячим резервом:

- 140 CPU 67160S

При использовании модулей безопасности ЦП с функцией горячего резерва в системах с горячим резервом один ЦПУ становится основным, а второй резервным.

Модуль ЦП безопасности с горячим резервом отличается от модуля ЦП безопасности без горячего резерва в назначении порта Ethernet. В модуле ЦП безопасности без горячего резерва данный порт служит для связи с другими устройствами по обычному кабелю Ethernet. В модуле ЦП безопасности с горячим резервом этот порт используется для обмена данными между основным и резервным контроллерами по оптоволоконной линии. Поскольку оптоволоконная линия не является частью контура безопасности, значения коэффициента вероятности отказа (PFD) и коэффициента вероятностей отказов в час (PFH) ЦПУ с горячим резервом аналогичны значениям этих коэффициентов ЦПУ без горячего резерва.

Определение конфигурации с горячим резервом

Конфигурация с горячим резервом включает в себя два одинаковых локальных монтажных шасси и не менее одного устройства удаленного ввода/вывода, потому что вводы/выводы невозможно расположить на локальном шасси при использовании конфигурации с горячим резервом.

Кроме модуля питания каждое локальное монтажное шасси обязательно содержит

- модуль 140 CPU 671 60S, и
- модуль 140 CRP 932 00

Кроме модуля питания и модулей ввода/вывода, удаленное устройство (-а) обязательно содержит

- модуль 140 CRA 932 00

Примечание: В системе безопасности разрешено применять только модули удаленного ввода/вывода с высокой отказоустойчивостью, которые предусматривают двойную систему кабелей.

Примеры конфигурации с горячим резервом см. в разделе *Примеры конфигурации ПЛК безопасности Quantum, стр. 61*.

Определение рабочих режимов

Контроллер безопасности с горячим резервом поддерживает работу
- в безопасном режиме, и
- в служебном режиме

В любом режиме контроллер может пребывать в одном из следующих состояний:
- работать в качестве основного
  Когда контроллер работает как основной, он выполняет пользовательскую логику и управляет процессом.
- работать в качестве резервного
  Когда один контроллер работает как основной, он показывает, что резервный контроллер работает нормально и готов в любой момент принять на себя функции основного, если он придет в неисправность. Как только резервный контроллер берет на себя функции основного, он сразу же автоматически переключается в Безопасный режим.
- работать в состоянии offline
  Данный режим является режимом по умолчанию, который выбирается либо оператором, либо определяется самим ЦПУ. В данном состоянии контроллер выполняет полностью весь проект, но без записи вводов/выводов.
- пребывать в состоянии offline

В данном состоянии контроллер не выполняет пользовательскую логику и не управляет процессом.
Основной ЦПУ и резервный ЦПУ могут одновременно пребывать в двух последних состояниях.

Примечание: При возникновении неисправности модуль ЦП безопасности с горячим резервом ведет себя аналогично
модулю ЦП безопасности без горячего резерва.
При возникновении ошибки в приложении, контроллер переходит в
- состояние ожидания, если работает в Служебном режиме.
- состояние неисправности, если работает в Безопасном режиме.

Описание случаев, когда используется состояние Offline

Когда речь идет о состоянии offline следует понимать разницу между двумя следующими ситуациями:

если ...	**то ...**
основной контроллер переключается в состояние работы в offline	резервный контроллер принимает на себя функции
резервный контроллер переключается в состояние работы в offline	функция горячего резерва становится недоступной.
отсоединяется оптоволоконный кабель	резервный контроллер переключается в состояние работы в offline
конфигурация аппаратных средств, установленная в проекте, не соответствует фактической конфигурации	либо основной, либо резервный контроллер переключается в состоянии работы в offline.
происходит несоответствие логики	резервный контроллер переключается в состояние работы в offline
резервный CRP прекращает работу	резервный контроллер переключается в состояние работы в offline

Влияние выключения контроллера на безопасную продолжительность процесса

Когда основной ЦПУ обнаруживает внутреннюю или внешнюю неполадку, он прекращает обмен данными с резервным ЦПУ и обработку ввода/вывода. Как только резервный ЦПУ определяет, что обмен данными с основным ЦПУ прекращен, он берет на себя функции основного ЦПУ и начинает выполнять пользовательскую логику и обрабатывать вводы/выводы. Поэтому, модули выводов обязаны осуществлять фильтрацию состояния утери обмена данными с основным ЦПУ во избежание сбоев, если происходит выключение контроллера. Для этого необходимо ввести время ожидания (timeout) для модуля выводов. В результате время отклика контроллера будет больше, чем время ожидания, заданное для модуля выводов, что отразится на безопасной продолжительности процесса.
Более подробное описание безопасной продолжительности процесса см. в разделе *Безопасная продолжительность процесса, стр. 74*.

Готовность функций горячего резерва

Кроме стандартных функций горячего резерва можно применять функциональные блоки EFB для программирования автоматического переключения между основным и резервным контроллерами для проверки готовности резервного контроллера принимать на себя функции основного. Иначе говоря, резервный контроллер периодически становится основным, а основной принимает на себя функции резервного.
В таблице ниже приведены функции горячего резерва и наличие каждой из них в Служебном режиме и Безопасном режиме:

Функция	Служебный режим	Безопасный режим
Горячий резерв (Hot Standby)	ДА	ДА
Переключение (Switch Over)	ДА	ДА
Переключение EFB (EFB Swap)	НЕТ	ДА
Клавиатура (Keypad)	ДА	ДА
Несоответствие логики (Logic Mismatch)	ДА	НЕТ
Обновление ОС (OS Upgrade)	ДА, если резервный пребывает в состоянии offline	НЕТ
Передача проекта (Application Transfer)	ДА	НЕТ

Более подробно правила конфигурирования и эксплуатации систем Quantum с горячим резервом см. в руководстве пользователя на системы Modicon Quantum с горячим резервом и применением Unity.

2.2 Модуль вводов/выводов безопасности

Начальные сведения

Введение

В данном параграфе приведены три модуля безопасности вводов/выводов, предназначенные для применения в составе контроллеров безопасности Quantum. Описание функций, поддерживаемых всеми модулями, дано в общем описании модулей, а описание индивидуальных функций приведено по отдельности для каждого.

Что в этом параграфе?

В этом параграфе имеются следующие темы:

Общие сведения о модулях вводов/выводов безопасности

Введение

В данном параграфе приведены три модуля вводов/выводов безопасности Quantum, которые имеют сертификаты соответствия для применения в составе контроллеров безопасности Quantum:

- 140 SAI 940 00S (модуль аналогового ввода)
- 140 SDI 953 00S (модуль цифрового ввода)
- 140 SDO 953 00S (модуль цифрового вывода)

Три модуля вводов/выводов безопасности позволяют подключить к контроллеру безопасности датчики и пускатели, которые являются частью контура безопасности. В состав каждого модуля входит две системы на базе микроконтроллеров, которые выполняют одинаковую программу, обладают одинаковыми данными и периодически проверяют друг друга. Данные модули ввода/вывода подходят для установки, как в локальные монтажные шасси, так и в устройства удаленного ввода/вывода.

Модули ввода/вывода безопасности обеспечивают возможность контроля линии, см. *Диагностика модулей вводов/выводов безопасности, стр. 45* и Модули аналогового и дискретного ввода/вывода Quantum, справочник.

Примечание: Для маркировки модулей вводов/выводов безопасности применяются красные этикетки из комплекта поставки модулей безопасности Quantum.

Определение связи между ЦПУ и вводом/выводом

Как правило, модуль ЦП безопасности Quantum управляет всеми процессами обмена данными всех шасси, а остальные модули выступают в качестве ведомых устройств (slave). Обмен данными между модулем ЦП безопасности и модулем ввода/вывода безопасности осуществляется через двухпортовое ОЗУ, размещенное в модуле ввода/вывода.

Для установки связи между ЦПУ и устройством удаленного ввода/вывода (RIO) необходимы два следующих нейтральных модуля:

- 140 CRP 932 00 (RIO головной адаптер), установленный на локальном монтажном шасси
- 140 CRA 932 00 (RIO адаптер удаленного устройства), установленный на устройстве удаленного ввода/вывода (RIO)

В протоколе связи между модулем ЦП безопасности и модулем ввода/вывода безопасности предусмотрены возможности диагностики. Подробнее см. *Диагностика модулей вводов/выводов безопасности, стр. 45.*

Определение ограничений относительно модулей ввода/вывода

Когда речь идет о связи между модулем ЦП безопасности Quantum и модулем ввода/вывода необходимо соблюдать следующие требования в отношении модулей ввода/вывода: • Контроллер безопасности Quantum не имеет возможности обращение к вводу/выводу через Ethernet или по сети Modbus Plus Инструментальная система Unity Pro XLS не имеет возможности проверки соответствия данному требованию, поскольку обращения из Ethernet и сети Modbus Plus к другим контроллерам (не вводам/выводам) разрешены, см. также *Связь между контроллерами, стр. 109.*

	**ВНИМАНИЕ** **НЕДОПУСТИМЫЙ ОБМЕН ДАННЫМИ** Убедитесь, что вводы/выводы Ethernet и Modbus Plus в контроллере безопасности не сконфигурированы. В спектр вашей ответственности входит гарантия отсутствия обращений к вводам/выводам через Ethernet или по сети Modbus Plus. При любом отклонении от данного требования Ваша система не будет признана соответствующей требованиям стандарта IEC 61508. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

- Устройства распределенного ввода/вывода, которые обмениваются данными по сети Modbus Plus, нельзя использовать в контроллерах безопасности Quantum. Проверка отсутствия сконфигурированных распределенных вводов/выводов обеспечивается инструментальной системой Unity Pro XLS. При обнаружении несоответствия данному требованию система выдает ошибку и не генерирует код.
- В контроллерах безопасности Quantum нельзя использовать вводы/выводы, которые обмениваются данными по полевым шинам. Проверка отсутствия сконфигурированных вводов/выводов полевых шин обеспечивается инструментальной системой Unity Pro XLS. При обнаружении несоответствия данному требованию система выдает ошибку и не генерирует код.

Модули вводов/выводов безопасности в конфигурациях с высокой отказоустойчивостью

Введение

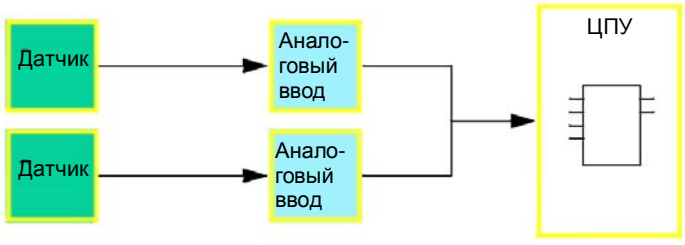
Для увеличения отказоустойчивости можно применять методику резервирования модулей вводов/выводов безопасности Quantum. Однако увеличение безопасности за счет использования резервирования модулей безопасности не достигается. Компания разработала функциональные блоки для контроля состояния для конфигурации с двумя модулями с резервированием.

Оператор и обслуживающий персонал определяют состояние модулей и необходимость их замены по системным словам. Каждый бит в таком слове отображает состояние одного канала. Подробнее см. главу "Модуль вводов/выводов безопасности Quantum" в *справочнике "Quantum с инструментальной системой Unity Pro, дискретным и аналоговым вводом/выводом"*. Если система имеет уровень безопасности SIL2, она все равно продолжит работу и единственным ограничением по времени для замены отказавшего модуля будет контрольное испытание, которое проводится с определенной периодичностью.

Допускается размещать модули в одном удаленном устройстве. Тем не менее, во избежание проблем (отказ модуля питания или удаленного адаптера) компания рекомендует размещать их в разных удаленных устройствах, см. также главу *Примеры конфигурации ПЛК безопасности Quantum, стр. 61*.

Отказоустойчивые модули аналогового ввода

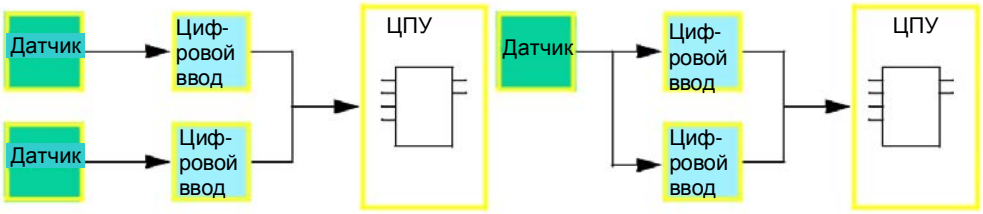
К отказоустойчивым модулям аналогового ввода безопасности подключаются два датчика, причем каждый подсоединяется к отдельной точке ввода. Точки ввода должна размещаться на разных модулях вводов. На рисунке ниже приведен пример конфигурации с резервированием аналогового ввода:



Функциональные блоки `S_AISIL2`, см. также *Функции/Функциональные блоки для систем безопасности, стр. 82* применяются для выбора вводов и контроля состояния модулей.

Отказоустойчивые модули цифровых вводов

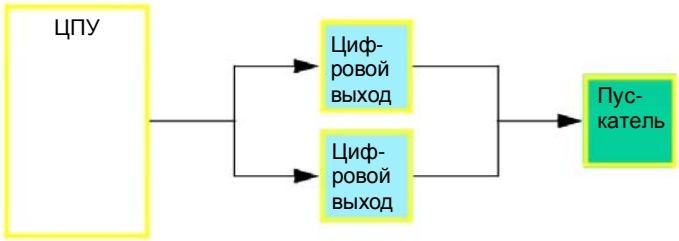
К резервированным модулям цифровых вводов может подсоединяться как один, так и два датчика. Точки ввода должны размещаться на разных модулях вводов. Если подсоединен один датчик, модули питаются от одного источника питания процесса. Соединительные провода выбираются с учетом характеристик модулей (характеристики вводов по короткому замыканию, обрыве, нулю и одному уровню, напряжению и току), которые указаны в Справочнике по аппаратному обеспечению Quantum.
На рисунке ниже приведены примеры конфигурации с резервированием цифрового ввода:



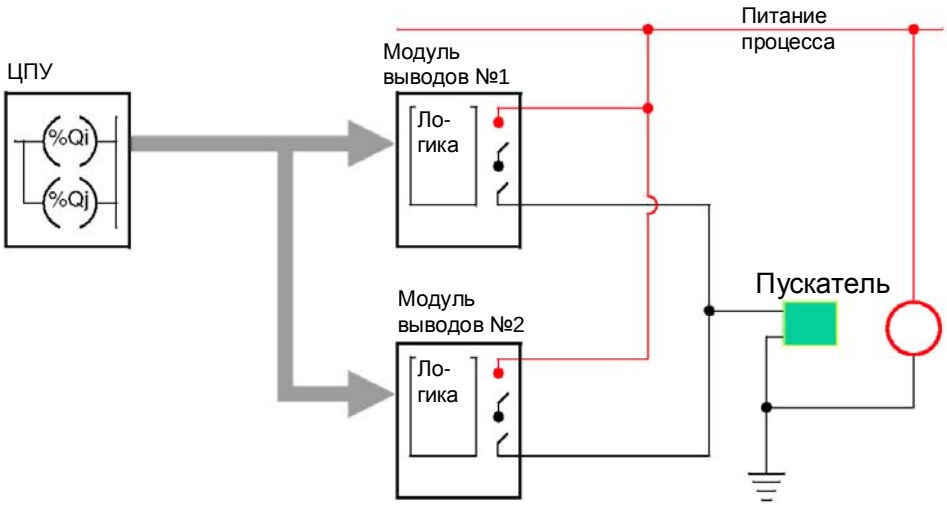
Функциональные блоки S_DISIL2, см. также *Функции/Функциональные блоки для систем безопасности, стр. 82* применяются для выбора вводов и контроля состояния модулей.

Отказоустойчивые модули цифровых выводов

Когда речь идет об отказоустойчивых модулях цифрового вывода, два вывода должны быть на разных модулях, и соединены параллельно и подведены к одному пускателю.
На рисунке ниже приведен пример конфигурации с резервированием цифрового вывода:



На рисунке ниже приведена электрическая схема для данной конфигурации:



Функциональный блок не обязателен, потому что одинаковый сигнал с ЦПУ поступает на оба вывода.

Диагностика модулей вводов/выводов безопасности

Определение диагностики вводов/выводов

В таблице ниже приведены функции полевой диагностики модулей вводов/выводов безопасности:

Диагностика	Аналоговый ввод	Цифровой ввод	Цифровой вывод
Вне диапазона	ДА	–	–
Обрыв провода	ДА	ДА	–
Отказ полевого питания	–	ДА	ДА
Перегрузка	–	–	ДА

Кроме этого возможности проверки связи между модулем ЦП безопасности и модулями вводов/выводов безопасности поддерживает контроллер безопасности Quantum, например функция CRC. Таким образом, осуществляется проверка соответствия принятых данных отправленными, но и проверка данных на предмет обновления. Для устранения помех, вызванных например электромагнитной совместимости, которые могут временно повредить данные, можно выставить максимальную последовательную ошибку CRC для каждого модуля (в диапазоне от 0 до 3). Подробнее см. главу "Конфигурирование модулей ввода/вывода в системах безопасности" в руководстве на *инструментальную систему Unity Pro XLS, Рабочие режимы*.

Диагностика при включении

При включении модуль ввода/вывода выполняет расширенную самодиагностику. Как правило, на это уходит около 30 секунд. Если диагностика обнаруживает неисправность, состояние модулей расценивается как неисправное и они не включаются. Вводам и выводам присваивается состояние 0.

Диагностика во время работы

Во время работы модуль ввода/вывода также выполняет самодиагностику. Модули ввода осуществляют проверку способности получения данных от датчиков по всему диапазону. Модули выводов осуществляют проверку выключателей импульсами продолжительностью менее 1 мс.
Если к модулю цифрового ввода или вывода не подсоединен внешний источник питания постоянного тока напряжением 24В, диагностика при включении не может быть проведена, и модули не включатся.

Определение диагностики перенапряжения

Поскольку электроника может не достигать теоретического максимального выходного напряжения источника питания, модули ввода/вывода должны обеспечивать мониторинг напряжения питания шасси.
В таблице ниже приводится описание мониторинга питания:

Питание ...	**контролируется ...**
шасси, теоретическое максимальное выходное напряжение которого составляет 18,5 В,	двумя средствами контроля перенапряжения, т.е. по одному на каждую микропроцессорную систему. Каждое средство контроля обеспечивает защиту от перенапряжения посредством размыкание собственного выключателя питания, и включения собственного блока повторного запуска, который управляет переключением между включенным и выключенным состояниями и при включении выполняет повторный запуск обоих процессоров.
на стороне полевых устройств, которое генерируется преобразователями постоянного тока в постоянный ток,	двумя средствами контроля перенапряжения и пониженного напряжения, т.е. по одному на каждую микропроцессорную систему. При отказе двух изолированных преобразователей постоянного тока в постоянный ток (DC-DC), генерирующих питание для полевой электроники, средства контроля формируют сигнал неисправности в соответствующий процессор через изолятор.
процесса типа PELV, где максимальное выходное напряжение составляет 60 В,	двумя средствами контроля перенапряжения и пониженного напряжения, т.е. по одному на каждую микропроцессорную систему (по такому же принципу, как они контролируют преобразователи постоянного тока в постоянный ток. При отказе средства контроля формируют сигнал неисправности в пользовательскую логику путем присвоение соответствующего значения биту состояния, таким образом, извещая систему о возможной несогласованности на вводах.

ОПАСНО

УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ

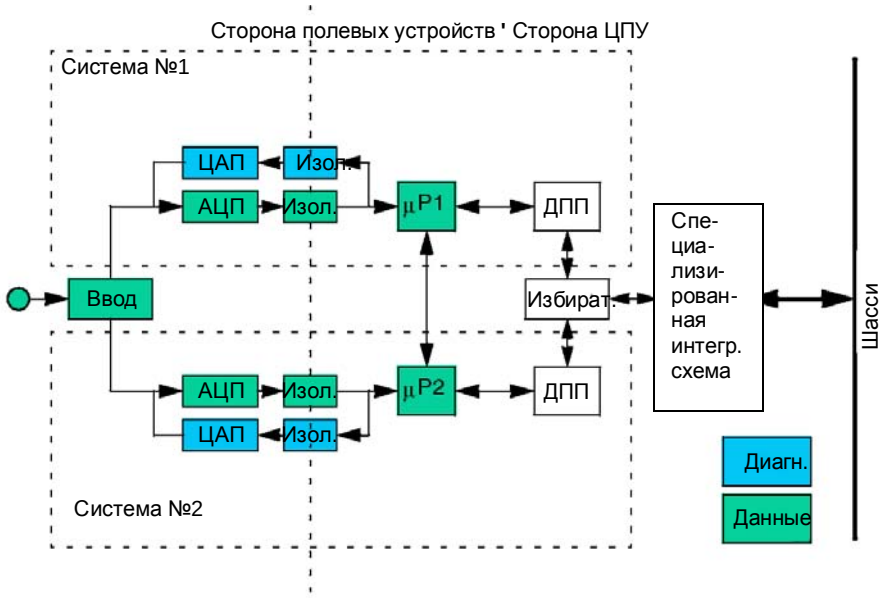
Используйте правильное питание процесса типа PELV с максимальным выходным напряжением 60 В.

Несоблюдение этих указаний может привести к смертельному исходу или серьезным травмам.

Модуль аналогового ввода безопасности

Архитектура

На рисунке ниже приведена архитектура модуля аналогового ввода безопасности Quantum:



АЦП Аналого-цифровой преобразователь
ЦАП Цифро-аналоговый преобразователь
Diag Внутренняя диагностика
DPM Двухпортовая память
Isol Электрическая изоляция
µ**P** Микропроцессор

Сведения о проводке

Для соответствия требованиям по экранированию проводов необходимо применять комплекты средств заземления для экранированных проводов аналоговых вводов.

Компания рекомендует применять следующие устройства из каталога Advantys STB (MKTED206061EN) или аналогичные:

- Комплект заземления, шифр STB XSP 3000
- Клеммы для комплекта заземления, шифр STB XSP 3010 или STB XSP 3020

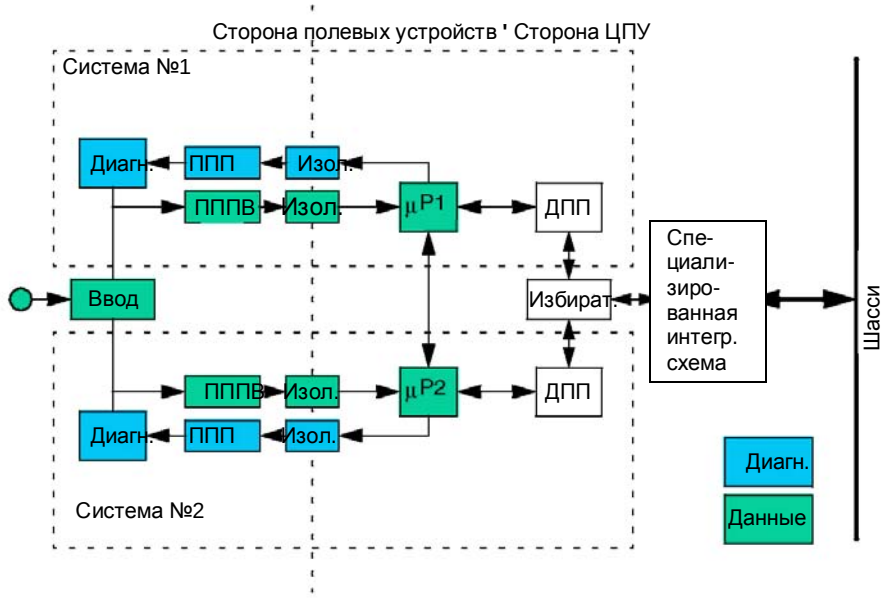
Неиспользуемые входные каналы неиспользуемых модулей ввода следует закоротить. Это необходимо для предотвращения появления ошибок вследствие обнаружения разомкнутой цепи неиспользуемых вводов модулей аналогового ввода безопасности.

Применение для управления котлами	Когда данные устройства применяются для управления котлами, модули аналоговых вводов безопасности необходимо контролировать на предмет замыкания на землю (утечка тока). Применяется беспотенциальное соединение проводов. При помощи шунтирующего резистора (например, на 250 Ом), включенного между заземляющей рейкой комплекта заземления и землей, можно измерить напряжение при утечке тока на одном из аналоговых вводов. Для обнаружения утечки необходимо контролировать это напряжение.
Описание диагностики	На стороне полевых устройств имеется 8 изолированных независимых входных каналов. Сбор данных с каждого ввода обеспечивается двумя одинаковыми цепями. Каждый микропроцессор управляет своим АЦП через изоляторы, таким образом, осуществляя сбор входных данных. Далее, микропроцессор управляет каждым ЦАП и при необходимости может увеличивать его полное сопротивление (нейтральным образом) либо уменьшать, таким образом, оказывая принудительное воздействие (фиксируя) на вход АЦП во время диагностики. Модуль аналоговых вводов выполняет • быструю самодиагностику во время нормального цикличного сбора данных для выявления расхождений, которые могут привести к внутренней неполадке. • расширенную самодиагностику во время проверочного сбора данных для проверки состояния каждого канала.
Описание контроля питания	Контроля питания не предусмотрено. Данная функция выполняется во время диагностики, поскольку АЦП и ЦАП выдают значения в зависимости от их напряжения питания.

Модуль цифрового ввода безопасности

Архитектура

На рисунке ниже приведена архитектура модуля цифрового ввода безопасности Quantum:



Диаг Внутренняя диагностика
ППП последовательно-параллельный преобразователь цифрового ввода
ППВ параллельно-последовательный преобразователь цифрового ввода
DPM Двухпортовая память
Изол Электрическая изоляция
µ**P** Микропроцессор

Сведения о проводке

Примечание: Цифровые вводы безопасности включаются в обесточенном состоянии. Состоянием ввода безопасности является обесточенное состояние, а это означает, что когда ввод становится обесточенным, выполняется функция безопасности. Поэтому, провода подбираются с учетом данного требования.

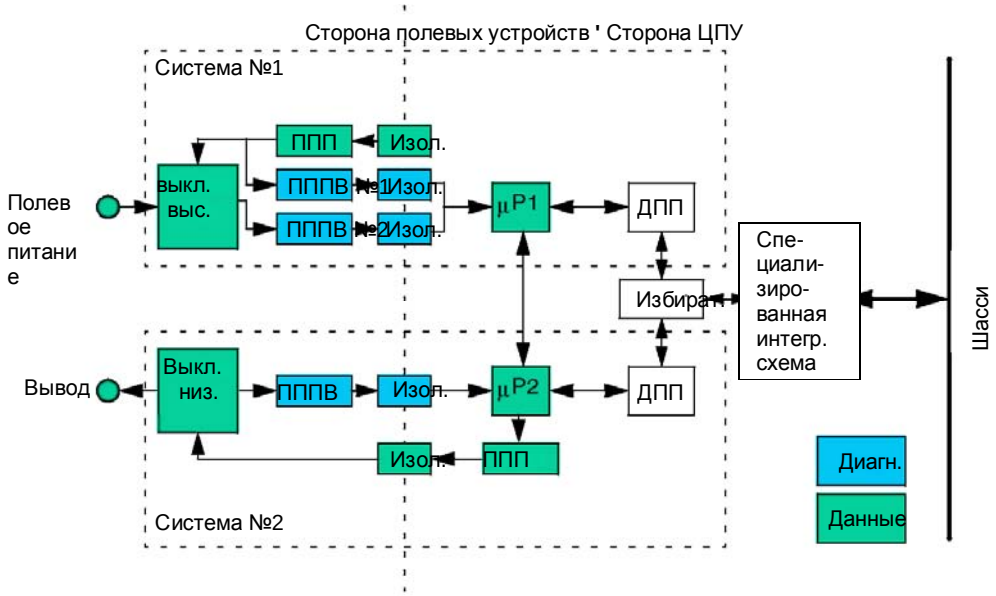
Неиспользуемые входные каналы неиспользуемых модулей ввода следует подсоединить к напряжению постоянного тока 24 В. Это необходимо для предотвращения появления ошибок вследствие обнаружения разомкнутой цепи неиспользуемых вводов модулей цифрового ввода безопасности.

Описание диагностики	Каждый входной канал использует общую входную цепь и две независимых цепи сбора данных. Каждый микропроцессор управляет параллельно-последовательный преобразователь цифрового ввода (ПППВ, который выполняет выборку входных данных. Далее, он управляет последовательно-параллельный преобразователь цифрового ввода (ППП) на каждой входной цепи, который в свою очередь управляет блоком диагностики для установления диагностических случаев. Для возможности сравнительного анализа сбор данных выполняется синхронно.
Описание обнаружения ошибок во входном канале	Модуль цифрового ввода отслеживает питание со стороны полевых устройств. Проверка внешних проводов выполняется контролером тока утечки. Минимальный ток утечки составляет 1мА. Если ток утечки отсутствует, данное состояние считается как обрыв во внешних цепях. Если контакт "сухой", необходим нагрузочный резистор номиналом 15 КОм, чтобы не фиксировалось состояние обрыва провода. Каждая входная цепь имеет выключатели, которые периодически принудительным образом замыкаются или размыкаются для проверки состояния цепи. Каждая входная цепь проверять индивидуально, и если обнаруживается неисправность, то в бите диагностики выставляется соответствующее состояние.

Модуль цифрового вывода безопасности

Архитектура

На рисунке ниже приведена архитектура модуля цифрового вывода безопасности Quantum:



Диаг Внутренняя диагностика
ППП последовательно-параллельный преобразователь цифрового вывода
ПППВ параллельно-последовательный преобразователь цифрового вывода
DPM Двухпортовая память
Isol Электрическая изоляция
µ**P** Микропроцессор

Сведения о проводке

Необходимо обеспечить защиту полевых источников питания модулей цифрового вывода безопасности в виде предохранителя. Данный предохранитель защитит модуль не только от обратной мощности, но и перенапряжения в данном источнике Не допускается каких-либо ограничений по току, при этом полевой источник питания должен обеспечивать ток 50 А в течение 0,2 сек при К.З. Предохранитель выбирается в зависимости от нагрузки, но его номинал не должен превышать 16 * 0,5 * 1,25 = 10 А (IEC 61131-2). Предохранитель должен быть быстро срабатывающим. Таким образом, необходимо применять предохранитель 16 А на входе полевого питания каждого модуля цифрового вывода.

ВНИМАНИЕ

ОПАСНОСТЬ КОРОТКОГО ЗАМЫКАНИЯ

Для защиты полевого источника питания от обратной мощности и перенапряжение применяется быстросрабатывающий предохранитель на 10 А.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Примечание: Считается обязательным подсоединять не менее 2 проводов заземления (0 В) к клеммной колодке.

Описание диагностики

Для проверки работы выключателей короткий импульс подается на модули вывода (во внутренних схемах модуля циклы диагностики вставляются периодически). Процедура диагностики выглядит следующим образом:

Шаг	Описание
1	Команда переключения изменяется на время, короткое настолько, чтобы не сработал пускатель, но не более 1 мс. Если пускатель реагирует на время, выбранное равным 1 мс, нарушения можно избежать путем параллельного использования двух выводов одного модуля.
2	Проверка результата.
3	Восстанавливается правильная команда переключения.

Описание контроля питания

Каждая выходная цепь содержит два последовательно включенных выключателя, управляемых индивидуально двумя процессорами. Первый микропроцессор использует последовательно-параллельный преобразователь цифрового вывода для управления своим выключателем, а второй микропроцессор управляет своим выключателем после преобразования. В обеих микропроцессорных системах напряжение средней точки сравнивается с пороговым значением 1. Обе системы обмениваются результатами, оценивают состояние средней точки и выполняют диагностику состояния выключателей во время каждого цикла. Если обнаруживается ошибка в одном из каналов, он отключается, и информация об этом передается в ЦПУ в биты диагностики с соответствующим значением.

Определение времени ожидания

Время ожидания для модулей выводов безопасности задается в следующих случаях:
- определение неисправности ЦПУ
- возникновении ошибки связи

Можно присвоить один из следующих вариантов времени ожидания:
- поддержание последнего значения
- значение 0, задается пользователем (состояние безопасности)
- значение 1, задается пользователем

Более подробно о настройке времени ожидания и времени ожидания модулей цифрового вывода см. в главе "Настройка модулей ввода/вывода для проектов безопасности" в руководстве на *Инструментальную систему Unity Pro XLS, Режимы работы.*

	**ВНИМАНИЕ**
	ВОЗМОЖНАЯ УТРАТА СПОСОБНОСТИ ПЕРЕХОДИТЬ В БЕЗОПАСНОЕ СОСТОЯНИЕ Выставляйте время выдержки равным 0 для цифровых модулей выводов безопасности. Контроллер безопасности Quantum гарантированно обеспечивает только переключение выводов в безопасное состояние, т.е. 0 или обесточенное состояние. Время выдержки также можно выставить равным 1, но гарантии при этом не даются. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**
	**ВНИМАНИЕ**
	ОПАСНОСТЬ СКРЫТОЙ НЕИСПРАВНОСТИ Следует помнить, что вывод переключается в обесточенное состояние независимо от значения, установленного в качестве времени ожидания, если модуль определяет внутреннюю неисправность. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Определение времени ожидания модуля

Время ожидания модуля необходимо настроить. Значение выбирается с учетом продолжительности цикла контроллера, конфигурации горячего резерва (если горячий резерв используется), и безопасной продолжительности процесса, см. *Безопасная продолжительность процесса, стр. 74*.

При постоянных неудачных попытках обмена с ЦПУ модуль цифровых выводов перезагружается после фиксированного времени ожидания, равного 65 секундам, таким образом, состояние всех выводов изменится на 0 независимо от заданного времени ожидания.

2.3 Модули питания

Модули питания ПЛК безопасности Quantum

Введение

Следующие модули питания имеют сертификаты соответствия для применения в контроллерах безопасности Quantum:

- 140 CPS 124 20

	**ВНИМАНИЕ** **УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ** Разрешается применять другие модули питания кроме Quantum 140 CPS 124 20. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Особенности модуля

Данный модуль имеет функцию контроля и защиты от перенапряжения. Далее, модуль поддерживает функцию резервирования. При отказе одного модуля другой принимает на себя функции и начинает снабжать монтажное шасси необходимым питанием.

Примечание: Компания рекомендует всегда применять по два модуля питания Quantum для каждого монтажного шасси в контроллерах безопасности Quantum.

Примечание: Одного модуля питания (140 CPS 124 20) должно быть достаточно для нормального обеспечения питанием удаленного устройства.

Подробнее о конфигурации модулей см. *Примеры конфигурации ПЛК безопасности Quantum, стр. 61*.

2.4 Модули, не влияющие на уровень безопасности

Модули, не влияющие на уровень безопасности, ПЛК безопасности Quantum

Введение

Следующие модули имеют сертификаты соответствия и могут применяться в качестве модулей, не влияющих на уровень безопасности, в контроллерах безопасности Quantum:

- 140 CRP 932 00 (RIO Головной адаптер)
- 140 CRA 932 00 (RIO адаптер удаленного устройства)
- 140NOE771 11 (Модуль Ethernet)
- 140 XBP 016 00 (Шасси, 16 слотов)
- 140 XBP 010 00 (Шасси, 10 слотов)
- 140 XBP 006 00 (Шасси, 6 слотов)
- 140 DDI 353 00 (модуль цифрового ввода)
- 140 DDO 353 00 (модуль цифрового вывода)
- 140 ACI 040 00 (модуль аналогового ввода)
- 140 ACO 020 00 (модуль аналогового вывода)

Определение адаптеров удаленного ввода/вывода

Головной адаптер удаленного ввода/вывода (RIO) 140 CRP 932 00 и адаптер удаленного устройства 140 CRA 932 00 обеспечивают связь между модулем ЦП безопасности и удаленными вводами/выводами безопасности. Подробнее об этой теме см. *Описание связи между ЦПУ и вводами/выводами, стр. 40*. Все стандартные компоненты компании , предназначенные для соединения проводами удаленных вводов/выводов (кабели, соединительные разъемы и так далее) можно применять в системе безопасности.

Определение модуля Ethernet

Модуль Ethernet 140 NOE 771 11 обеспечивает связь между контроллером безопасности и другими контроллерами, ЧМИ и вводами/выводами по сети Ethernet. Данный модуль не изменяет данные, имеющие отношение к безопасности, и поэтому не является частью контура безопасности. Подробнее об этой теме см. *Связь между контроллерами, стр. 109*. Модуль Ethernet можно устанавливать только в локальное монтажное шасси.

Определение шасси

Шасси 140 XBP 016 00, 140 XBP 010 00 и 140 XBP 006 00 представляют собой устройства, предназначенные для установки всех модулей безопасности и модулей, не влияющих на уровень безопасности.

Примечание: Средства расширения шасси нельзя применять в контроллерах безопасности Quantum.

Определение модулей ввода/вывода

Модули ввода/вывода в контроллере безопасности можно настраивать. Тем не менее, они должны являться частью контура безопасности.

	**ПРЕДУПРЕЖДЕНИЕ** **НЕПРАВИЛЬНОЕ ИСПОЛЬЗОВАНИЕ ДАННЫХ БЕЗОПАСНОСТИ** Запрещается использовать входы или выходы модулей, не влияющих на уровень безопасности, в качестве выходов безопасности. Данные модули применяются исключительно для обработки сигналов, не имеющих отношение к безопасности. На логику, применяющуюся для обработки нейтральных вводов/выводов, распространяются те же правила, что и на логику безопасности. Нейтральные вводы/вывода должны быть внесены в безопасный раздел памяти (свободный раздел памяти используется только для функциональных блоков S_S_MOVE_***). **Не соблюдение этих инструкций может привести к серьезным травмам или повреждению оборудования.**

2.5 Поведение системы при неполадках

Начальные сведения

Введение

Модули ЦП безопасности и модули вводов/выводов безопасности имеют встроенные средства диагностики, при помощи которых проверяется проверка правильности работы модулей. В данной главе приводится описание поведения модулей при появлении неполадки. Далее приводится описание Ваших действий.

Что в этом параграфе?

В этом параграфе имеются следующие темы:

Модули безопасности ЦП - поведение при неисправности

Общие сведения

Система диагностики ЦПУ проверяет правильность работы аппаратных средств и программы, см. *Модуль ЦП безопасности, без горячего резерва, стр. 34*. При обнаружении отказа во время одной из проверок ЦПУ переходит в состояние ошибки и состояние всех выводов безопасности меняется безопасным.

Устранение неисправностей

При обнаружении неисправности выполните следующие действия:

Шаг	Действие
1	Выключите питание всего контроллера.
2	Затем снова включите. **Результат:** Запущена самодиагностика.
3	Проверьте содержимое системного слова %SW125, %SW126 и %SW127 и получите сведения о состоянии неисправности, см. *Описание системных слов от %SW60 до %SW127, стр. 162*.
4	Направьте сведения из системных слов, указанных в шаге 3 и из проекта инструментальной системы Unity Pro в службу поддержки компании .

Некоторые неисправности могут носить временный характер и пропасть после перезапуска контроллера. В других случаях может потребоваться замена ЦПУ.

Примечание: При необходимости можно включить опцию автоматического запуска ЦПУ - **Automatic start in Run** (хотя стоит отметить, что в случае контроллера безопасности это не рекомендуется). Если выявленная диагностикой неисправность сохраняется, ЦПУ снова переходит в состояние неисправности и останавливается. Чтобы иметь возможность просмотреть значения системных слов необходимо предотвратить повторный запуск

- либо вынув карту памяти PCMCIA (приложение хранится на карте памяти)
- либо вставить пустую карту памяти PCMCIA (приложение хранится в памяти).

ВНИМАНИЕ

НЕПРЕДНАМЕРЕННЫЕ ОТКЛОНЕНИЯ В РАБОТЕ ОБОРУДОВАНИЯ

Используйте опцию **Automatic start in Run** только в редких случаях. При использовании данной опции Вам придется запрограммировать и настроить систему таким образом, чтобы она нормально работала после перезапуска.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Содержимое системного слова

Слово %SW125 содержит причину обнаруженной неисправности и может иметь следующее значение:

Код	Описание
0x5AF1	неправильная последовательность (непредсказуемое выполнение в ЦПУ)
0x5AF2	ошибка памяти (неправильный адрес)
0x5AF3	ошибка сравнения (результат, полученный после выполнения процессором Intel отличается от результата, полученного после выполнения прикладным процессором)
0x5AF4	неисправность часов реального времени
0x5AF5	ошибка при инициализации выполнения двойного кода
0x5AF6	ошибка включения таймера "watchdog"
0x5AF7	ошибка во время проверки памяти (занимает свыше 8 часов)
0x5AF8	ошибка при проверке памяти (неисправность ОЗУ)

Слова %SW126 и %SW127 содержат сведения, предназначенные для внутреннего пользования и детального анализа неисправностей специалистами компании .

Модули вводов/выводов безопасности - поведение при неисправности

Общие сведения

Модули вводов/выводов безопасности могут выявлять внутренние ошибки
- либо в канале
- либо во всем модуле

Неисправность канала

Если в канале обнаружена неполадка, этот канал переключается в безопасное состояние, а другой канал продолжает работать. Сведения о неисправности содержатся в регистрах состояния модулей (см. главу "Модуль вводов/выводов безопасности Quantum" в справочнике *Модули аналоговых и дискретных вводов/выводов Quantum)*. В зависимости от типа неисправности может потребоваться замена всего модуля.

Неисправность модуля

При обнаружении неисправности модуль ввода/вывода перезагружается, выполняется повторный запуск и запускается система самодиагностики при включении:

Если самодиагностика при включении питания ...	**Тогда, модуль ...**
завершается успешно	запускается и далее нормально работает.
выявляет ошибки	перезапускается и процедура повторяется заново. В этом случае модуль подлежит замене.

2.6 Примеры конфигурации

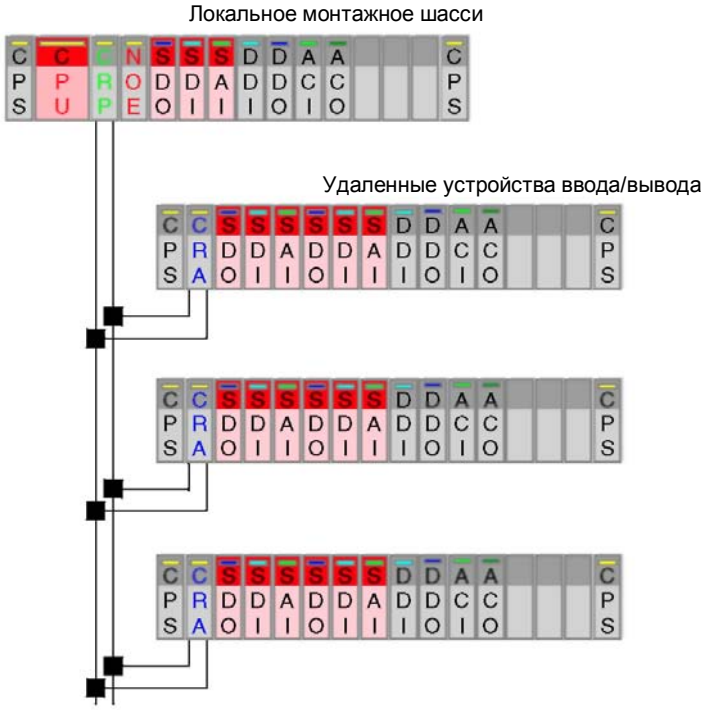
Примеры конфигурации ПЛК безопасности Quantum

Введение

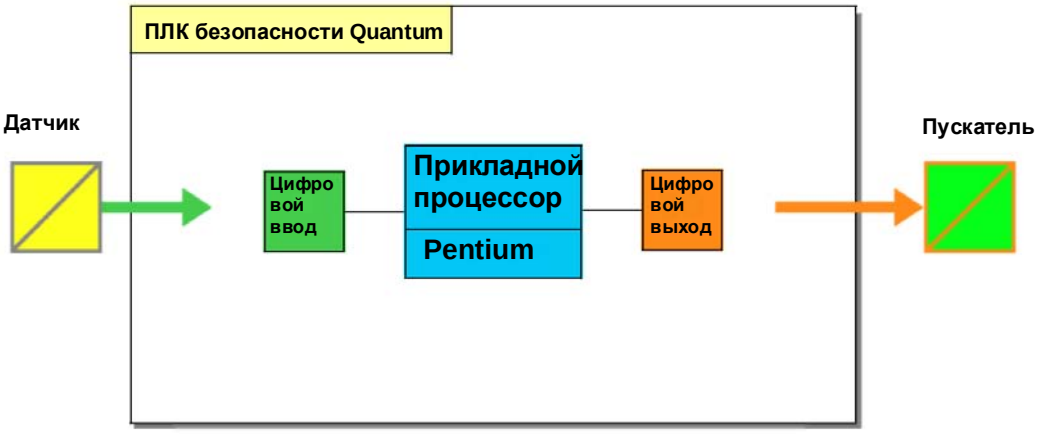
В состав контроллера безопасности Quantum входит локальное монтажное шасси и устройства удаленного ввода/вывода. На локальном шасси должен быть установлен модуль ЦП безопасности, модули питания, пригодные к использованию в системах безопасности, и модули вводов и выводов безопасности. Если используется модуль Ethernet NOE, он также устанавливается на локальное шасси. Модули, не влияющие на уровень безопасности, за исключением модуля Ethernet NOE, могут устанавливаться как на локальное монтажное шасси, так и удаленные устройства ввода/вывода. В зависимости от потребностей и степени отказоустойчивости контроллер безопасности, а также модуль вводов/выводов безопасности можно сконфигурировать как с резервированием, так и без него.

Конфигурация без резерва

На рисунке ниже показан пример конфигурации контроллера безопасности Quantum без горячего резерва. В данном случае в состав контроллера входит локальное монтажное шасси и устройства удаленного ввода/вывода:



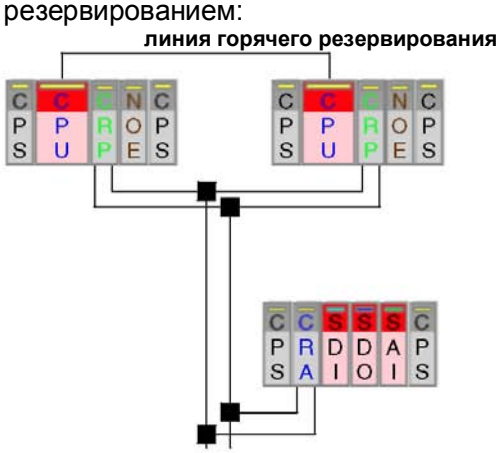
Следующий рисунок дает соответствующий функциональный обзор:



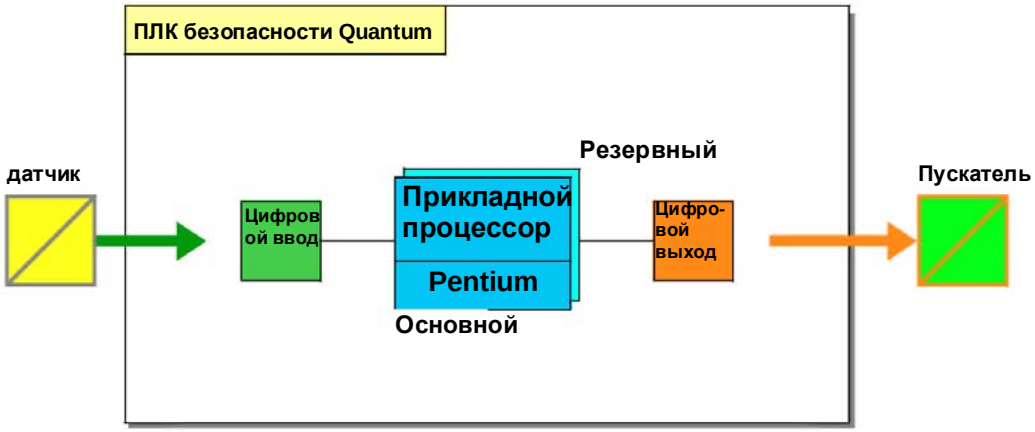
Примечание: Только устройства безопасности компании имеют сертификаты для применения в контроллерах безопасности Quantum, и поэтому подходят для работы с данными безопасности. Модули, не влияющие на уровень безопасности, такие как модуль Ethernet NOE, имеют сертификаты только для работы с данными, не имеющими отношения к безопасности. Тем не менее, они могут входить в состав контроллера безопасности Quantum, потому что не препятствуют работе системы безопасности. Тем не менее, они не способны выполнять функции безопасности. Кроме этого, можно подсоединять другие устройства, например средства человеко-машинного интерфейс (ЧМИ). Данные устройства не являются частью контура безопасности, потому что они не могут записывать данные безопасности напрямую, см. также *Связь между контроллером и ЧМИ, стр. 111*.

Конфигурации с резервированием ЦПУ для увеличения отказоустойчивости

На рисунке ниже приведен пример контроллера безопасности Quantum с горячим резервированием. В данном случае контроллер состоит из ЦПУ с резервированием:

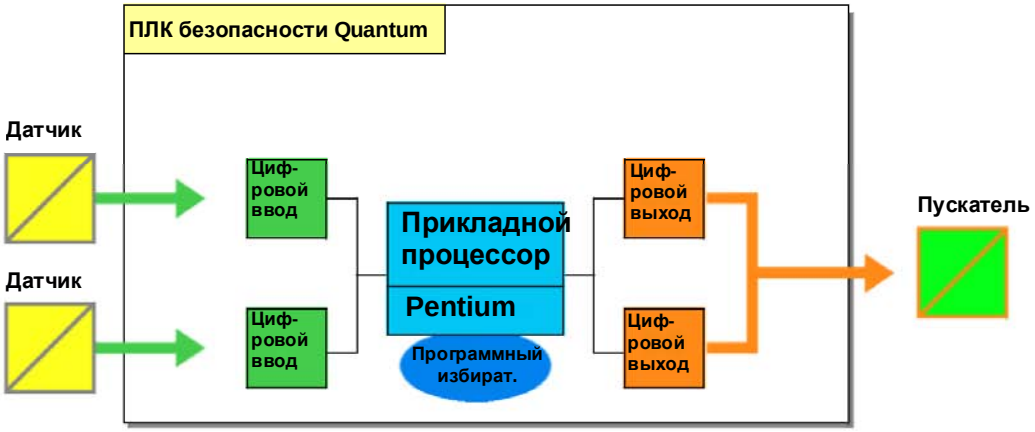


Следующий рисунок дает соответствующий функциональный обзор:



Конфигурации с резервированием вводов/выводов для увеличения отказоустойчивости

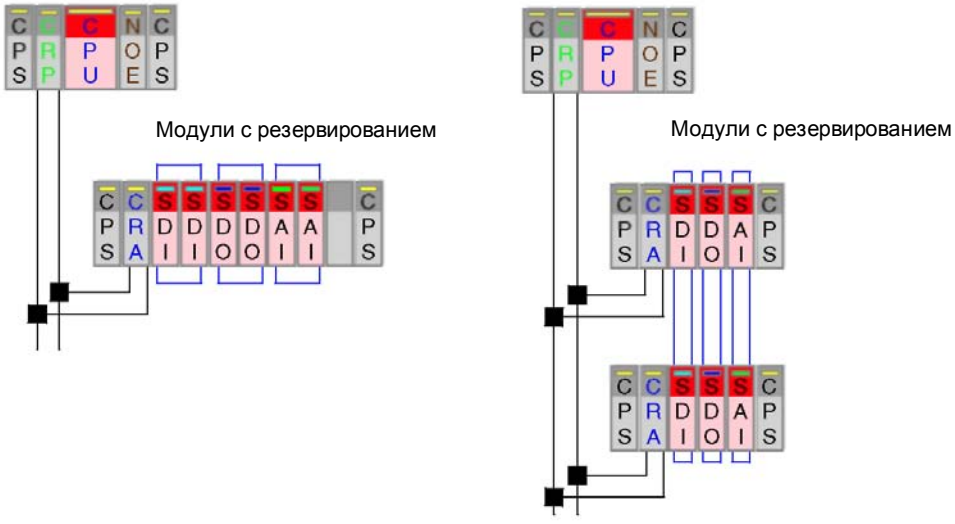
На рисунке ниже приведена функциональная схема конфигурации с резервированием вводов/выводов. В данном случае в состав входит один ЦПУ и вводы/выводы с резервированием:



Модули вводов/выводов безопасности с резервированием можно устанавливать

- либо в одно устройство удаленного ввода/вывода (не рекомендуется)
- либо в разные устройства удаленного ввода/вывода (рекомендуется, когда используются модули вводов/выводов безопасности с резервированием).

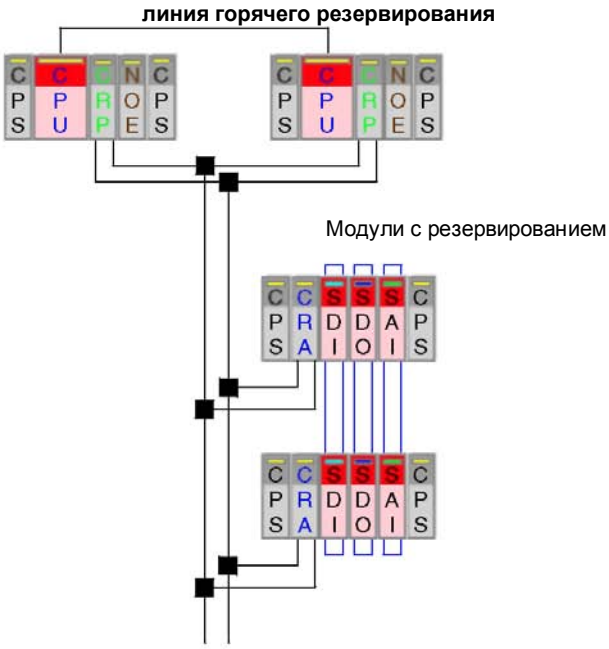
На рисунке ниже показаны вводы/выводв с резервированием, установленные в одном устройстве удаленного ввода/вывода (слева) и в разных устройствах удаленного ввода/вывода (справа):



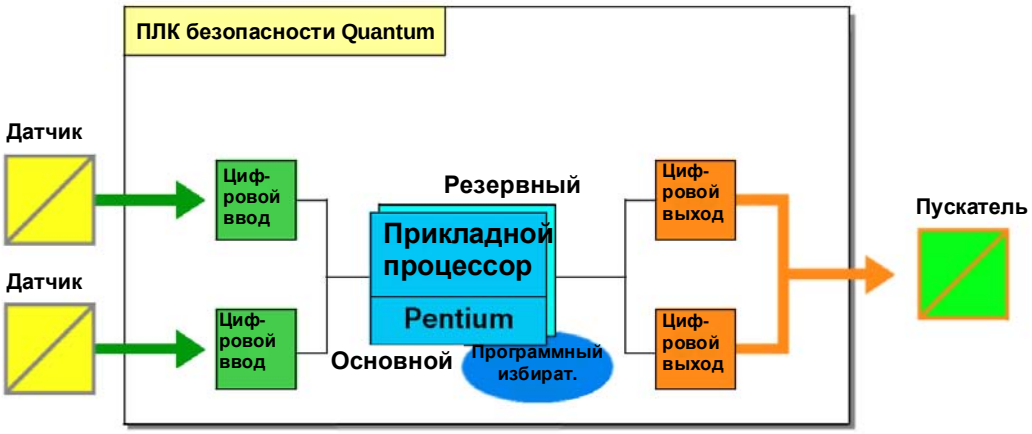
Примечание: Компания рекомендует всегда устанавливать модули вводов/выводов безопасности с резервированием в разные устройства удаленного ввода/вывода.

Конфигурации с резервированием ЦПУ и вводов/выводов

На рисунке ниже приведен пример контроллера безопасности Quantum с резервированием. В данном случае контроллер состоит из ЦПУ с резервированием и вводов/выводов с резервированием:



Следующий рисунок дает соответствующий функциональный обзор:



Примечание: Компания рекомендует всегда устанавливать модули вводов/выводов безопасности с резервированием в разные устройства удаленного ввода/вывода.

Программирование

3

Начальные сведения

Введение

В этой главе рассматриваются темы, важные с точки зрения программирования проекта безопасности. С одной стороны, приводится описание требований безопасности, с другой стороны - объясняются специальные функции.

Что в этой главе?

В этой главе содержатся следующие параграфы:

3.1 Общие сведения о программировании

Начальные сведения

Введение

В этом параграфе приводятся общие сведения по программированию проекта безопасности с учетом требований к программированию и мониторингу.

Что в этом параграфе?

В этом параграфе содержатся следующие темы:

Языки программирования

Введение

Для программирования проекта безопасности разрешается использовать только два следующих языка программирования:

- язык функциональных блок-схем (FBD)
- язык лестничной логики (LD)

Оба этих языка установлены стандартом IEC 61131-3 для программирования программируемых логических контроллеров.

Описание ограничений по языку

При создании проекта безопасности действуют следующие ограничения:

- Во время создания проекта инструментальная система Unity Pro XLS ограничивает выбор языка программирования.
- Во время импорта инструментальная система Unity Pro XLS игнорирует все разделы, не использующие схемы FBD или LD, но не прерывает процесс импорта. Если в частях программы использован язык, отличный от FBD или LD, это приведет к ошибке.
- Во время анализа инструментальная система Unity Pro XLS проверяет язык в каждой части программы. Если в части программы выявлена ошибка, программа не будет создана.

Подробное описание ограничений по структуре программы, элементам языка и конфигурации данных приведено в теме *Требования к программированию и исключения, стр. 71.*

Требования к программированию и исключения

Введение

Для программирования проекта безопасности необходимо использовать только языки программирования FBD и LD, соблюдая в то же время перечень приведенных ниже правил, касающихся структуры программы, элементов языка и конфигурации данных.

Требования к структуре программы

Вы можете выполнять следующие действия:

- программировать проект безопасности в разделах управляющей задачи (MAST task)

Вы не можете выполнять следующие действия:

- программировать задачи **FAST, TIMER, INTERRUPT** и **AUX**. При импорте инструментальная система Unity Pro XLS игнорирует неразрешенные объекты и информирует пользователя об их существовании. Если пользователь продолжает операцию, то импорт осуществляется без неразрешенных объектов, что может привести к ошибкам или сбою, если импорт будет невозможен.
- использовать подпрограммы (разделы SR).
- составлять план сегментов.
- параллельно вызывать устройства удаленного ввода/вывода.

	ВНИМАНИЕ
	**ВОЗМОЖНАЯ УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ** Запрещается использовать функцию условного исполнения раздела. Хотя существует возможность условно исполнять разделы на основе значения переменной типа Boolean (видимой в режиме online), компания не рекомендует использовать эту функцию в инструментальной системе Unity Pro XLS. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Требования к элементам языка

Вы можете применять только:
- функции и функциональные блоки (FFBs), сертифицированные к применению в логике безопасности и описанные в библиотеке блоков безопасности инструментальной системы Unity Pro.

Вы не можете применять:
- производные функциональные блоки (DFB) или
- выражения структурированного текста (ST).

В языке лестничной логики (LD) вы не можете применять:
- катушки приостановки,
- катушки вызова,
- возвраты,
- рабочие блоки, или
- сравнительные блоки.

Примечание: Несмотря на то, что в языках FBD и LD разрешены переходы к меткам, компания не рекомендует применять их, чтобы структура логики безопасности была лучше.

Требования к конфигурации данных

Вы можете применять только:
- данные расширенного типа (EDT) `BOOL, EBOOL, BYTE, WORD, DWORD, INT, UINT, DINT, UDINT` и `TIME`.
- простые массивы, но только для глобального соединения в сети Ethernet
- прямую адресацию, например, указывая %MW4000 при помощи катушки в языке лестничной логики.
- переменные, привязанные к определенному месту. Все случаи использования переменных не только проверяются на привязку к определенному месту, но также на привязку к соответствующей области памяти, см. также *Раздел памяти, стр. 105.*

Вы не можете создавать:
- производные типы данных (DDT).

Примечание: Не разрешается использовать переменные из раздела свободной памяти в пользовательской логике, если только пользователь не может связать их с вводом функциональных блоков `S_SMOVE_BIT` или `S_SMOVE_WORD`, см. также *Раздел памяти, стр. 105*.

Проверки при программировании

Во время создания проекта безопасности, программа Unity Pro XLS предлагает только те опции, которые разрешены для логики безопасности. Попытка создания неразрешенных объектов приводит к ошибке.

Однако неразрешенные объекты можно вставлять посредством импорта файла источника. Таким образом, инструментальная система Unity Pro XLS проверяет все объекты во время анализа. При выявленном несоблюдении какого-либо требования или обнаружении неразрешенного объекта, инструментальная система Unity Pro XLS выдает ошибку и не генерирует проект пользователя.

В настройках проекта инструментальной системы Unity Pro XLS имеются различные опции предупреждений, которые выдаются системой во время проверки языка:
- Неиспользуемые переменные
- Многократная запись переменных
- Неприсвоенные параметры
- Многократное использование функциональных блоков
- Дублирование адресов

ВНИМАНИЕ

ВОЗМОЖНАЯ УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ

Включить все опции предупреждений в настройках проекта и убедиться, что они не являются критическими и что их использование является правильным.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Требования к мониторингу

Инструментальная система Unity Pro XLS представляет собой единственное программное средство, используемое для загрузки или изменения проекта безопасности. Другие программные пакеты или ЧМИ могут только отслеживать состояние и функции системы безопасности, но они не позволяют менять их. Другим устройствам разрешено считывать данные из контроллера безопасности, но запись данных в контроллер безопасности имеет ограничения, см. также *Раздел памяти, стр. 105.*

Безопасная продолжительность процесса

Определение безопасной продолжительности процесса

Безопасная продолжительность процесса (PST) - критически важный параметр каждого технологического процесса. Он определяется как период между появлением сбоя в работе контролируемого оборудования (EUC) и возникновением опасного события в случае невыполнения функции безопасности.

Примечание: Безопасная продолжительность процесса обусловлена технологическим процессом. Необходимо, чтобы система безопасности выполняла функции безопасности не позднее времени, определенного как безопасная продолжительность процесса.

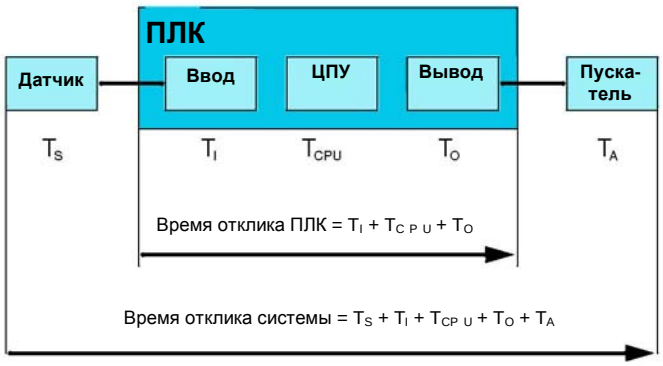
Определение времени отклика системы

Время отклика системы представляет собой сумму времени отклика ПЛК, времени отклика используемого датчика (TS) и времени отклика используемого пускателя (TA). Значения T_S и T_A зависят от конкретного устройства.

Применяется следующее уравнение:

Время отклика системы = время отклика ПЛК + T_S + T_A

Иллюстрация к этому уравнению приведена ниже:



Время отклика системы должно быть меньше времени безопасной продолжительности процесса.

Определение времени отклика ПЛК

Время отклика ПЛК представляет собой сумму времени отклика используемого модуля ввода (T_I) и времени отклика используемого модуля вывода (T_O) и время отклика ЦПУ (T_{CPU}).

Применяется следующее уравнение:

Время отклика ПЛК = T_{CPU} + T_I + T_O

Определение времени отклика ЦПУ

Время отклика ЦПУ непосредственно зависит от времени цикла ЦПУ, необходимого для выполнения логики безопасности. Сигнал может появиться в самом начале выполнения цикла, после того как другие сигналы были уже обработаны. Поэтому для отклика на сигнал может потребоваться два цикла.

Соответственно, применяется следующее уравнение:

Время отклика ЦПУ = 2 x продолжительность цикла ЦПУ

Кроме того, можно определить максимальное количество допустимых ошибок CRC (N_{CRC}) во время связи с другими вводами/выводами. Данное условие вводится для снижения ложных воздействий (например, вызванных нарушением электромагнитной совместимости). Количество допустимых ошибок можно задать в диапазоне от 0 до 3. Данное значение следует учитывать, поскольку возрастает количество циклов модуля вывода, необходимых для отклика.

Таким образом, уравнение выше принимает вид:

Время отклика ЦПУ = (2 + N_{CRC}) x продолжительность цикла ЦПУ

Определение времени отклика модулей ввода

Максимальное время отклика (в самом худшем случае) модуля цифрового ввода безопасности и модуля аналогового ввода безопасности T_I составляет 45 мс (3 x продолжительность цикла модуля).

Определение времени отклика модулей вывода

Максимальное время отклика (T_O) модуля цифрового вывода безопасности представляет собой сумму 15 мс и заданного времени ожидания модуля *T_{OUT}. Время ожидания модуля должно быть обязательно больше продолжительность цикла ЦПУ.

Соответственно, применяется следующее уравнение:

$T_O = T_{OUT}$ + 15 мс

Более подробно о настройке времени ожидания модулей цифрового вывода см. в главе "Настройка модулей ввода/вывода для проектов безопасности" в руководстве на Инструментальную систему Unity Pro XLS, Режим работы.

Определение максимальной продолжительности цикла ЦПУ

Зная требуемое время PST и максимальное время отклика датчиков и пускателей, можно рассчитать максимальное время отклика ПЛК, приемлемое для конкретного технологического процесса.

Чтобы время отклика системы было меньше времени безопасной продолжительности процесса, максимальное время цикла ЦПУ должно удовлетворять следующему условию:

Макс. продолжительность цикла ЦПУ < (PST - T_I - T_O - T_S - T_A) / (2 + N_{CRC})

Кроме того, необходимо учитывать следующую зависимость между максимальным временем отклика модулей вывода ($T_{O)}$ и максимальным временем продолжительности цикла ЦПУ:

Макс. продолжительность цикла ЦПУ < T_O / (1 + N_{CRC})

Пример расчета

Даны следующие значения:
- требуемое время безопасной продолжительности процесса (PST) = 1,1 с
- T_I = 45 мс
- T_O = TOUT + 15 мс = 140 мс + 15 мс = 155 мс
- T_S = 100 мс
- T_A = 500 мс
- N_{CRC} = 1

Максимальное время продолжительность цикла ЦПУ вычисляется следующим образом:

Макс. продолжительность цикла ЦПУ < (1100 мс - 45 мс - 155 мс - 100 мс - 500 мс) / 3

Макс. продолжительность цикла ЦПУ < 100 мс

Требование, состоящее в том, чтобы время ожидания модуля цифрового вывода было больше времени продолжительности цикла ЦПУ, удовлетворено:

TOUT = 140 мс > продолжительность цикла ЦПУ (и макс. < 100 мс)

Продолжительность цикла ЦПУ в системе с горячим резервом

Для нормально работающей системы с горячим резервированием формула времени продолжительности цикла ЦПУ выглядит аналогичным образом:

Макс. продолжительность цикла ЦПУ < (PST - T_I - T_O - T_S - T_A) / (2 + N_{CRC})

Кроме того, необходимо учитывать следующую зависимость между максимальным временем отклика модулей вывода (T_O) и максимальным временем продолжительности цикла ЦПУ:

Макс. продолжительность цикла ЦПУ < T_O / (3 + N_{CRC})

Конфигурирование максимальной продолжительности цикла ЦПУ

Контроллеры безопасности Quantum могут работать в непрерывном (цикличном) или периодическом режиме. Разницы между циклическим и периодическим режимами стандартного контроллера Quantum и контроллера безопасности Quantum нет. В обоих случаях вам потребуется задать максимальное приемлемое время продолжительности цикла ЦПУ в инструментальной системе Unity Pro XLS.

Максимальное допустимое время продолжительности цикла ЦПУ (таймер "watchdog") задается в свойствах главной задачи (MAST). Подробнее см. главу "Программирование" в руководстве с описанием рабочих режимов *инструментальной системы Unity Pro* и главу "Введение в главную задачу" в справочнике *Структура программы и языки Unity Pro*.

Примечание: Минимальное время продолжительности цикла ЦПУ составляет 20 мс.

Примечание: Следует задавать максимальное количество только действительно необходимых %M и %MW. Все сконфигурированные диапазоны памяти %M и %MW будут сравниваться во время выполнения двойного кода, поэтому времени потребуется больше (примерно 5,5 мс на каждые 10,000 слов). Таким образом, увеличивать продолжительность цикла нет необходимости, если вы сконфигурировали больше памяти, чем нужно.

Время продолжительности цикла ЦПУ необходимо проверять при вводе проекта в эксплуатацию. На этом этапе инструментальная система Unity Pro XLS предоставляет значения в реальном масштабе времени от ПЛК.

Эти данные можно просмотреть
- на закладке **Task** (меню **Tools -> PLC Screen)**.
- в слове %SW30, где содержится текущее время выполнения задачи MAST .
- в слове %SW31, где содержится максимальное время выполнения задачи MAST .
- в слове %SW32, где содержится минимальное время выполнения задачи MAST .

Подробнее см. *Определение системных слов от %SW30 до %SW59, стр. 158* или в главе "Определение системных слов от %SW30 до %SW47" в справочнике *Структура программы и языки Unity Pro.* Если заданное пользователем максимально допустимое время продолжительности цикла ЦПУ превышено, потребуется скорректировать значения настройки или логику пользователи, или оба сразу, чтобы добиться требуемого значения.

ВНИМАНИЕ

ОПАСНОСТЬ ПРЕВЫШЕНИЯ БЕЗОПАСНОЙ ПРОДОЛЖИТЕЛЬНОСТИ ПРОЦЕССА

Вводите максимальное время продолжительности цикла ЦПУ с учетом установленного времени безопасной продолжительности процесса.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

3.2 Описание программного обеспечения

Начальные сведения

Введение

В данном параграфе приводится описание возможностей инструментальной системы Unity Pro XLS, разработанных специально для программирования проектов безопасности.

Что в этом параграфе?

В этом параграфе имеются следующие темы:

Инструментальная система Unity Pro XLS

Введение

В соответствии с требованиями стандарта IEC 61508 разрешается применять только лицензированное программное обеспечение для программирования проектов безопасности. Поэтому компания разработала специальную версию инструментальной системы Unity Pro XLS (eXtra Large Safety). В данной версии можно и выполнять диагностику неисправностей, и обеспечивать защиту проекта в объеме, достаточном для программирования проекта безопасности.

Примечание: При создании нового проекта в инструментальной системе Unity Pro XLS вы выбирате тип контроллера Quantum, таким образом определяя вид создаваемого проекта - проект безопасности или обычный, т.е. не имеющий отношения к безопасности.

Проект безопасности и обычный

Инструментальную систему Unity Pro XLS можно использовать для программирования как обычных проектов, так и проектов безопасности. Благодаря этому вам не потребуется другое программное обеспечение для программирования. На одном компьютере может быть установлена только одна версия этой программы.

Проект безопасности хранится в виде двоичных файлах проекта *(STU)* и в файлах архива проекта *(STA).* Данные файлы можно открыть только в специальной версии инструментальной системы Unity Pro для создания проектов безопасности. Кроме этого, пользователь может загружать исполняемые двоичные файлы *(APX)* только в модуль ЦП безопасности. Подробнее см. главу "Службы в режиме Offline" в руководстве на инструментальную систему Unity Pro, Рабочие режимы

Обычные проекты, созданные в обычной версии инструментальной системы Unity Pro, можно экспортировать при помощи подходящей версии программы Unity Pro и импортировать в версию Unity Pro XLS.

Определение проекта защиты

В инструментальной системе Unity Pro XLS предусмотрена защита от несанкционированного доступа к проектам безопасности, контроллеру безопасности Quantum и непосредственно самой инструментальной системе Unity Pro XLS.

Ваш проект безопасности и контроллер безопасности Quantum защищены при помощи следующих механизмов:
- Защита проекта безопасности реализована в виде защиты паролем на уровне приложения (т.е. паролем проекта). При создании проекта безопасности используется пустой пароль, который вы можете изменить.
- Контроллер безопасности Quantum также имеет защиту в виде пароля проекта. Если в контроллере отсутствует проект, можно ввести любой пароль.
- При подключении к контроллеру безопасности появится запрос на ввод пароля проекта, если в данный момент в инструментальной системе Unity Pro XLS открыт другой проект, или не открыт ни один из проектов.

Защита самой инструментальной системы Unity Pro XLS реализована при помощи следующих механизмов:
- Вы можете установить права доступа или выбрать список функций, которые пользователь имеет право использовать в Security Editor, который входит в комплект инструментальной системы Unity Pro XLS (и имеет те же функциональные возможности, что и версия Unity Pro XL).
- По истечении заданного времени бездействия инструментальная система Unity Pro XLS автоматически блокируется. Для продолжения работы потребуется ввести пароль проекта. Пока инструментальная система Unity Pro XLS находится в заблокированном состоянии, соединение с контроллером не прерывается и он остается в текущем режиме.

Определение редактора Security Editor

Для защиты инструментальной системы Unity Pro XLS от несанкционированного доступа предусмотрен редактор Security Editor, который позволяет
- устанавливать правила, создавать профили и пользователей.
- управлять правами доступа к системе.

Например, можно ограничить доступ пользователей в отношении
- создания или изменения пароля проекта,
- переключения в Служебный режим, или
- изменения времени ожидания, после которого программа автоматически заблокируется.

Подробнее о редакторе Security Editor см. в главе "Управление правами доступа" в руководстве *Инструментальная система Unity Pro, Рабочие режимы* и главе "Управление конфиденциальностью в системе Unity Pro XLS" в руководстве *Инструментальная система Unity Pro XLS, Особенности режимов работы.*

Примечание: Используйте возможности редактора Security Editor для защиты инструментальной системы Unity Pro XLS от несанкционированного доступа. Стоит отметить, что возможности редактора Security Editor не устраняют необходимость защиты проекта безопасности паролем.

Определение функции автоматической блокировки

В инструментальной системе Unity Pro XLS предусмотрена возможность включения функции блокировки по истечению заданного времени простоя для защиты от несанкционированного доступа. По истечению времени инструментальная система Unity Pro XLS предложит ввести пароль проекта.

Подробное описание функции автоматической блокировки см. в главе "Защита проекта безопасности в инструментальной системе Unity Pro XLS" в руководстве *Особенности работы инструментальной системы Unity Pro XLS*.

Значения по умолчанию

При создании нового проекта безопасности значения по умолчанию выглядят следующим образом:

- Пароль проекта - пустой.
- Функция автоматической блокировки включена, время простоя составляет 10 минут, по истечении которых Unity Pro XLS будет заблокирована.

Функции/Функциональные блоки для систем безопасности

Введение

Компания разработала ряд элементарных функций (EF) и функциональных блоков (EFB), которые сертифицированы для применения в проектах безопасности. Подробнее см. библиотеку функциональных блоков Unity Pro для применения в проектах безопасности.

Примечания

Функциональные блоки FFB, которые можно использовать для различных типов данных, имеют метку в виде ***.

Например, элементарную функцию S_AND_*** можно применять со следующими типами данных

- BOOL как S_AND_BOOL.
- BYTE как S_AND_BYTE.
- WORD как S_AND_WORD.
- DWORD как S_AND_DWORD.

Определение математических функциональных блоков (FFB) для проектов безопасности

В таблице ниже приведен перечень функциональных блоков (FFB), принадлежащих семейству математических функций:

Наименование	Тип	Применяется для...
S_ADD_***	EF	сложения значений вводов
S_SUB_***	EF	вычитания значения ввода 2 из значения ввода 1
S_MUL_***	EF	умножения значения ввода
S_DIV_***	EF	деления значения ввода делителя на значение ввода делимого
S_NEG_***	EF	отрицания значений ввода
S_ABS_***	EF	вычисления абсолютной величины значения ввода
S_SIGN_***	EF	определения знаков "минус"
S_SMOVE_BIT	EFB	присвоения значения ввода выводу (для использования данных из раздела свободной памяти в логике безопасности)
S_SMOVE_WORD		

Определение сравнительных функциональных блоков (FFB) для проектов безопасности

В таблице ниже приведен перечень функциональных блоков (FFB), принадлежащих семейству функций сравнения:

Наименование	Тип	Применяется для сравнения значений последующих вводов...
S_EQ_***	EF	на равенство
S_GT_***	EF	на убывание
S_GE_***	EF	на убывание или равенство
S_LT_***	EF	на возрастание
S_LE_***	EF	на возрастание или равенство
S_NE_***	EF	на неравенство

Определение логических функциональных блоков (FFB) для проектов безопасности

В таблице ниже приведен перечень функциональных блоков (FFB), принадлежащих семейству логических функций:

Наименование	Тип	Применяется для...
S_AND_***	EF	побитовой цепочке AND последовательности входных битов
S_OR_***	EF	битовой цепочке OR последовательности входных битов
S_XOR_***	EF	битовой цепочке XOR последовательности входных битов
S_NOT_***	EF	побитового отрицания входной последовательности
S_SHL_***	EF	сдвига комбинации битов влево
S_SHR_***	EF	сдвига комбинации битов вправо
S_ROL_***	EF	кругообразного поворота комбинации разрядов влево
S_ROR_***	EF	кругообразного поворота комбинации разрядов вправо
S_RS	EFB	в качестве памяти сброса (RS) с доминантным вводом сброса
S_SR	EFB	в качестве памяти состояния (SR) с доминантным вводом состояния
S_F_TRIG	EFB	обнаружения заднего фронта импульса
S_R_TRIG	EFB	обнаружения переднего фронта импульса

Определение статистических функциональных блоков (FFB) для проектов безопасности

В таблице ниже приведен перечень функциональных блоков (FFB), принадлежащих к семейству статистических функций:

Наименование	Тип	Применяется для...
S_MIN_***	EF	присвоения наименьшего значения ввода выводу
S_MAX_***	EF	присвоения наибольшего значения ввода выводу
S_LIMIT_***	EF	передачи неизмененного значения ввода выводу, если он находится в пределах диапазона (между мин. и макс.)
S_MUX_***	EF	передачи соответствующего значения ввода выводу в зависимости от значения ввода K
S_SEL	EF	двоичной выборки между двумя значения вводов

Определение функциональных блоков (FFB) таймеров и счетчиков для проектов безопасности

В таблице ниже приведен перечень функциональных блоков (FFB), принадлежащих к семейству функций таймеров и счетчиков:

Наименование	Тип	Применяется для...
S_CTU_***	EFB	отсчета на возрастание
S_CTD_***	EFB	отсчета на убывание
S_CTUD_***	EFB	отсчета на возрастание и убывание
S_TON	EFB	в качестве таймера задержки включения
S_TOF	EFB	в качестве таймера задержки выключения
S_TP	EFB	формирования импульса определенной длины

Определение функциональных блоков преобразования типов (FFB) для проектов безопасности

В таблице ниже приведен перечень функциональных блоков (FFB), принадлежащих к семейству функций преобразования типов:

Наименование	Тип	Применяется для преобразования значения ввода из...
S_BOOL_TO_***	EF	типа BOOL в тип BYTE, WORD, DWORD, INT, DINT, UINT или UDINT
S_BYTE_TO_***	EF	типа BYTE в тип BOOL, WORD, DWORD, INT, DINT, UINT или UDINT
S_WORD_TO_***	EF	типа WORD в тип BOOL, BYTE, DWORD, INT, DINT, UINT, или UDINT
S_DWORD_TO_***	EF	типа DWORD в тип BOOL, BYTE, WORD, INT, DINT, UINT или UDINT
S_INT_TO_***	EF	типа INT в тип BOOL, BYTE, WORD, DWORD, DINT, UINT или UDINT
S_DINT_TO_***	EF	типа DINT в тип BOOL, BYTE, WORD, DWORD, INT, UINT или UDINT
S_UINT_TO_***	EF	типа UINT в тип BOOL, BYTE, WORD, DWORD, INT, DINT или UDINT
S_UDINT_TO_***	EF	типа UDINT в тип BOOL, BYTE, WORD, DWORD, INT, DINT, или UINT

Определение функциональных блоков типов (FFB) для отказоустойчивых конфигураций

В таблице ниже приведен перечень функциональных блоков (FFB), принадлежащих к семейству функций для отказоустойчивых конфигураций:

Наименование	Тип	Применяется для...
S_DISIL2	EFB	выбора данных из двух модулей цифрового ввода, если модули ввода резервированные
S_AISIL2	EFB	выбора данных из двух модулей аналогового ввода, если модули ввода резервированные

Определение функциональных блоков (FFB) для конфигураций с горячим резервом

В таблице ниже приведен перечень функциональных блоков (FFB), принадлежащих к семейству функций для конфигураций с горячим резервированием:

Наименование	Тип	Применяется для...
S_HSBY_SWAP	EFB	переключением между основным и резервным ЦПУ при использовании конфигурации с горячим резервом

Подробнее об использовании функциональных блоков (FFB) в проекте безопасности см. в *библиотеке блоков Unity Pro, предназначенных для применения в проектах безопасности.*

Пароль проекта

Защита паролем

Вам потребуется вводить пароль проекта в следующих случаях:
- при открытии существующего проекта безопасности
- при изменении пароля проекта
- при открытии пароля проекта
- при подключении к контроллеру безопасности
- при превышении заданного времени бездействия и после включения функции автоблокировки

Подробное описание защиты паролем см. в главе "Свойства проекта и пароль в инструментальной системе Unity Pro XLS" в руководстве на инструментальную систему Unity Pro XLS, Особенности режима работы.

Примечание: Из соображений безопасности и для защиты проекта от несанкционированного доступа компания настоятельно рекомендует сменить пароль по умолчанию на собственный сразу же после выбора модуля ЦП безопасности Quantum. Если вы не смените пароль по умолчанию, пустой пароль сохранится даже после сохранения и закрытия вашего проекта. При повторном открытии проекта просто щелкните мышкой на **OK**, оставив поле ввода пароля пустым. Смените пароль как можно скорее.

Если вы забыли пароль проекта

Подробное описание действий, которые необходимо выполнить, если вы забыли пароль проекта, см. в главе "Если вы забыли пароль" в руководстве на *инструментальную систему Unity Pro XLS, Особенности режима работы*.

3.3 Рабочие режимы

Начальные сведения

Введение

В данном параграфе приводится описание рабочих режимов контроллера безопасности Quantum, в частности подробно рассмотрены два режима.

Что в этом параграфе?

В этом параграфе содержатся следующие темы:

Рабочие режимы контроллера безопасности

Введение

По умолчанию контроллер безопасности Quantum выполняют функции безопасности, таким образом обеспечивая безопасное выполнение контролируемого процесса. При этом вы также должны иметь возможность выполнить отладку или внести изменения в свой проект.

Поэтому контроллер безопасности Quantum поддерживает два рабочих режима:
- Безопасный режим
- Служебный режим

В Безопасном режиме контроллер управляет вашим процессом, а в Служебном режиме можно при необходимости выполнить отладку или скорректировать проект.

Особенности служебного и безопасного режимов

Рабочий режим контроллера безопасности Quantum зависит от таких событий, как исключения в проекте, включения и выключения питания и так далее. Функции, предусмотренные в инструментальной системе Unity Pro XLS, зависят от рабочего режима контроллера.

Переключение между режимами выполняется при определенных условиях и в соответствии с установленными процедурами. Подробнее см. главу "Переключение между Безопасным и Служебным режимами" в руководстве на *инструментальную систему Unity Pro XLS, Особенности режима работы.*

Вы можете воздействовать на контроллер безопасности при помощи:
- инструментальной системы Unity Pro XLS
- клавиатуры модуля ЦП безопасности Quantum
- ключа

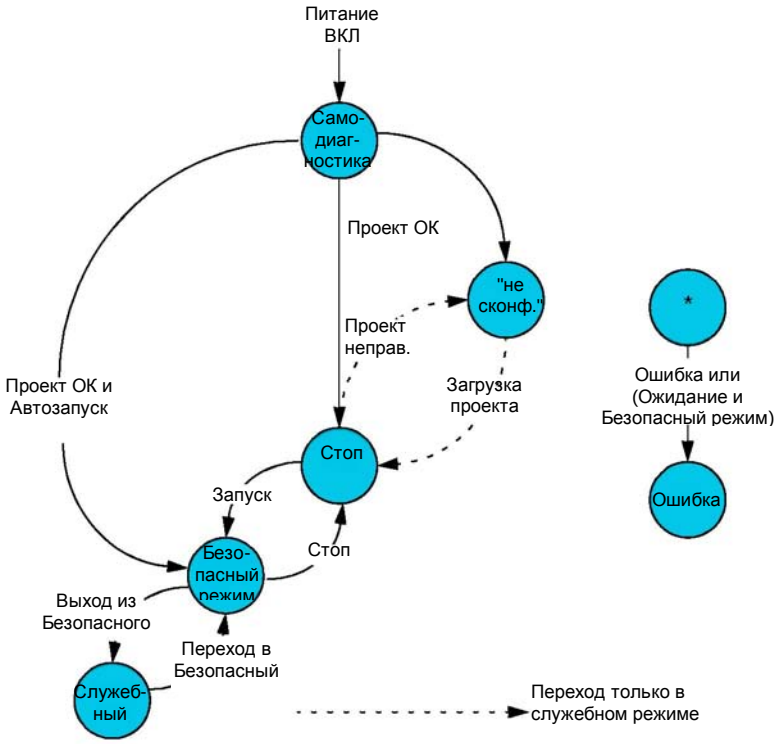
В зависимости от рабочего режима контроллер безопасности может находиться в разных состояниях.

При включении питания контроллер автоматически переходит в Безопасный режим, но только в случае выполнения двух условий:
- Проект нормальный
- Опция автозапуска **Automatic start in Run** включена.

Если проект неправильный (содержит ошибки), контроллер перейдет в состояние "не сконфигурирован" в Служебном режиме (только в том случае, если ключ открыт). В данном состоянии контроллера вы сможете загрузить проект.

При возникновении ошибки контроллер переходит в
- состояние ожидания, если работает в Служебном режиме.
- состояние неисправности, если работает в Безопасном режиме.

На рисунке ниже приведена схема состояний контроллера безопасности Quantum:



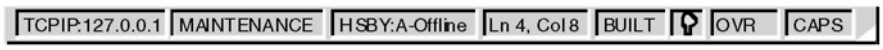
Идентификация рабочего режима

Отличить один режим от другого можно

- на ЖК-дисплее ЦПУ или
- в строке состояния в окне ПЛК в инструментальной системе Unity Pro XLS.

ЖК-дисплей ЦПУ выводит индикацию текущего рабочего режима в виде букв *M* (Служебный режим) и *S (*Безопасный режим).

В строке состояния окна ПЛК индикация текущего режима выводится так, как показано на рисунке ниже:



Безопасный режим

Определение безопасного режима

Безопасный режим - это режим по умолчанию контроллера безопасности Quantum. Безопасный режим имеет некоторые ограничения, в частности отсутствует возможность внесения изменений и запрещены работы, связанные с обслуживанием контроллера.

Ограничения в Безопасном режиме

Если контроллер работает в Безопасном режиме, в инструментальной системе Unity Pro XLS запрещены следующие действия:

- Запрещены изменения загрузки.
- Запрещена настройка и фиксация переменных безопасности и вводов/выводов безопасности
- Запрещена отладка с точками остановки, точками просмотра и в один этап
- Таблицы анимации и диспетчерские окна не могут записывать переменные безопасности и вводы/выводы безопасности.
- Раздел безопасной памяти имеет защиту от записи; а это значит, что человеко-машинный интерфейс (ЧМИ) и другие контроллеры не могут записывать в него данные. Данное условие находится под контролем контроллера безопасности, см. также *Раздел памяти, стр. 105.*

Примечание: Логические анимации, таблицы анимаций и диспетчерские окна могут влиять на время опроса.

Примечание: При помощи OSLoader можно загрузить новую версию прошивки процессорного модуля Ethernet в модуль ЦП безопасности Quantum. Однако это можно сделать только в Служебном режиме.

ПРЕДУПРЕЖДЕНИЕ

ВОЗМОЖНАЯ УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ

Не загружайте новую версию прошивки процессорного модуля Ethernet в модуль ЦП безопасности Quantum в Безопасном режиме. Это можно сделать, но не рекомендуется.

Несоблюдение этих инструкций может привести к серьезным травмам или повреждению оборудования.

Состояния безопасного режима

Переключившись в Безопасный режим, контроллер может находиться в рабочем состоянии или в состоянии неисправности. Если контроллер в рабочем состоянии, то действуют все наложенные ограничения и выполняется сравнительный анализ результатов выполнения двойного кода пользователя. Если проверка выявляет ошибку, контроллер переходит в состояние неисправности, потому что не имеет возможности ее устранить.

Вход в Безопасный режим

Существует 4 способа входа в Безопасный режим:
- при включении питания контроллера безопасности
- при переходе в Безопасный режим из Служебного режима
- при блокировке ключа
- при отсоединении инструментальной системы Unity Pro XLS либо в результате действий Пользователя, либо вследствие обрыва соединения

При включении питания контроллер безопасности автоматически переходит в Безопасный режим.

Примечание: После включения питания и при условии наличия правильного проекта контроллер выполняет холодный пуск.

Таким образом, происходит повторная инициализация проекта и система выполняет:
- инициализацию данных с использованием исходных значений, заданных в проекте
- инициализацию элементарных функциональных блоков (EFBs) на основании исходных данных
- инициализацию данных, объявленных в элементарных функциональных блоках (EFB)
- инициализацию системных битов и слов
- отмену любой функции фиксирования, см. также *Функция фиксирования, стр. 94*

Переключиться из Служебного режима в Безопасный режим можно, только если контроллер не находится в состоянии отладки проекта.

Примечание: Данные, которые были сделаны фиксированными до переключения в Безопасный режим, останутся такими же и после переключения, см. также *Функция фиксирования, стр. 94*.

Более подробные сведения о переключении из Служебного режима в Безопасный режим можно найти в главе "Переключение между Безопасным и Служебный режимами" в руководстве на *инструментальную систему Unity Pro XLS, Особенности режима работы*.

Опция Automatic Start in Run

При необходимости можно сделать так, что проект будет автоматически запускаться в Безопасном режиме при включении питания. Для этого надо включить опцию автоматического запуска при включении питания **Automatic start in Run**, см. также главу "Конфигурация процессорных модулей Quantum" в руководстве на *инструментальную систему Unity Pro, Режимы работы*. Однако, компания рекомендует использовать для запуска проекта команду **Run** вместо опции **Automatic start in Run**.

ВНИМАНИЕ

НЕПРЕДНАМЕРЕННЫЕ ОТКЛОНЕНИЯ В РАБОТЕ ОБОРУДОВАНИЯ

Используйте опцию **Automatic start in Run** только в редких случаях. При использовании данной опции вам придется запрограммировать и настроить систему таким образом, чтобы она нормально работала после перезапуска.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Служебный режим

Определение Служебного режима

Служебный режим контроллера безопасности Quantum - это временный режим, предусмотренный для изменения и отладки проекта.

Особенности Служебного режима

Если контроллер работает в Служебном режиме, в инструментальной системе Unity Pro XLS запрещены следующие действия:

- Запрещены изменения загрузки.
- Запрещена настройка и фиксация переменных безопасности и вводов/выводов безопасности. Тем не менее, переменные типа EB00L можно делать фиксированными.
- Можно переключиться в Безопасный режим пока включения функция фиксирования. Фиксированные переменные останутся фиксированными, см. также *Функция фиксирования, стр. 94.*
- Запрещена отладка с точками остановки, точками просмотра и в один этап. Тем не менее, контроллер должен находиться в работающем состоянии.
- Таблицы анимации и диспетчерские окна могут записывать переменные безопасности и вводы/выводы безопасности.
- Раздел безопасной памяти имеет защиту от записи; это означает, что ЧМИ и другие контроллеру не имеют права записи в него. Данное условие находится под контролем контроллера безопасности, см. также *Раздел памяти, стр. 105.*

Вход в Служебный режим

Вы можете войти в Служебный режим только из Безопасного режима, потому что при включении питания контроллер автоматически включается в Безопасном режиме. Чтобы выйти из Безопасного режима и войти в Служебный режим, необходимо разблокировать ключ. Подробное описание переключения между режимами см. в главе "Переключение между Безопасным и Служебным режимами" в руководстве на *инструментальную систему Unity Pro XLS, Особенности режима работы*.

Состояния служебного режима

В Служебном режиме контроллер может находиться в работающем состоянии, или состоянии ожидания. Когда контроллер находится в работающем состоянии, можно вносить изменения в проект. Далее, вы можете переключиться в Режим отладки, если необходимо отладить или изменить программу. В работающем состоянии контроллера двойной код выполняется, но результат сравнительного анализа игнорируется.

	**ОПАСНО**
	ОПАСНОСТЬ УТРАТЫ ФУНКЦИИ БЕЗОПАСНОСТИ ВО ВРЕМЯ ПУСКО-НАЛАДОЧНЫХ РАБОТ И ОБСЛУЖИВАНИЯ При внесении изменений в работающую систему всегда соблюдайте требования, установленные в стандарте IEC 61508. **Несоблюдение этих инструкций может привести к смертельному исходу или серьезным травмам.**

Функция фиксирования

Введение

Функция фиксирования работает только в Служебном режиме. Тем не менее, можно переключиться из Служебного режима в Безопасный режим, и фиксированные данные при этом останутся фиксированными.

Примечание: См. последнюю версию документа *Maintenance Override* организации TÜV, где приведены правила, которые необходимо соблюдать при использовании функции фиксирования в системе безопасности. Данный документ можно скачать с сайта TÜV Rheinland Group *http://www.tuvasi.com/*.

	ОПАСНО
	**УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ** Убедитесь в том, что функция фиксирования носит временный характер, и логика пользователя контролирует состояние функции фиксирования (слово %SW108, см. *Определение системных слов от %SW60 до %SW127, стр. 162*). **Несоблюдение этих инструкций может привести к смертельному исходу или серьезным травмам.**

Обработка фиксированных данных

Поскольку фиксированные данные останутся фиксированными, инструментальная система Unity Pro XLS предупреждает пользователя об этом перед выполнением команды переключения.

Примечание: При потере соединения между контроллером и инструментальной системой Unity Pro XLS последняя также выдает пользователю предупреждение об имеющихся фиксированных данных независимо от рабочего режима контроллера. Данный факт обусловлен тем, что контроллер автоматически переключается в Безопасный режим при потере соединения с Unity Pro XLS в результате действия пользователя или ошибки связи.

ВНИМАНИЕ

ОПАСНОСТЬ ОБРАБОТКИ ФИКСИРОВАННЫХ ДАННЫХ

Проверьте состояние данных перед переключением из Служебного режима в Безопасный режим. Фиксированные данные останутся фиксированными, а контроллер постарается их обработать. Проверьте, что контроллер будет обрабатывать правильные нефиксированные данные перед выполнением функций безопасности.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Можно проверить состояние функции фиксирования в системном слове %SW108. В данном слове содержится количество фиксированных битов модуля ввода/вывода. Значение системного слова увеличивается при каждом применении фиксирования и уменьшается, соответственно, при каждой отмене фиксирования.

3.4 Специальные функции и процедуры

Начальные сведения

Введение

В данном параграфе приводится описание специальных функций и процедур с использованием инструментальной системы Unity Pro XLS для программирования проектов безопасности.

Что в этом параграфе?

В этом параграфе имеются следующие темы:

Проверка среды программирования

Введение

Инструментальная система Unity Pro XLS предоставляет возможность выполнения самодиагностики для проверки правильности версий текущих используемых компонентов, а также выявления возможных ошибок, например, неисправности жесткого диска. Самодиагностика выполняется на основании анализа функции CRC.

Описание самодиагностики

Во время самодиагностики инструментальная система Unity Pro XLS выполняет проверку версии и CRC
- библиотек DLL инструментальной системы Unity Pro XLS,
- базы данных библиотеки FFB, и
- базы данных каталога аппаратных средств

ВНИМАНИЕ

ОПАСНОСТЬ ПОВРЕЖДЕНИЯ ПРОГРАММЫ

Функцию самодиагностики инструментальной системы Unity Pro XLS следует запускать регулярно для проверки целостности вашей программы. Как минимум, самодиагностику необходимо выполнять
- после установки или удаления любого программного обеспечения с вашего компьютера
- перед загрузкой рабочей программы в ПЛК безопасности.
- перед измерением программы в работающем ПЛК безопасности.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Подробное описание правил запуска самодиагностики см. в главе "Самодиагностика в инструментальной системе Unity Pro XLS", руководство на *инструментальную систему Unity Pro XLS, Рабочие режимы.*

Включение ПЛК безопасности Quantum

Предварительные условия

Перед запуском контроллера безопасности Quantum необходимо, чтобы
- ваша система безопасности была правильно сконфигурирована,
- программирование вашего проекта безопасности было выполнено правильно,
- проверка целостности вашего проекта безопасности и инструментальной системы Unity Pro XLS была выполнена,
- инструментальная система Unity Pro XLS была подсоединена к ПЛК безопасности, и
- ваш проект безопасности был загружен в ПЛК безопасности.

Включение ПЛК безопасности Quantum

Если контроллер безопасности Quantum содержит правильный проект, он выполняет только холодный пуск. Поэтому вы можете запустить проект безопасности только при помощи холодного пуска. Исключением является ситуация, если вы только загрузили проект в контроллер.

Таким образом, вы можете запустить свой проект, если контроллер находится в одном из следующих исходных состояний:
- ПЛК включен, а проект безопасности загружен после подачи питания.
- ПЛК выключен.

Далее, инструментальная система Unity Pro XLS поддерживает опцию **Automatic start in Run**. Если эта опция выбрана, контроллер автоматически запускается в Безопасном режиме после включения питания. Однако обращаем ваше внимание на то, что компания не рекомендует включать данную опцию.

ВНИМАНИЕ

НЕПРЕДНАМЕРЕННЫЕ ОТКЛОНЕНИЯ В РАБОТЕ ОБОРУДОВАНИЯ

Используйте опцию **Automatic start in Run** только в редких случаях. При использовании данной опции вам придется запрограммировать и настроить систему таким образом, чтобы она нормально работала после перезапуска.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Подробное описание методик запуска проекта безопасности см. в главе "Запуск и остановка проекта безопасности" в руководстве на *инструментальную систему Unity Pro XLS, Рабочие режимы*.

Метка версии

Описание метки версии

В инструментальной системе Unity Pro XLS каждый сгенерированный двоичный файл проекта безопасности имеет метку версии (version stamp), где указана дата и время создания. Таким образом, вы можете проверить, изменялся ли ваш проект, и когда он изменялся.

Подробное описание процедуры проверки версии проекта см. в главе "Свойства проекта инструментальной системы Unity Pro XLS" в руководстве на *инструментальную систему Unity Pro XLS, Рабочий режим*.

Выгрузка

Выгрузка проекта безопасности

Проекты безопасности также можно выгружать из контроллера в инструментальную систему Unity Pro XLS. Для выгрузки проекта вам потребуется включить данную опцию в свойствах проекта. Для подключения к контроллеру вам потребуется пароль для проекта безопасности. Кроме этого, для выгрузки проекта необходимо переключить контроллер в служебный режим. Подробнее см. главу Свойства проекта" в руководстве на *инструментальную систему Unity Pro, Рабочие режимы*

Создание резервных копий проектов

Введение

Инструментальная система Unity Pro XLS может выполнять проверку целостности вашего проекта безопасности. Данная проверка выполняется на основании вычисления CRC при закрытии или открытии проекта. Если значение CRC изменилось, значит, ваш проект поврежден или испорчен. В этом случае сравнительный анализ обоих значений завершается с отрицательным результатом и инструментальная система Unity Pro XLS не сможет открыть ваш проект. В результате, вы не сможете установить связь между инструментальной системой Unity Pro XLS и контроллером безопасности, и, следовательно, не сможете изменить или восстановить поврежденный проект.

Описание создания резервных копий

Кроме выгрузки проекта из контроллера (см. *Выгрузка, стр. 100*), единственным способом получить доступ к вашему проекту - это наличие копии его оригинальной версии, другими словами, резервной копии проекта. При помощи резервной копии вы сможете восстановить данные проекта

ВНИМАНИЕ

УТРАТА СПОСОБНОСТИ ВЫПОЛНЯТЬ ФУНКЦИИ БЕЗОПАСНОСТИ

Регулярно создавайте резервные копии проекта безопасности. В случае повреждения проекта вы не сможете открыть его, изменить или восстановить без резервной копии.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Рекомендации по созданию резервных копий

Немаловажное значение при создании резервных копий играет правильное планирование работы, а также

- программное обеспечение для создания резервных копий.
  Функция автоматического создания резервных копий не зависит от человеческого фактора в отличие от создания резервных копий вручную.
- процедура создания резервных копий.
  Создание более одной резервной копии и хранение копий в другом месте существенно увеличивает вероятность успешного восстановления данных.
- тип резервной копии.
  Как правило, в зависимости от данных, содержащихся в резервной копии, постепенной (т.е. инкрементной) или дифференциальной
- периодичность создания резервной копии.
  Вероятность успешного восстановления данных зависит от регулярности создания резервных копий.
- тип носителя, где хранится резервная копия.
  Несмотря на то, что хранение резервных копий на жестком диске более практично, лучше хранить их в другом месте.

Рекомендации по восстановлению данных

Использование резервной копии будет эффективным только при соблюдении правильной методики восстановления данных. Поэтому важно не только иметь резервные копии данных, но и располагать соответствующим программным обеспечением, необходимым для их чтения.

Примечание: Методика создания резервных копий подбирается наиболее оптимальной для вашей системы безопасности. Создавайте подходящее количество резервных копий соответствующего типа. Чаще пробуйте восстанавливать оригинальный проект из резервных копий, чтобы быть уверенным, что все в норме.

Неисправности

Введение

Если при проведении внутренней самодиагностики или проверке системы обнаруживается неисправность или ошибка, поведение контроллера безопасности Quantum будет зависеть от режима, в котором он работает.

Поведение в Безопасном режиме

Если контроллер работает в безопасном режиме, то при обнаружении единичной неисправности он переходит в состояние неисправности, потому что не имеет возможности восстановиться. Состояние неисправности блокируется на аппаратном уровне. Ваш проект останавливается, и вы не имеете возможности вмешаться или установить с ним связь.

Выход из состояния неисправности

Единственным способом выхода из состояния неисправности является повторный пуск контроллера, после он выполнит самодиагностику и инициализацию вашего проекта.

Если ваш проект ...	**Тогда, контроллер...**
правильный	переходит в состояние Остановки, что он вынужден сделать принудительным образом в связи с обнаруженной неисправностью
неправильный	переходит в состояние "не сконфигурирован".

В зависимости от состояния, в котором находится контроллер, выполните следующие действия:

Если ваш проект ...	**то ...**
остановлен, и опция автозапуска включена,	• либо снова включение питание контроллера • либо выполните команду **Run**.
остановлен, и опция автозапуска выключена,	выполните команду **Run**.
в состоянии "не сконфигурирован"	загрузите резервную копию проекта.

Поведение в Служебном режиме

Если контроллер работает в Служебном режиме, он переходит
- в состояние ожидания при обнаружении ошибки во время диагностики.
- в состояние неисправности при включении аппаратного таймера "watchdog".

Когда контроллер пребывает в состоянии ожидания, вы все равно можете установить с ним связь и выполнить отладку проекта. При помощи команды **Init** или путем загрузки проекта вы можете остановить контроллер, а затем повторно запустить. Когда контроллер находится в состоянии неисправности, он ведет себя таким же образом, как было описано в *Поведение в Безопасном режиме.*

3.5 Связь

Начальные сведения

Введение

В данном параграфе приводится описание коммуникации между контроллером безопасности Quantum и инструментальной системой Unity Pro XLS, а также другими устройствами.

Что в этом параграфе?

В этом параграфе имеются следующие темы:

Раздел памяти

Введение

В Безопасном режиме Модуль ЦП безопасности блокирует любые попытки записи в следующие разделы памяти:
- %M или %Q (регистр 0x)
- %MW или %QW (регистр 4x)
- данные EFB

Тем не менее, поскольку у вас может возникнуть необходимость записать данные в контроллер безопасности, память разделена на безопасную область и свободную область, таким образом, вы можете записывать данные в %M и %MW.

Описание безопасной памяти

Раздел безопасной памяти имеет защиту от записи и не позволяют ни одному устройству записывать туда данные.

Примечание: Управление правом доступа для записи осуществляется внутри ЦПУ, поскольку некоторые процедуры обмена данными, например с ЧМИ или другими контроллерами (безопасности или обычными) не настроены в контроллере безопасности при помощи инструментальной системы Unity Pro XLS, и поэтому не могут быть проверены в конфигурации Unity Pro XLS.

Описание защиты от записи

Для предотвращения записи в безопасную область памяти другими устройствами, предусмотрен механизм блокировки. Контроллер не будет выполнять ни одну команду записи и вернет код ошибки.

Описание раздела свободной памяти

Раздел свободной памяти (UMA) представляет собой специальный выделенный раздел памяти для битов и слов, который не имеет защиты от записи. Данный раздел имеет следующие характеристики:
- он расположен в начале всего раздела памяти.
- его размер можно выбрать в инструментальной системе Unity Pro XLS.
- данные из него нельзя использовать напрямую, а только при помощи специальных функциональных блоков.

Конфигурирование раздела свободной памяти

При помощи инструментальной системы Unity Pro XLS вы можете выбрать размер свободной памяти в конфигурации ЦПУ с учетом следующих ограничений:

- в %MW, пределом является
  - последнее слово в свободном разделе памяти или
  - 0, если данный раздел не используется.
- в %M пределом является
  - а кратное 16 и последнее %M в свободном разделе или
  - 0, если данный раздел не используется.

Примечание: Сначала сконфигурируйте свободный раздел памяти достаточно большого объема. Если этот раздел памяти понадобится изменить позднее, все адреса надо будет изменить.

ПРЕДУПРЕЖДЕНИЕ

ОПАСНОСТЬ ПОВРЕЖДЕНИЯ ПРОЕКТА

Убедитесь, что размер раздела свободной памяти правильно сохранен в модуле ЦП безопасности Quantum после загрузки приложения контроллера. Для этого вам необходимо считать системные слова %SW110 и %SW111 (например, при помощи таблицы анимации) и сравнить их с заданными значениями в вашем приложении.

Несоблюдение этих инструкций может привести к серьезным травмам или повреждению оборудования.

Использование данных из раздела свободной памяти

Для выполнения функций безопасности вы можете только обрабатывать данные, сохраненные в разделе памяти. Если необходимо получить доступ к функциям безопасности, вы можете использовать данные из раздела свободной памяти. Однако из соображений безопасности вы не сможете обработать их непосредственным образом. Вам придется перенести данные из раздела свободной памяти в раздел безопасной памяти, чтобы функции безопасности смогли использовать эти данные.

Подробное описание процедуры переноса данных из раздела свободной памяти в раздел безопасной памяти см. в главе "Использование данных из раздела свободной памяти" в руководстве на *инструментальную систему Unity Pro XLS, Рабочий режим*.

Описание функциональных блоков для безопасного переноса данных

Поскольку вы не можете непосредственно работать со значениями, хранящимися в разделе свободной памяти, существует два функциональных блока, которые служат для переноса данных из раздела свободной памяти в раздел безопасной памяти:

- S_MOVE_BIT для получения доступа к битам
- S_MOVE_WORD для получения доступа к словам

Переменные из раздела свободной памяти связаны с входным значением функционального блока, а его выходное значения связано с переменной безопасности. Прямые адреса использовать нельзя, потому что они воспринимаются как целые (int).СЛОВО, которое надо перенести, выбирается в разделе свободной памяти. Если фактическое значение лежит вне предела, выходному значению присваивается 0 и формируется ошибка. Дополнительные входные значения применяются для контроля правильности переноса данных функциональными блоками в выходные значения в случае, когда некоторые данные могут быть использованы только вместе в одном цикле.

Примечание: Рекомендуется давать переменным из раздела свободной памяти удобные имена и снабжать их комментариями. Это упростит проверку вашего проекта безопасности.

Описание защиты от записи

На основании времени редактирования и времени создания инструментальная система Unity Pro XLS проверяет, что используются только переменные из раздела свободной памяти в качестве входных значений функциональных блоков MOVE. кроме этого, инструментальная система Unity Pro XLS поддерживает функцию перекрестных ссылок для поиска правила применения переменной.

ВНИМАНИЕ

ОПАСНОСТЬ ОБРАБОТКИ НЕВЕРНЫХ ДАННЫХ

Убедитесь, что данные, которые переносятся в раздел безопасной памяти, являются верными. Когда данные переносятся в раздел безопасной памяти при помощи функциональных блоков MOVE, нельзя считать, что это автоматически означает, что данные верны. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Чтобы убедиться, что перенос данных выполнен правильно, можно дважды записать данные (в 2 разные переменные) и сравнить их.

Связь между ПК и контроллерами

Введение

Если программирование вашего проекта безопасности успешно завершено, вы можете загрузить его, запустить или отредактировать, подключившись из инструментальной системы Unity Pro XLS к контроллеру безопасности Quantum. Чтобы установить связь между контроллером и программой вам потребуется подключить инструментальную систему Unity Pro XLS через:

- Modbus TCP (либо с ЦПУ, либо модуль NOE)
- сеть Modbus Plus
- интерфейс Modbus RS232 / RS485
- интерфейс USB

Связь между инструментальной системой Unity Pro XLS и контроллером безопасности Quantum не является частью контура безопасности, но, несмотря на это, требует проверки. В частности, для проверки правильности переноса данных и отсутствия ошибок связи во время загрузки проекта применяется функция контроля CRC. Тем не менее, вам следует также дополнительно проверить версию проекта и его работоспособность, а также среду Unity Pro XLS.

Для прокладки сети Ethernet применяются стандартные устройства Ethernet .

Связь между контроллерами

Введение

Когда речь идет о контроллере безопасности, то можно осуществлять запись только в другие контроллеры. Считывание данных из других контроллеров можно выполнять только из свободного раздела памяти, см. также *Раздел памяти, стр. 105*.

Примечание: Управление правом доступа для записи осуществляется внутри ЦПУ, поскольку некоторые процедуры обмена данными, например с ЧМИ или другими контроллерами безопасности или обычными, не настроены в контроллере безопасности при помощи инструментальной системы Unity Pro XLS, и поэтому не могут быть проверены в конфигурации Unity Pro XLS.

Контроллер безопасности Quantum может связываться с другими контроллерами через:

- Modbus TCP (либо с ЦПУ, либо модуль NOE)
- сеть Modbus Plus
- интерфейс Modbus RS232 / RS485

Данные виды соединений относятся к тем, которые не влияют не уровень безопасности.

Примечание: Соединение с контроллером безопасности Quantum по сети Modbus, чтобы он при этом выступал в роли ведущего устройства (Modbus Master) невозможно, потому что необходимые для этого функциональные блоки не имеют сертификаты для применения в проектах безопасности. Тем не менее, контроллер безопасности может выступать в роли ведомого (Modbus slave) и связываться/обмениваться данными с другими контроллерами и даже принимать данные в раздел свободной памяти.

Описание соединения по Ethernet

Кабель сети Ethernet подсоединяется

- либо к порту Ethernet на модуле ЦПУ
- либо к модулю Ethernet 140 NOE 771 11.

Примечание: У резервируемого модуля безопасности ЦПУ порт Ethernet применяется для обмена данными между основным и резервным ЦПУ, и поэтому не может использоваться для соединения с другими контроллерами или ЧМИ.

Модуль Ethernet 140 NOE 771 11 имеет сертификат соответствия для применения в качестве модуля, не влияющего на уровень безопасности, в контроллерах безопасности Quantum. Соединение может устанавливаться как пиринговым (peer-to-peer), так и глобальным (global data).

Для прокладки сети Ethernet применяются стандартные устройства Ethernet .

Настройка пирингового соединения в сети Ethernet	Пиринговое соединение настраивается в инструментальной системе Unity Pro XLS в разделе настройки сети Ethernet независимо для чтения и записи. Инструментальная система Unity Pro XLS проверяет, что при чтении используется только раздел свободной памяти. Если данное требование нарушается, система формирует ошибку и не генерирует код.
Настройка глобального соединения данных в сети Ethernet	Глобальное соединение настраивается в инструментальной системе Unity Pro XLS в разделе настроек сети Ethernet для публикации данные для записи и подписки на данные для чтения. Поскольку считывание разрешено только из раздела свободной памяти, инструментальная система Unity Pro XLS проверяет соответствие данному требованию, и выдает ошибку, если оно нарушается.
Описание соединения по сети Modbus Plus	Модуль Modbus Plus 140 NOM 2XX 00 нельзя использовать для соединения. Вместо него разрешается использовать только сетевой порт Modbus Plus модуля ЦПУ. В сети Modbus Plus можно установить как пиринговое соединение, так и соединение глобальных данных.
Настройка пирингового соединения в сети Modbus Plus	Пиринговое соединение настраивается в инструментальной системе Unity Pro XLS в разделе настройки сети Modbus Plus независимо для чтения и записи. Инструментальная система Unity Pro XLS проверяет, что при чтении используется только раздел свободной памяти. Если данное требование нарушается, система формирует ошибку и не генерирует код.
Настройка глобального соединения данных в сети Modbus Plus	Соединение глобальных данных настраивается в инструментальной системе Unity Pro XLS в разделе настройки сети Modbus Plus независимо для чтения и записи. Инструментальная система Unity Pro XLS проверяет, что при чтении используется только раздел свободной памяти. Если данное требование нарушается, система формирует ошибку и не генерирует код.

	**ВНИМАНИЕ** **СКРЫТАЯ УТЕРЯ ДАННЫХ** Следует помнить, что модуль ЦП безопасности Quantum управляет правами доступа на запись в самого себя. Хотя вы можете попытаться записать данные с внешнего устройства в контроллер безопасности Quantum через Ethernet, эти данные будут проигнорированы, потому что контроллер безопасности имеет защиту от записи. Если, например, используется соединение глобальных данных, данные могут быть утеряны, а вы не узнаете об этом. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Связь между контроллером и ЧМИ

Введение

Интерфейс ЧМИ используется для считывания данных из контроллера безопасности. Однако можно осуществлять запись в раздел свободной памяти контроллера, см. также *Раздел памяти, стр. 105.* Контроллер безопасности Quantum может связываться с другими ЧМИ через:

- Modbus TCP (либо с ЦПУ, либо модуль NOE)
- сеть Modbus Plus
- интерфейс Modbus RS232 / RS485

Соединение между контроллером и ЧМИ не настраивается в инструментальной системе Unity Pro XLS. Поэтому соединением нельзя управлять из программы и модуль безопасности ЦП Quantum сам обеспечивает защиту от записи с ЧМИ.

Описание защиты от записи

Раздел безопасной памяти контроллера безопасности имеет защиту от записи, и вы не можете писать туда данные. При попытке записи контроллер просто не выполнит команду записи, см. также *Описание защиты от записи, стр. 105*.

Запись в Служебном Режиме

Даже в Служебном режиме существует защита от записи раздела безопасной памяти для контроллеров и ЧМИ. Но в инструментальной системе Unity Pro XLS вы можете изменять и настраивать данные.

В программе Unity Pro XLS вы можете

- изменять логику.
- вводить значения
- фиксировать значения
- выполнять отладку

При помощи сервера OFS Schneider OPC можно изменять данные в разделе безопасной памяти в Служебном режиме.

	ВНИМАНИЕ
	**ОПАСНОСТЬ ОБРАБОТКИ ФИКСИРОВАННЫХ ДАННЫХ** Если вы собираетесь изменять данные в Служебном режиме, см. последнюю версию документа TÜV *Maintenance Override*. Данный документ можно скачать с сайта TÜV Rheinland Group *http://www.tuvasi.com/*. **Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.**

Контрольные проверки

4

Начальные сведения

Введение

В отношении системы, выполняющей функции безопасности, необходимо соблюдать требования безопасности при проведении работ по установке, настройке, программированию, вводу в эксплуатацию и эксплуатации в соответствии со стандартом IEC 61508. Для обеспечения соответствия требованиям безопасности компания рекомендует применять контрольные проверки, приведенные ниже в технологических картах. Следует помнить, что перечень данных контрольных проверок не является исчерпывающим, и вы, в любом случае, обязаны соблюдать все требования безопасности, установленные в стандарте IEC 61508 и данном руководстве.

Что в этой главе?

В этой главе содержатся следующие темы:

Контрольные проверки настройки системы безопасности

Введение

Примечание: Следует помнить, что перечень данных контрольных проверок не является исчерпывающим, и вы, в любом случае, обязаны соблюдать все требования безопасности, установленные в стандарте IEC 61508 и данном руководстве.

Контрольные проверки

Компания рекомендует выполнять данные контрольные проверки конфигурации вашей системы безопасности:

Проверки	**Ссылка на данное руководство**	**Выполнено**	**Примечания**
Проверить значения коэффициентов PFD/PFH для всего контура безопасности.	*Сертификаты безопасности, стр. 17*	£	
Соблюдайте все правила, приведенные в следующих справочниках: • *Quantum и Unity Pro, Справочник по аппаратным средствам* • *Модули аналогового и дискретного ввода/вывода Quantum, Справочник* • *Заземление и электромагнитная совместимость ПЛК, Руководство пользователя* • *Кабели для удаленного ввода/вывода Modicon, Руководство по проектированию и монтажу* • *Горячее резервирование* для *Quantum, Руководство пользователя* • *Архитектура соединений ПЛК Quantum и Premium, Справочник* • *Сеть Modbus Plus, Руководство по проектированию и монтажу* • *Конфигурация TCPIP/IP Quantum TCPIP/IP, Руководство пользователя* • *Модули Ethernet 140 NOE 771 xx, Руководство пользователя*		£	
Проверить всю комплектацию и провода при вводе в эксплуатацию.		£	
Применять только сертифицированные модули безопасности и модули, не влияющие на уровень безопасности.	*Сертификаты безопасности, стр. 17*	£	
Применять модули только с сертифицированным "вшитым" программным обеспечением. Для проверки версии "вшитого" программного обеспечения модулей ЦПУ, CRP/CRA и NOE, а также процессорных модулей ЦПУ Ethernet и резервируемых ЦПУ используйте OSloader. Версия прошивки модулей вводов/выводов безопасности указана на шильдике, размещенном на корпусе.	*Сертификаты безопасности, стр. 17*	£	
Введите правильное значение максимального времени опроса в соответствии с процессом	*Требования к мониторингу, стр. 73*, *Ограничения в Безопасном режиме, стр. 91*, *Безопасная продолжительность процесса, стр. 74*	£	
Используйте пароль для защиты проекта безопасности от несанкционированного доступа.	*Пароль, стр. 86*	£	

Проверки	Ссылка на данное руководство	Выполнено	Примечания
Используйте только отказоустойчивые модули удаленного ввода/вывода (140 CRP 932 00 и 140 CRA 932 00) с двумя кабелями.	*Описание адаптеров устройств удаленного ввода/вывода, стр. 55*, *Описание связи между ЦПУ и вводом/выводом, стр. 40*	£	
Защищайте источник питания модулей цифрового вывода предохранителем.	*Сведения о проводах, стр. 52*	£	
Для повышения отказоустойчивости системы ставьте по два модуля питания на каждое монтажное шасси и удаленное устройство. Для лучшего теплорассеяния устанавливайте модули питания на разных сторонах монтажного шасси или удаленного устройства.	*Модули питания для контроллеров безопасности Quantum, стр. 54*	£	
Проверьте, что один модуль питания в каждом монтажном шассе в состоянии обеспечить нормальное питание.	*Модули питания для контроллеров безопасности Quantum, стр. 54*	£	
Проверьте, что адреса всех модулей CRA введены правильно.	*Описание адаптеров устройств удаленного ввода/вывода, стр. 55*	£	
Запрещается записывать данные из других устройств (ПЛК, ЧМИ и др.) в раздел безопасной памяти.	*Связь, стр. 104*	£	
Запрещается загружать программное обеспечение (т.е. прошивку) в процессорный модуль Ethernet, когда контроллер работает в Безопасном режиме.	*Ограничения в Безопасном режиме, стр. 91*	£	

Контрольные проверки программирования проекта безопасности

Введение

Примечание: Следует помнить, что перечень данных контрольных проверок не является исчерпывающим, и вы, в любом случае, обязаны соблюдать все требования безопасности, установленные в стандарте IEC 61508 и данном руководстве.

Контрольные проверки

Компания рекомендует выполнять данные контрольные проверки правильного программирования вашей системы безопасности:

Проверки	**Ссылка на данное руководство**	**Выполнено**	**Примечания**
Регулярно проверяйте инструментальную систему Unity Pro XLS на целостность.	*Проверка среды программирования, стр. 97*	£	
Проверьте, что ваш проект правильный.	*Требования к программированию, стр. 29*	£	
Проверить всю логику при вводе в эксплуатацию.			
Правильно настройте %M и %MW.	*Раздел памяти, стр. 105*	£	
Правильно настройте максимальный размер области свободной памяти для %M и %MW.	*Описание максимальной продолжительности цикла ЦПУ, стр. 75*	£	
Проверьте правильность загрузки заданных максимальных областей UMA для %M и %MW (проверьте при помощи %SW110 и %SW111).	*Раздел памяти, стр. 105*	£	
Проверьте правильность применения данных, не имеющих отношения к безопасности, из раздела свободной памяти при помощи функциональных блоков S_SMOVE_***.	*Раздел памяти, стр. 105*	£	
Проверьте диапазон данных WORD из данных, не имеющих отношения к безопасности, из раздела свободной памяти при помощи функционального блока S_SMOVE_WORD.	*Раздел памяти, стр. 105*	£	
Запрещается условное исполнение областей логики безопасности.	*Требования к структуре программы, стр. 71*	£	
Запрещается использовать переходы к меткам внутри логики языка FBD и LD.	*Требования к элементам языка, стр. 72*	£	
Программируйте логику, не имеющую отношения к безопасности, для ввода/вывода, не влияющего на уровень безопасности, в разных областях.	*Номенклатура модулей, не влияющих на уровень безопасности, стр. 19*	£	
Присваивайте переменным, не имеющим отношения к безопасности, удобные имена и снабжайте их комментариями.	*Раздел памяти, стр. 105*	£	
Проверьте, что вводы и выводы модулей ввода/вывода, которые не влияют на уровень безопасности, используются для вычисления выводов безопасности.	*Описание модулей ввода/вывода, стр. 56*	£	

Проверки	Ссылка на данное руководство	Выполнено	Примечания
Не рекомендуется одновременно отслеживать большой объем данных в системе Unity Pro XLS (потому что увеличится время опроса).	*Требования к мониторингу, стр. 73*	£	
Включите все опции предупреждений во время анализа (находятся в настройках проекта). Проверьте, что все предупреждения не являются критическими, а поведение предсказуемое.	*Проверка программирования, стр. 73*	£	

Контрольные проверки модулей ввода/вывода

Введение

Примечание: Следует помнить, что перечень данных контрольных проверок не является исчерпывающим, и вы, в любом случае, обязаны соблюдать все требования безопасности, установленные в стандарте IEC 61508 и данном руководстве.

Контрольные проверки модулей ввода/вывода

Компания рекомендует выполнять данные контрольные проверки ваших модулей ввода/вывода:

Проверки	**Ссылка на данное руководство**	**Выполнено**	**Примечания**
Не используйте вводы/выводы Ethernet.	*Описание ограничений по модулям ввода/вывода, стр. 41*	£	
Не используйте вводы/выводы Modbus Plus.	*Описание ограничений по модулям ввода/вывода, стр. 41*	£	
Не используйте вводы/выводы, не влияющие на уровень безопасности, для функций безопасности.	*Описание модулей ввода/вывода, стр. 56*	£	
Для нормального срабатывания проводка цифровых вводов/выводов должны быть обесточена (состояние неисправности проводки должно быть аналогично обесточенному состоянию).	*Сведения о проводах, стр. 49*	£	
Применяйте правильные заземляющие приспособления для экранированных проводов аналоговых вводов.	*Сведения о проводах, стр. 47*	£	
Когда модули аналоговых вводов применяются для управления котлами, их необходимо контролировать на предмет замыкания на землю (утечка тока).	*Специальные требования к стандартным областям применения, стр. 127*	£	
Проверьте, что время ожидания, установленное для модулей вывода, подходит для подсоединенного устройства и контролируемого процесса.	*Описание времени ожидания, стр. 53*	£	
В резервируемой системе ввода/вывода используйте два канала ввода/вывода разных модулей, расположенных в разных устройствах удаленного ввода/вывода.	*Конфигурации с резервированием вводов/выводов для увеличения отказоустойчивости, стр. 65*	£	
Неиспользуемые входные каналы неиспользуемых модулей ввода следует закоротить.	*Сведения о проводах, стр.* 47, *Сведения о проводах, стр. 49*	£	
Соединительные провода между вводами/выводами модулей ввода/вывода и датчиками или пускателями должны быть подходящего размера/вида.	*Описание адаптеров устройств удаленного ввода/вывода, стр. 55*	£	

Проверки	Ссылка на данное руководство	Выполнено	Примечания
Проверьте, что все датчики и пускатели, которые подсоединены к модулям ввода/вывода, подходят по характеристикам для модулей ввода/вывода.	*Безопасная продолжительность процесса, стр. 74*	£	
Маркируйте модули безопасности красными этикетками для клеммных колодок, которыми комплектуются модули ввода/вывода безопасности.	*Общие сведения о модулях ввода/вывода безопасности, стр. 40*	£	

Контрольные проверки по эксплуатации, обслуживанию и ремонту

Введение

Примечание: Следует помнить, что перечень данных контрольных проверок не является исчерпывающим, и вы, в любом случае, обязаны соблюдать все требования безопасности, установленные в стандарте IEC 61508 и данном руководстве.

Контрольные проверки

Компания рекомендует выполнять следующие контрольные проверки при обслуживании или ремонте системы безопасности:

Проверки	**Ссылка на данное руководство**	**Выполнено**	**Примечания**
Установите стандартный порядок действий (SOP) при проведении обслуживания, ремонта или эксплуатации инструментальной системы безопасности. Убедитесь, что порядок действий будет соблюдаться.		£	
Разработайте план технического обслуживания вашей системы безопасности в соответствии с периодичностью контрольных испытаний.	*Периодичность контрольных испытаний, стр. 21*	£	
Выполняйте обслуживание системы безопасности в соответствии с разработанным планом технического обслуживания.		£	
Регулярно создавайте резервные копии проекта безопасности.	*Создание резервных копий проекта, стр. 101*	£	
При изменении системы безопасности соблюдайте требования, установленные в главах 7.15 и 7.16 стандарта IEC61508-1 (даже если изменения вносятся только в компоненты, которые не имеют отношения к безопасности).		£	
Соблюдайте указания из руководства по обслуживанию *Maintenance Override,* разработанного организацией TÜV, при использовании функции фиксирования (документ можно скачать по адресу *http://www.tuvasi.com/*).	*Функция фиксирования, стр. 94*	£	
Проверьте, что после проведения работ по обслуживанию выключили функцию фиксирования (либо как часть приложения, либо при помощи соответствующей стандартной процедуры).	*Функция фиксирования, стр. 94*	£	
Следите за состоянием модулей безопасности ввода/вывода (состояние, пределы диапазона, перегрузка, правильность канала), см. также справочник *Модули дискретного и аналогового ввода/вывода Quantum*.	*Описание адаптеров устройств удаленного ввода/вывода, стр. 55*, *Описание связи между ЦПУ и вводом/выводом, стр. 40*	£	
Если в системе с резервируемым вводом/выводом случается отказ одного из резервированных модулей, сообщите об этом обслуживающему персоналу.	*Модули вводов/выводов безопасности в конфигурациях с высокой отказоустойчивостью, стр. 42*	£	

Проверки	Ссылка на данное руководство	Выполнено	Примечания
При обнаружении неисправности в одном из парных кабелей системы удаленного ввода/вывода сообщите об этом обслуживающему персоналу.	*Определение конфигурации с горячим резервом, стр. 36*, *Описание адаптеров устройств удаленного ввода/вывода , стр. 55*, *Описание связи между ЦПУ и вводом/выводом, стр. 40*	£	
Если в системе с резервированными модулями питания случается отказ одного из двух модулей питания, сообщите об этом обслуживающему персоналу.	*Модули питания для контроллеров безопасности Quantum, стр. 54*	£	
В системе с горячим резервированием (HSBY) регулярно проверяйте работу резервного контроллера при помощи функционального блока S_HSBY_SWAP.	*Готовность функций горячего резерва, стр. 38*	£	
При замене модуля CRA проверьте, что адрес введен правильно.	*Описание адаптеров устройств удаленного ввода/вывода, стр. 55*	£	
Убедитесь, что ваш персонал владеет всей необходимой информацией и навыками для проведения работ по установке, запуску и обслуживанию системы безопасности.	*Обучение, стр. 27*	£	
Соблюдайте требования по электромагнитной совместимости, электрике, механическим факторам, климатическому воздействию.	*Требования к аппаратному обеспечению, стр. 28*	£	

ОПАСНО

ОПАСНОСТЬ УТРАТЫ ФУНКЦИИ БЕЗОПАСНОСТИ ВО ВРЕМЯ ПУСКО-НАЛАДОЧНЫХ РАБОТ И ОБСЛУЖИВАНИЯ

При внесении изменений в работающую систему всегда соблюдайте требования, установленные в стандарте IEC 61508.

Несоблюдение этих инструкций может привести к смертельному исходу или серьезным травмам.

Специальные требования к стандартным областям применения

5

Специальные требования к стандартным областям применения

Системы обнаружения пожара и утечки газа

Системы обнаружения пожара и утечки газа должны соответствовать требованиям, установленным стандартом EN 54.

Для нормального выполнения функция защиты данные системы должны работать в непрерывном режиме. Следовательно, должны соблюдаться следующие промышленные требования:

- Если для выполнения защиты на вводы и выводы подается напряжение, контроллер должен обнаружить обрыв или короткое замыкание в проводке между контроллером и полевыми устройствами, и включить тревогу.
- Вся система ПЛК должна иметь резервированные источники питания. Далее, источники питания, которые активируют важнейшие выводы и считывают важные с точки зрения безопасности вводы, должны быть резервированными. Необходимо контролировать правильность работы всех источников питания.
- Обесточенные выводы можно применять в обычном режиме работы. Когда необходимо предпринять меры по ликвидации проблемы, на выводы подается напряжение. Системы такого типа должны отслеживать правильность подключения важных выводов к конечным устройствам.
- В качестве полевого источника питания применяется источник постоянного тока напряжением 24 В +/- 10%.

Система аварийной остановки

В системах аварийной остановки (ESD) безопасным состоянием установки считается обесточенное состояние или нулевой уровень (0).

Системы управления котлами

В системах управления котлами безопасным состоянием установки считается обесточенное состояние или нулевой уровень (0).

Если требуется, чтобы система безопасности соответствовала требованиям стандарта EN 50156 на электрическое оборудование для печей, а также требованиям стандарта EN 298 для систем автоматического управления газовыми горелками, общее время цикла контроллера должно быть таким, чтобы безопасное отключение можно было выполнить не позднее, чем спустя 1 секунду после возникновения проблемы в технологическом процессе. Правила вычисления см. в *Безопасная продолжительность процесса, стр. 74*.

Когда данные устройства применяются для управления котлами, модули аналоговых вводов безопасности необходимо контролировать на предмет замыкания на землю (утечка тока). Применяется беспотенциальное соединение проводов. При помощи шунтирующего резистора (например, на 250 Ом), включенного между заземляющей рейкой комплекта заземления и землей, можно измерить напряжение при утечке тока на одном из аналоговых вводов. Для обнаружения утечки необходимо контролировать это напряжение.

В качестве полевого источника питания применяется источник постоянного тока напряжением 24 В +/- 10%.

Приложения

Начальные сведения

Введение

В данных приложениях представлена информация о стандарте безопасности IEC 61508 и принятых в данном стандарте уровнях безопасности (SIL). Кроме этого, приводятся технические характеристики модулей безопасности и модулей, не влияющих на уровень безопасности, а также примеры расчетов.

Что в этом Приложении?

В данном приложении содержатся следущие главы:

IEC 61508

A

Начальные сведения

Введение

В данной главе представлена общая информация о концепции безопасности, принятой в стандарте безопасности IEC 61508, а также подробно рассмотрены принятые уровни безопасности (SIL).

Что в этой главе?

В этой главе имеются следующие темы:

Общие сведения о стандарте IEC 61508

Введение

Системы безопасности разрабатываются для применения в процессах, где риск нанесения вреда человеку, окружающей среде, оборудованию или производству необходимо удерживать на допустимом уровне.Степень риска зависит от вероятности появления и тяжести последствий и, таким образом, устанавливает необходимость применения определенных средств защиты. Когда речь идет о таком понятии, как безопасность процесса, учитываются следующие два фактора:

- правила и требования, установленные государственными властями для защиты людей, окружающей среды, оборудования и производства
- средства, необходимые для соответствия данным установленным требованиям и правилам

Описание стандарта IEC 61508

Стандарт IEC 61508 представляет собой технический стандарт, устанавливающий требования к системам безопасности.
В данном документе рассматривается вопрос функциональной безопасности электрических, электронных и программируемых электронных систем безопасности. Под понятием системы безопасности подразумевается система обеспечения безопасности, выполняющая одну или более специальных функций для удержания степени риска на приемлемом уровне. Такие функции носят определение функций безопасности. Система считается функционально безопасной, если произвольные, систематические или наиболее распространенные неисправности не становятся причиной выхода системы из строя, травмирования или смерти людей, причинения вреда окружающей среде, порче оборудования или нарушения производственного процесса.
В данном стандарте определен общий метод подхода ко всем жизненным циклам систем, которые обеспечивают выполнение функций безопасности. В рамках данного документа представлены методики проектирования, разработки и утверждения аппаратных и программных средств для систем безопасности. Кроме этого, данный стандарт устанавливает правила касательно менеджмента функциональной безопасности и документации.

Описание стандарта IEC 61511

Требования функциональной безопасности, установленные в стандарте IEC 61508 и специально адаптированые для перерабатывающей промышленной отрасли, представлены в следующем техническом стандарте:
• Стандарт IEC 61511: Функциональная безопасность - инструментальные системы безопасности для перерабатывающей промышленности.

В данном стандарте приводится определение назначения систем обеспечения безопасности, начиная с самой ранней стадии проектирования и вплоть до стадии пуско-наладочных работ. При этом также рассмотрены различные модификации систем и способы вывода систем из эксплуатации. В завершение, в данном документе рассматривается безопасный срок службы всех компонентов системы обеспечения безопасности, применяемой в перерабатывающей промышленности.

Описание степеней опасности	В стандарте IEC 61508 рассматриваются концепции анализа степени риска и функции безопасности. Степень риска зависит от вероятности появления и тяжести последствий. Степень риска можно снизить до приемлемого уровня при помощи функции безопасности в составе электрической, электронной или программируемой электронной системы. Далее, степень риска необходимо максимально снизить до уровня, достижимого в реальных условиях. В общих словах, стандарт IEC 61508 рассматривает вопрос опасности следующим образом: • полного отсутствия риска опасности добиться невозможно. • вопросу безопасности необходимо уделять должное внимание с самого начала • вероятность появления недопустимого риска опасности необходимо свести к минимуму

Уровни безопасности (SIL)

Введение

Цифровые обозначения уровня безопасности (SIL) отражают стойкость системы к неисправностям и, таким образом, демонстрируют способность системы с определенной долей вероятности обеспечивать выполнение функции безопасности. Стандарт IEC 61508 устанавливает четыре уровня безопасности в зависимости от степени опасности или тяжести последствий, оказываемых процессом, для которого применяется данная система безопасности. Чем выше степень вреда окружающей среде и общественности, тем выше выше требования безопасности для снижения риска данной опасности.

Описание цифровых обозначений SIL

В нижеприведенной таблице приводится зависимость между назначением функции безопасности и цифровым обозначением уровня SIL:

Уровень SIL	Назначение функции безопасности
4	защита окружающей среды и населения
3	защита людей
2	• защита собственности и производственного оборудования • защита людей
1	защита производственных площадок

SIL требований Описание

Для обеспечения функциональной безопасности предусмотрено два вида обязательных требований:

- требования к функциям безопасности, которые устанавливают необходимые функции безопасности
- требования по уровню SIL, которые определяют необходимую степень вероятности выполнения функций безопасности

Требования к функциям безопасности формируются на основании данных, полученных в результате анализа опасности, и требований по уровню безопасности, полученных в результате оценки степени риска.

К вышеупомянутым требованиям относятся следующие величины:

- среднее время наработки на отказ
- вероятность отказа
- частота отказов
- диагностическое покрытие
- коэффициент безопасных отказов
- отказоустойчивость аппаратных средств

В зависимости от уровня безопасности данные значения не должны превышать установленных пределов.

Описание цифровых обозначений SIL

В соответствии с определениями, данными в стандарте IEC 61508, обозначение SIL зависит от коэффициента безопасных отказов (SFF) и коэффициента отказоустойчивости (HFT) подсистемы, обеспечивающей выполнение функции безопасности. Коэффициент безопасных отказов (HFT) величины n означает, что n+1 отказов могут привести к невозможности выполнения функции безопасности, означая, таким образом, невозможность перехода в безопасное состояние. Коэффициент SFF зависит от частоты отказов и диагностического покрытия.

В таблице ниже показана зависимость между коэффициентами SFF, HFT и SIL для сложных подсистем обеспечения безопасности в соответствии с требованиями стандарта IEC 61508-2, где невозможно четко определить отказ всех компонентов:

SFF	**HFT=0**	**HFT=1**	**HFT=2**
SFF ≤ 60%	-	SIL1	SIL2
60% < SFF ≤ 90%	SIL1	SIL2	SIL3
90% < SFF ≤ 99%	SIL2	SIL3	SIL4
SFF > 99%	SIL3	SIL4	SIL4

Существует два метода повышения уровня безопасности SIL:

- через повышение коэффициента HFT методом ввода дополнительных независимых контуров выключения
- через повышение коэффициента SFF методом дополнительной диагностики

SIL-Demand Relation Описание

Стандарт IEC 61508 устанавливает различия между режимами низкой и высокой (или постоянной) загрузки системы безопасности.

В режиме низкой загрузки система обеспечения безопасности активируется не чаще 1 раза в год или не больше чем вдвое по сравнению с периодичностью контрольного испытания. Уровень безопасности (SIL) системы безопасности низкой нагрузки напрямую соответствует ее средней вероятности отказа от выполнения требуемой функции безопасности, или проще говоря, вероятности отказа выполнять функции безопасности (PFD).

В режиме высокой загрузки система обеспечения безопасности активируется чаще 1 раза в год или больше чем вдвое по сравнению с периодичностью контрольного испытания. Уровень безопасности (SIL) такой системы безопасности напрямую соответствует средней вероятности серьезного отказа данной системы в час, или проще говоря, вероятности отказа в час (PFH).

Уровни SIL для режима низкой загрузки

В таблице ниже приводятся требования к системе, работающей в низком режиме загрузки:

Уровень SIL	Вероятность отказа выполнения требуемой функции
4	от $\geq 10^{-5}$ до $< 10^{-4}$
3	от $\geq 10^{-4}$ до $< 10^{-3}$
2	от $\geq 10^{-3}$ до $< 10^{-2}$
1	от $\geq 10^{-2}$ до $< 10^{-1}$

Уровни SIL для режима высокой загрузки

В таблице ниже приводятся требования к системе, работающей в высоком режиме загрузки:

Уровень SIL	Вероятность отказа в час
4	от $\geq 10^{-9}$ до $< 10^{-8}$
3	от $\geq 10^{-8}$ до $< 10^{-7}$
2	от $\geq 10^{-7}$ до $< 10^{-6}$
1	от $\geq 10^{-6}$ до $< 10^{-5}$

Для уровня SIL2 требуемые значения вероятности отказа комплексной системы безопасности выглядят следующим образом:

- PFD> 10^{-3} до < 10^{-2} для низкой загрузки
- PFH >10^{-7} до < 10^{-6} для высокой загрузки

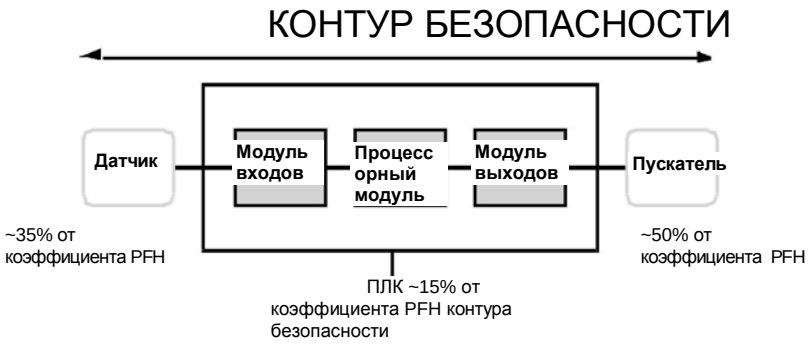
Описание контура безопасности

При расчете частоты отказов определенная вероятность отказа компонентов системы безопасности или контура безопасности берется в расчет для получения величины общей вероятности.

Контур безопасности состоит из трех элементов:

- датчик
- защитный ПЛК
- пускатель

На рисунке ниже показан типичный пример контура безопасности с вероятностью отказов его элементов.



На рисунке выше показано, что на долю ПЛК приходится всего 10-20%, поскольку вероятность отказа датчиков и пускателей, как правило, существенно выше.

Осторожное заключение о том, что на долю безопасности ПЛК в общей вероятности отказа приходится 10%, увеличивает допустимые пределы действия, в результате чего требования к вероятности отказа ПЛК будут следующими:

- PFD >10^{-4} до < 10^{-3} для низкой нагрузки
- PFH >10^{-8} до < 10^{-7} для высокой нагрузки

Описание уравнения PFD

В стандарте IEC 61508 предполагается, что половина всех отказов завершается в безопасном состоянии. Поэтому частота отказов ***X*** далее подразделяется на

- λ_S - безопасный отказ, и
- λ_D - опасный отказ, который далее подразделяется на
- λ_{DD} - опасный отказ, выявленный во время внутренней диагностики
- λ_{DU} - опасный отказ, оставшийся невыявленным.

При расчете коэффициента частоты отказов используется среднее время наработки на отказ (зависит от конкретного модуля). Правила расчета приведены ниже:

λ= 1/Средняя наработка на отказ

Уравнение для вычисления вероятности отказа выглядит следующим образом:

$PFD(t) = \lambda_{DU} \times t$

t - это период времени между 2 контрольными испытаниями.
Когда речь идет о вероятности отказа в час, подразумевается, что период времени равен 1 часу. Поэтому уравнение с коэффициентом PFD приводится к следующему виду:
$PFH = \lambda_{DU}$

Системные объекты

B

Начальные сведения

Введение

В данной главе приводится описание системных битов и слов контроллеров безопасности Quantum.

Примечание: Символы, соответствующие каждому битовому объекту или системному слову, приводятся в таблицах с описанием данных объектов, но не считаются стандартными компонентами программного обеспечения. Поэтому при необходимости они могут вводиться через редактор данных. Они предложены для того, чтобы обеспечить однородность их наименований в различных приложениях.

Что в этой главе?

В этой главе имеются следующие параграфы:

B.1 Системные биты

Начальные сведения

Введение

В данном параграфе приводится описание системных битов контроллеров безопасности Quantum.
Для удобства пользователя все системные биты стандартных ПЛК Quantum перечислены, но разъясняются только в случае, если использованы в ПЛК безопасности Quantum.

Что в этом параграфе?

В этом параграфе имеются следущие темы:

Представление системных битов

Основные положения

ПЛК Quantum применяют %Si системных битов, которые отображают состояние ПЛК, или они могут быть использованы для управления способом работы.
Эти биты можно протестировать в пользовательской программе для обнаружения какой-либо функциональной разработки.
Некоторые из этих битов могут быть переключены в начальное или обычное состояние программой или пользователем. Остальные биты автоматически переключаются системой. Наконец, имеются биты, которые только отображают состояние ПЛК.

Подробное описание

Примечание: В ПЛК безопасности Quantum могут использоваться не все системные биты. Неиспользуемые системные биты отмечены в столбце **Quant. Safety** "НЕТ".
Ниже в таблице приведено описание системных битов от %S0 до %S13

Обозначение бита	**Функция**	**Описание**	**Начальное состояние**	**Доступ к записи**	**Quant.** Безопасность
%S0 COLDSTART	Холодный пуск	Обычно установленный в 0, этот бит устанавливается в 1 с помощью: • восстановления питания с потерей данных (отказ батареи), • пользовательской программы, • терминала, • замены картриджа, • загрузки программы Этот бит устанавливается в 1 во время первого полностью восстановленного цикла ПЛК в режиме RUN или STOP. Он сбрасывается в 0 системой перед следующим циклом.	1 (1 цикл)	НЕТ	ДА
%S1 WARMSTART	Горячий пуск	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	0	НЕТ	НЕТ
%S4 TB10MS	Время 10 мс	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	-	НЕТ	НЕТ
%S5 TB100MS	Время 100 мс	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	-	НЕТ	НЕТ
%S6 TB1SEC	Время 1 мс	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	-	НЕТ	НЕТ
%S7 TB1MIN	Время 1 мин	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	-	НЕТ	НЕТ
%S10 IOERR	Сбой ввода/ вывода	Обычно установленный в 1, он устанавливается в 0 при обнаружении сбоя ввода/вывода во входном монтажном шасси или устройстве на Fipio (например, несовместимая конфигурация, сбой обмена, сбой аппаратуры и т. д.). Бит %S10 сбрасывается в 1 системой сразу после устранения сбоя.	1	НЕТ	ДА
%S11 WDG	Переполнение схемы безопасности	Обычно установленный в 1, он устанавливается в 0 системой сразу после того, как время выполнения задачи становится больше максимального времени выполнения (например, схема безопасности), объявленного в свойствах задачи.	0	НЕТ	ДА

Обозначение бита	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%S12 PLCRUNNING	ПЛК в RUN	Этот бит устанавливается системой в 1, когда ПЛК находится в режиме RUN. Он устанавливается системой в 0, как только ПЛК выходит из режима RUN (STOP, INIT и т. д.).	0	НЕТ	ДА
%S13 1RSTSCANRUN	Первый цикл после переключения в RUN	Обычно установленный в 0, он устанавливается системой в 1 во время первого цикла главной задачи после установки ПЛК в режим RUN.	-	НЕТ	ДА

ВНИМАНИЕ

НЕПРЕДНАМЕРЕННЫЕ ОТКЛОНЕНИЯ В РАБОТЕ ОБОРУДОВАНИЯ

В ПЛК безопасности Quantum ошибки связи из модулей NOE, CRA и CRP не сообщаются в бите %S10.

Ответственность за правильное использование этих системных битов полностью лежит на вас.

Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Подробное описание

Примечание: В ПЛК безопасности Quantum могут использоваться не все системные биты. Неиспользуемые системные биты отмечены в столбце **Quant. Safety** "НЕТ".
Ниже в таблице приведено описание системных битов от %S15 до %S21:

Обозначение бита	**Функция**	**Описание**	**Начальное состояние**	**Доступ к записи**	**Quant. Безо**пасность
%S15 STRINGERROR	Сбой последовательности символов	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%S16 IOERRTSK	Сбой задачи ввода/вывода	Обычно установленный в 1, он устанавливается системой в 0 при сбое в модуле ввода/вывода входного монтажного шасси или устройстве Fipio, сконфигурированном в задаче. Этот бит должен быть переключен в 1 пользователем.	1	ДА	ДА
%S17 CARRY	Выход вращения или сдвига	Обычно в 0 Во время операции вращения или сдвига этот бит принимает состояние исходящего бита.	0	НЕТ	ДА
%S18 OVERFLOW	Переполнение или арифметическая ошибка	Обычно установленный в 0, он устанавливается системой в 1 в случае переполнения при наличии • результата выше + 32 767 или меньше - 32 768, в одиночной длине, • результата выше + 65 535, в целом числе без знака, • результата выше + 2 147 483 647 или меньше - 2 147 483 648, в двойной длине, • результата выше +4 294 967 296, в двойной длине или целом числе без знака • вещественных значений вне пределов, • деления на 0, • корня отрицательного числа, • фиксирования к несуществующему шагу на барабане, • заполнения уже полного регистра, опустошения уже пустого регистра. Он должен проверяться пользовательской программой после каждой операции, если имеется риск переполнения, а затем сбрасываться пользователем в 0 при переполнении. Когда бит %S18 переключается в 1, приложение останавливается в состоянии ошибки, если бит %S78 был установлен в 1.	0	ДА	ДА

Обозначение бита	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%S19 OVERRUN	Период перегрузки задачи (периодическое сканирование)	Обычно установленный в 0, он устанавливается системой в 1 в случае интервала времени перегрузки (т. е. время выполнения задачи выше, чем период, определенный пользователем в конфигурации или запрограммированный в слове %SW, связанном с задачей). Пользователь должен переключить этот бит в 0. Каждая задача управляет собственным битом %S19.	0	ДА	ДА
%S20 INDEXOVF	Переполнение указателя	Обычно установленный в 0, он устанавливается в 1, когда адрес указанного объекта становится меньше 0 или превышает количество объектов, объявленных в конфигурации. В этом случае это выглядит, как указатель был равен 0. Он должен проверяться пользовательской программой после каждой операции, а затем сбрасываться пользователем в 0 при переполнении. Когда бит %S20 переключается в 1, приложение останавливается в состоянии ошибки, если бит %S78 был установлен в 1.	0	ДА	НЕТ
%S21 1RSTTASKRUN	Цикл первой задачи	Проверенный в задаче (Mast, Fast, Aux0, Aux1, Aux2 Aux3), бит %S21 указывает первый цикл этой задачи. %S21 установлен в 1 в начале цикла и сбрасывается в ноль в конце цикла. **Примечания**: Бит %S21 не имеет того же значения в PL7, как в Unity Pro.	0	НЕТ	ДА

ВНИМАНИЕ
НЕПРЕДНАМЕРЕННЫЕ ОТКЛОНЕНИЯ В РАБОТЕ ОБОРУДОВАНИЯ
В ПЛК безопасности Quantum ошибки связи из модулей NOE, CRA и CRP не сообщаются в бите %S16.
Ответственность за правильное использование этих системных битов полностью лежит на вас.
Несоблюдение этих инструкций может привести к смертельному исходу, серьезным травмам или повреждению оборудования.

Подробное описание

Примечание: В ПЛК безопасности Quantum могут использоваться не все системные биты. Неиспользуемые системные биты отмечены в столбце **Quant. Safety** "НЕТ".
Ниже в таблице приведено описание системных битов от %S30 до %S51:

Обозначение бита	**Функция**	**Описание**	**Начальное состояние**	**Доступ к записи**	**Quant. Безо**пасность
%S30 MASTACT	Активизация/ деактивизация главной задачи	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	1	ДА	НЕТ
%S31 FASTACT	Активизация/ деактивизация быстрой задачи	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%S32	Активизация/ деактивизация вспомогательных задач 0-3	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%S33					
%S34					
%S35					
%S38 ACTIVEVT	Разрешение/ запрет событий	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	1	ДА	НЕТ
%S39 EVTOVR	Насыщение в обработке события	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%S50 RTCWRITE	Обновление времени и даты с помощью слов от %SW50 до %SW53	Обычно установленный в 0, он устанавливается в 1 с помощью программы или терминала: • установлен в 0: обновление системных слов от %SW50 до %SW53 с помощью времени и даты из часов реального времени ПЛК, • установлен в 1: системные слова от %SW50 до %SW53 больше не обновляются, тем самым делая возможным изменить их. • Переключение из 1 в 0 обновляет часы реального времени на значения, введенные в слова от %SW50 до %SW53.	0	ДА	ДА
%S51 RTCERR	Потеря времени в часах реального времени	Этот управляемый системой бит, установленный в 1, показывает, что часы реального времени отсутствуют или что системные слова (от %SW50 до %SW53) бессмысленны. Если бит установлен в 1, часы должны быть переставлены на правильное время.	-	НЕТ	ДА

Подробное описание

Примечание: В ПЛК безопасности Quantum могут использоваться не все системные биты. Неиспользуемые системные биты отмечены в столбце **Quant. Safety** "НЕТ".
Ниже в таблице приведено описание системных битов от %S59 до %S122:

Обозначение бита	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%S59 RTCTUNING	Инкрементное обновление времени и даты с помощью слова %SW59	Обычно установленный в 0, он может быть установлен в 1 или 0 с помощью программы или терминала: • установлен в 0: система не управляет системным словом %SW59, • установлен в 1: система управляет границами в слове %SW59 для регулировки даты и текущего времени (путем приращения).	0	ДА	ДА
%S67 PCMCIABAT0	Состояние батареи платы памяти приложения	Этот бит используется для контроля состояния главной батареи, когда плата памяти находится в верхнем слоте PCMCIA (все Atriums, Premiums, и в Quantums (140 CPU 671 60, 140 CPU 651 60 и 140 CPU 651 50)): • установлен в 1: основное напряжение батареи снижено (приложение зафиксировано, но вы должны заменить батарею в соответствии с так называемой предиктивной процедурой техобслуживания), • установлен в 0: основное напряжение батареи достаточное (приложение всегда зафиксировано). Бит %S67 управляется: • в платах ОЗУ малой и средней емкости PV06 (версия записана на ярлыке платы), т. е., предлагается размер памяти ниже Unity =#768K: TSX MRP P 128K, TSX MRP P 224K TSX MCP C 224K, MCP C 512K, TSX MRP P 384K, TSX MRP C 448K, TSX MRP C 768K, • под Unity с версией **>** 2.02.	-	НЕТ	ДА
%S68 PLCBAT	состояние батареи процессора	Этот бит используется для проверки рабочего состояния резервной батареи для сохранения данных и программы в ОЗУ: • установлен в 0: батарея в наличии и в рабочем состоянии, • установлен в 1: батарея отсутствует или в нерабочем состоянии.	-	НЕТ	ДА
%S75 PCMCIABAT1	состояние батареи платы памяти хранения данных	Этот бит используется для контроля состояния главной батареи, когда плата памяти находится в нижнем слоте PCMCIA, см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro* **Примечание:** Данные, хранящиеся в плате памяти в слоте B, в безопасных проектах не обрабатываются.	-	НЕТ	НЕТ

Обозначение бита	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%S76 DIAGBUFFCONF	Сконфигурированный буфер диагностики	Этот бит устанавливается системой в 1, когда сконфигурирована опция диагностики. Затем резервируется буфер диагностики для хранения ошибок, обнаруженных DFB диагностики. Этот бит только для чтения.	0	НЕТ	ДА
%S77 DIAGBUFFFULL	Полный буфер диагностик	Этот бит устанавливается системой в 1, когда буфер, принимающий ошибки из блоков функции диагностики, полон. Этот бит только для чтения.	0	НЕТ	ДА
%S78 HALTIFERROR	Останавливает в случае ошибки	Обычно установленный в 0, этот бит может быть установлен пользователем в 1 для программирования остановки ПЛК в случае сбоя приложения: %S15, %S18, %20.	0	ДА	ДА
%S80 RSTMSGCNT	Перезапуск счетчиков сообщений	Обычно установленный в 0, этот бит может быть установлен пользователем в 1 для перезапуска счетчиков сообщений от %SW80 до %SW86.	0	ДА	ДА
%S94 SAVECURRVAL	Сохранение значений регулировки	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%S118 REMIOERR	Основной сбой ввода/вывода Fipio	Обычно установленный в 1, он устанавливается системой в 0 в случае сбоя в устройстве, подключенном к удаленной шине ввода/вывода RIO и Fipio. Эта шина переключается в 1 системой, когда сбой исчезает.	-	НЕТ	ДА
%S119 LOCIOERR	Основной сбой ввода/вывода монтажного шасси	Обычно установленный в 1, он устанавливается системой в 0 при сбое в модуле ввода/вывода, расположенного в одном из монтажных шасси. Эта шина переключается в 1 системой, когда сбой исчезает.	-	НЕТ	ДА
%S120 **%S121** **%S122**	Сбои шины DIO	см. главу "Системные биты" в *Справочнике по структуре программы и языкам Unity Pro*	-	НЕТ	НЕТ

B.2 Системные слова

Коротко

В этом разделе описаны системные слова ПЛК безопасности Quantum. Для удобства перечислены все системные слова стандартных ПЛК Quantum, но разъясняются только те, которые используются в ПЛК безопасности Quantum.

Введение

Что в этом параграфе?

В этом параграфе имеются следущие темы:

Подробное описание

Примечание: В ПЛК безопасности Quantum могут использоваться не все системные слова. Неиспользуемые системные слова отмечены в столбце **Quant. Safety** "НЕТ".
Ниже в таблице приведено описание системных слов от %SW0 to %SW21:

Обозначение слова	**Функция**	**Описание**	**Начальное состояние**	**Доступ к записи**	**Quant. Безо**пасность
%SW0 MASTPERIOD	Период сканирования главной задачи	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%SW1 FASTPERIOD	Период сканирования быстрой задачи	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%SW2, **%SW3**, **%SW4**, **%SW5**	Период сканирования вспомогательной задачи	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%SW8 TSKINHIBIN	Сбор данных контроля входной задачи	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%SW9 TSKINHIBOUT	Контроль обновления выходной задачи	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%SW10 TSKINIT	Первый цикл после холодного пуска	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	НЕТ	НЕТ
%SW11 WDGVALUE	Продолжительность таймера «watchdog»	Считывает продолжительность таймера «watchdog». Продолжительность выражается в миллисекундах (10...1500 мс). Это слово нельзя изменять.	-	НЕТ	ДА
%SW12 APMODE	Режим процессора приложения	Это слово отображает рабочий режим процессора приложения. Возможны следующие значения: • 16#A501: процессор приложения в режиме техобслуживания. • 16#5AFE: процессор приложения в безопасном режиме. Любое другое значение интерпретируется как ошибка. Это системное слово для стандартного ЦПУ Quantum недоступно.	16#A501	НЕТ	ДА

Обозначение слова	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%SW13 INTELMODE	Режим процессора Intel	Это слово отображает рабочий режим процессора Intel Pentium. Возможны следующие значения: • 16#501A: процессор приложения в режиме техобслуживания. • 16#5AFE: процессор приложения в безопасном режиме. Любое другое значение интерпретируется как ошибка. Это системное слово для стандартного ЦПУ Quantum недоступно.	16#501A	НЕТ	ДА
%SW14 OSCOMMVERS	Коммерческая версия процессора ПЛК	Это слово содержит коммерческую версию процессора ПЛК. **Пример: версия** 16#0135: 01; номер выпуска: 35	-	НЕТ	ДА
%SW15 OSCOMMPATCH	Исправленная версия процессора ПЛК	Это слово содержит коммерческую версию исправления процессора ПЛК. Оно закодировано в младшем разряде слова. коды: 0 = не исправлено, 1 = A, 2 = B... **Пример:** 16#0003 соответствует исправлению C.	-	НЕТ	ДА
%SW16 OSINTVERS	Номер версии микропрограммного обеспечения	Это слово содержит в шестнадцатеричном виде номер версии микропрограммного обеспечения процессора ПЛК. **Пример:** 16#0017 версия: 2.1; VN: 17	-	НЕТ	ДА
%SW17 FLOATSTAT	Состояние ошибки в плавающей операции	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ
%SW18 **%SW19** 100MSCOUNTER	Счетчик абсолютного времени	%SW18 является низким, а %SW19 – высоким словами для расчета продолжительностей. Оба приращаются системой каждую 1/10 секунды (даже если ПЛК находится в состоянии STOP, они больше не приращаются, если отключено питание). Они могут читаться или записываться пользовательской программой или терминалом.	0	ДА	ДА
%SW20 **%SW21** MSCOUNTER	Счетчик абсолютного времени	Низкое слово %SW20 и высокое слово %SW21 приращаются системой каждую 1/1000 секунды (даже если ПЛК находится в состоянии STOP, они больше не приращаются, если отключено питание). Они могут читаться пользовательской программой или терминалом. %SW20 and %SW21 перезапускаются при холодном пуске, но не при перезапуске из памяти.	0	НЕТ	ДА

Подробное описание

Примечание: В ПЛК безопасности Quantum могут использоваться не все системные слова. Неиспользуемые системные слова отмечены в столбце **Quant. Safety** "НЕТ".
Ниже в таблице приведено описание системных слов от %SW30 to %SW59:

Обозначение слова	**Функция**	**Описание**	**Начальное состояние**	**Доступ к записи**	**Quant. Безо**пасность
%SW30 MASTCURRTIME	Время выполнения главной задачи	Это слово отображает время выполнения последнего цикла главной задачи (в мс).	-	НЕТ	ДА
%SW31 MASTMAXTIME	Максимальное время выполнения главной задачи	Это слово отображает самое длительное время выполнения после последнего холодного запуска (в мс).	-	НЕТ	ДА
%SW32 MASTMINTIME	Минимальное время выполнения главной задачи	Это слово отображает самое короткое время выполнения после последнего холодного запуска (в мс).	-	НЕТ	ДА
%SW33 %SW34 %SW35	Время выполнения быстрой задачи	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	-	НЕТ	НЕТ
%SW36 to %SW47	Время выполнения вспомогательной задачи	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	-	НЕТ	НЕТ
%SW48 IOEVTNB	Количество событий	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	НЕТ

Обозначение слова	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%SW49 DAYOFWEEK **%SW50** SEC **%SW51** HOURMIN **%SW52** MONTHDAY **%SW53** YEAR	Часы реального времени	Системные слова, содержащие дату и текущее время (в BCD): • %SW49: день недели: • 1 = понедельник, • 2 = вторник, • 3 = среда, • 4 = четверг, • 5 = пятница, • 6 = суббота, • 7 = воскресенье, • %SW50: секунды (16#SS00), • %SW51: часы и минуты (16#HHMM), • %SW52: месяц и день (16#MMDD), • %SW53: год (16#YYYY). Эти слова управляются системой, когда бит %S50 установлен в 0. Эти слова могут быть записаны программой пользователя или с помощью терминала, когда %S50 установлен в 0.	-	ДА	ДА
%SW54 STOPSEC **%SW55** STOPHM **%SW56** STOPMD **%SW57** STOPYEAR **%SW58** STOPDAY	Часы реального времени на последней остановке	Системные слова, содержащие дату и время последнего сбоя питания или остановки ПЛК (в двоично-десятичном числе): • %SW54: секунды (00SS), • %SW55: часы и минуты (HHMM), • %SW56: месяц и день (MMDD), • %SW57: год (YYYY), • %SW58: старший байт содержит день недели (от 1 для понедельника до 7 для воскресенья), а младший байт содержит код для последней остановки: • 1 = изменение от RUN до STOP с помощью терминала или специализированного входа, • 2 = остановка с помощью таймера «watchdog» (задача ПЛК или перегрузка SFC), • 4 = колебания сетевого напряжения или блокировка платы памяти, • 5 = остановка из-за сбоя аппаратуры, • 6 = остановка из-за сбоя программы. Информация о типе сбоя программы хранится в %SW125.	-	НЕТ	ДА

Обозначение слова	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%SW59 ADJDATETIME	Регулировка текущей даты	Содержит 2 8-битовые серии для регулировки текущей даты. Эта операция всегда выполняется на нарастающем фронте бита. Это слово разрешается с помощью бита %S59, установленного в 1. Ниже на рисунке биты в левом столбце прибавляют значение, а биты в правом столбце уменьшают его:	0	ДА	ДА
					

Подробное описание

Примечание: В ПЛК безопасности Quantum могут использоваться не все системные слова. Неиспользуемые системные слова отмечены в столбце **Quant. Safety** "НЕТ".
Ниже в таблице приведено описание системных слов от %SW60 to %SW127:

Обозначение слова	**Функция**	**Описание**	**Начальное состояние**	**Доступ к записи**	**Quant. Безо**пасность
%SW60 HSB_CMD	Регистр команд горячего резерва Quantum	Значение различных битов слова %SW60: • %SW60.0=1 делает недействительными команды, введенные на дисплей (клавиатура). • %SW60.1 • =0 устанавливает ПЛК A в режим OFFLINE. • =1 устанавливает ПЛК A в режим RUN. • %SW60.2 • =0 устанавливает ПЛК B в режим OFFLINE. • =1 устанавливает ПЛК B в режим RUN. • %SW60.3=0 фиксирует резервный ПЛК в режиме OFFLINE, если приложения различаются. • %SW60.4 • =0 авторизует обновление программно-аппаратного обеспечения только после остановки приложения. • =1 авторизует обновление программно-аппаратного обеспечения без остановки приложения. • %SW60.5=1 запрос передачи приложения от резервного к основному. • %SW60.8 • =0 переключение адреса на порту 1 Modbus во время первичного обмена. • =1 нет переключения адреса на порту 1 Modbus во время первичного обмена.	0	НЕТ	ДА

Обозначение слова	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%SW61 HSB_STS	Регистр состояния Quantum	Значение различных битов слова %SW61: • биты рабочего режима ПЛК %SW61.0 и %SW61.1: • %SW61.1=0, %SW61.0=1: режим OFFLINE. • %SW61.1=1, %SW61.0=0: основной режим. • %SW61. 1=1, %SW61.0=1: второстепенный режим (резерв). • биты рабочего режима %SW61.2 и %SW61.3 из другого ПЛК • %SW61.3=0, %SW61.2=1: режим OFFLINE. • %SW61.3=1, %SW61.2=0: основной режим. • %SW61.3=1, %SW61.2=1: второстепенный режим (резерв). • %SW61.3=0, %SW61.2=0: удаленный ПЛК недоступен (выключен, нет связи). • %SW61.4=0 на обоих ПЛК приложения идентичны. • %SW61.5 • =0 ПЛК используется в качестве блока A. • =1 ПЛК используется в качестве блока B. • %SW61.14=0 нелокализованные переменные передаются. • %SW61.15 • =0 горячий резерв не активизирован. • =1 горячий резерв активизирован.	0	НЕТ	ДА
%SW62 HSBY_REVERSE 0 **%SW63** HSBY_REVERSE 1	Слово передачи	Эти два слова могут быть записаны пользователем в первом разделе главной задачи. Затем они автоматически передаются из резервного процессора для обновления основного ПЛК. Они могут быть считаны на основном ПЛК и использоваться в качестве основных параметров приложения.	0	ДА	ДА
%SW70 WEEKOFYEAR	Часы реального времени	Системное слово, содержащее количество недель в году: от 1 до 52.	-		ДА

Обозначение слова	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%SW71 KEY_SWITCH	Положение переключателей на передней панели ПЛК	Это слово обеспечивает изображение позиций переключателей на передней панели процессора Quantum. Оно автоматически обновляется системой. • %SW71.0 = 1 переключатель в положении "Память защищена", • %SW71.1 = 1 переключатель в положении "STOP", • %SW71.2 = 1 переключатель в положении "START", • %SW71.8 = 1 переключатель в положении "MEM", • %SW71.9 = 1 переключатель в положении "ASCII", • %SW71.10 = 1 переключатель в положении "RTU", • %SW71.от 3 до 7 и от 11 до 15 не используются.	0	НЕТ	ДА
%SW75 TIMEREVTNB	Счетчик событий таймерного типа	см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0		НЕТ
%SW76 DLASTREG	Функция диагностики: запись	Результат последней регистрации: • = 0 если запись была успешной, • =1 если буфер диагностики не был сконфигурирован, • =2 если буфер диагностики полон.	0		ДА
%SW77 DLASTDEREG	Функция диагностики: незапись	Результат последней разрегистрации: • = 0 если незапись была успешной, • =1 если буфер диагностики не был сконфигурирован, • =21 если идентификатор ошибки неисправен • =22 если ошибка не была записана.	0		ДА
%SW78 DNBERRBUF	Функция диагностики: количество ошибок	Количество ошибок в буфере диагностики.	0		ДА
%SW80 MSGCNT0 **%SW81** MSCNT1	Управление сообщениями	Эти слова обновляются системой, а также могут быть переключены с помощью %S80. • %SW80: Количество сообщений, отправляемых системой в порт терминала, • %SW81: Количество сообщений, принимаемых системой из порта терминала,	0	ДА	ДА
%SW87 MSTSERVCNT	Управление коммуникационным потоком	Количество запросов, обработанных синхронным сервером на цикл основной задачи.	0		ДА

Обозначение слова	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%SW90 MAXREQNB	Максимальное количество запросов, обработанных синхронным сервером на цикл основной задачи	Это слово применяется для максимальной установки количества запросов, обработанных ПЛК на цикл основной задачи Когда ЦПУ является сервером: это количество запросов должно быть между 2 (минимум) и N+4 (максимум). N: количество различается в зависимости от модели. Когда ЦПУ является клиентом: N: количество различается в зависимости от модели. Значение 0 не будет работать. Если введено значение, лежащее вне диапазона, то в расчет следует принять значение N. см. главу "Системные объекты" в *Справочнике по структуре программы и языкам Unity Pro*	0	ДА	ДА
%SW108 FORCEDIOIM	Количество фиксированных битов модуля ввода/вывода	Это системное слово считает количество фиксированных битов модуля ввода/вывода. Это слово инкрементируется для каждого фиксирования и декрементируется для каждой отмены фиксирования.	0	НЕТ	ДА
%SW110	Количество свободных областей памяти для %M.	Это системное слово дает информацию о размере свободных областей памяти для %M. Это системное слово для стандартного ЦПУ Quantum недоступно.	-	НЕТ	ДА
%SW111	Количество свободных областей памяти для %MW.	Это системное слово дает информацию о размере свободных областей памяти для %MW. Это системное слово для стандартного ЦПУ Quantum недоступно.	-	НЕТ	ДА
%SW124 CPUERR	Тип системного сбоя	Последний встречающийся тип системного сбоя записывается системой в слово (эти коды при холодном перезапуске не меняются): • 16#30: сбой системного кода, • 16#53: сбой таймаута во время изменений ввода/вывода, • 16#60 to 64: перегрузка стека, • 16#90: системный сбой переключения: Не предусмотрен IT.	-	НЕТ	ДА

Обозначение слова	Функция	Описание	Начальное состояние	Доступ к записи	Quant. Безопасность
%SW125 BLKERRTYPE	Последний обнаруженный сбой	В этом слове дан код последнего обнаруженного сбоя: Коды ошибок, приведенные ниже, вызывают остановку ПЛК, если %S78 установлено в 1. %S 15, %S 18 и %S20 всегда активизированы независимо от %S78: • 16#2258: выполнение команды HALT, • 16#DE87: ошибка вычисления с числами с плавающей точкой (%S18, эти ошибки перечислены в слове %SW17), • 16#DEB0: переполнение таймера «watchdog» (%S11), • 16#DEF0: деление на 0 (%S18), • 16#DEF1: ошибка передачи символьной строки (%S15), • 16#DEF2: арифметическая ошибка (%S18), • 16#DEF3: переполнение индекса (%S20). **Примечание:** Коды 16#8xxx и 16#7xxx не останавливают приложение и указывают ошибку в функциональных блоках. В случае ошибки безопасности ПЛК останавливается. После выключения питания и перезапуска ПЛК %SW 125 будет содержать код причины ошибки. • 0x5AF1 : Ошибка проверки упорядоченности (непредсказуемое выполнение в ЦПУ) • 0x5AF2: Ошибка в памяти (сбой адреса) • 0x5AF3: Ошибка сравнения (результаты выполнения процессора Intel и процессора приложения различаются) • 0x5AF4: Отказ часов реального времени • 0x5AF5: Выполнение ошибки инициализации двойного кода • 0x5AF6: Ошибка активизации таймера «watchdog» • 0x5AF7: Ошибка во время проверки памяти (занимает более 8 часов) • 0x5AF8: Ошибка в проверке памяти (отказ ОЗУ)	-	НЕТ	ДА

Обозначение слова	**Функция**	**Описание**	**Начальное состояние**	**Доступ к записи**	**Quant. Безо**пасность
%SW126 ERRADDR0 **%SW127** ERRADDR1	Адрес команды сбоя блокировки	Адрес команды, который генерирует сбой блокировки приложения. Для 16-битных процессоров: • %SW126 содержит смещение для этого адреса, • %SW126 содержит номер сегмента для этого адреса, Для 32-битных процессоров: • %SW126 содержит младшее слово для этого адреса, • %SW127 содержит младшее слово для этого адреса, В случае ошибки безопасности содержимое %SW126 и %SW127 предназначено только для .	0	ПОЖАР.	ДА

Описание системных слов от %SW128 до %SW180 и от %SW535 до %SW640 см. в главе "Системные слова Quantum" в *Справочнике по структуре программы и языкам Unity Pro.* Системные слова от SW181 до %SW534 в ПЛК безопасности Quantum не используются.

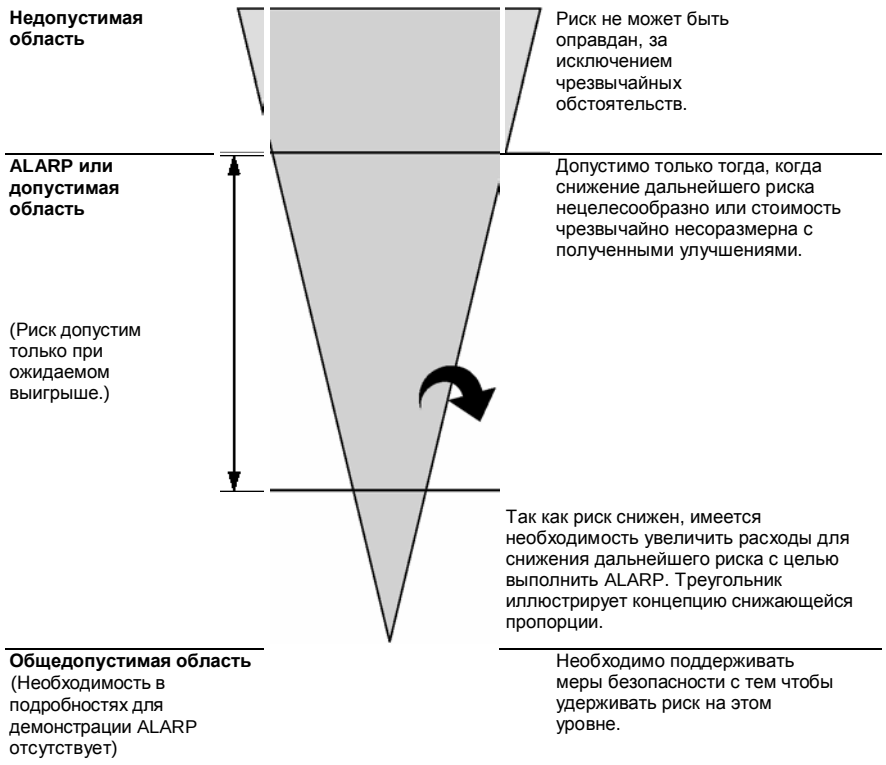
Глоссарий

!

Конфигурация диагностики 1002D
X вне Y
Например, 1 вне 2. Голосование и возможность резервирования системы, связанной с обеспечением безопасности.
D в 1oo2D относится к диагностике. Таким образом, D в 1oo2D означает 1 вне 2 с диагностикой.

A

ALARP
As low as is reasonably practicable, практически целесообразный низкий уровень



C

CCF

Common cause failure, сбой по общей причине
Этот вид сбоя является результатом одного или нескольких событий, что вызывает соответствующие неисправности двух или нескольких отдельных каналов в многоканальной системе, что приводит к неисправности системы. Показатель общей причины в системе двойных каналов является критическим для вероятности отказа по требованию для всей системы.

Холодный пуск
Cold start
Холодный пуск означает запуск компьютера с выключенным питанием

CPU
Central processing unit, центральное процессорное устройство

CRC
Cyclic redundancy check, циклический контроль избыточности

D

DC
Diagnostic coverage, диагностическое покрытие
Часть возможных опасных отказов λD, деленная на отказы, обнаруженные диагностикой, и отказы, оставшиеся необнаруженными.
$\lambda_D = \lambda_{DD} + \lambda_{DU}$
Диагностическое покрытие (DC) определяет часть опасных отказов, которые были обнаружены.
$\lambda_{DD} = \lambda_D$. DC
$\lambda DU = \lambda_D (1 - DC)$
Определение может быть также представлено в виде следующего уравнения, где DC – диагностическое покрытие, λ_{DD} – вероятность обнаруженных опасных отказов, а λ_D total – вероятность всех опасных отказов:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

DDT
Derived data type, тип производных данных
Данные производного типа назначается пользователем.

DFB
Derived function block, блок производной функции

DIO
Distributed input/output, распределенный ввод/вывод

DLL
Dynamic link library, динамически подключаемая библиотека

E

E/E/PES
Electrical/electronic/programmable electronic system, электрическая/электронная/программируемая электронная система

	Система контроля, защиты или наблюдения на основе одного или нескольких электрических/электронных/программируемых электронных (E/E/PE) устройств. Сюда включены все элементы системы, такие, как источники питания, датчики и другие устройства ввода, магистральные шины данных и другие каналы связи, а также пускатели и другие устройства вывода.
EDT	Elementary data type, элементарный тип данных Элементарный тип данных назначается заранее.
EF	Elementary function, элементарная функция
EFB	Elementary function block, блок элементарной функции
EMC	Электромагнитная совместимость Термин относится к источнику, контролю и измерению электромагнитных влияний на электронные системы.
EN	European Norm, Европейская норма Официальный европейский стандарт.
ESD	Emergency shutdown, аварийная остановка
EUC	Equipment under control, оборудование под управлением Этот термин означает оборудование, механизмы обработки данных, инструментальные средства или предприятия, используемые для производства, обработки, транспортировки, медицинской или другой деятельности.

F

FBD	Functional block diagram, функциональная блок-схема Язык программирования IEC 61131-3 для пользовательской логики ПЛК.
FFB	Function/function block, функция/функциональный блок
FMEA	Failure modes and effects analysis, анализ типов характера и последствий отказов
FMECA	Failure modes and effects criticality analysis, виды отказа и анализ критичности эффектов
functional safety, функциональная безопасность	Система определяется как функционально безопасная, если выборочные, систематические и общепричинные отказы не приводят к ложному срабатыванию системы и не вызывают травмы или смерть людей, повреждение оборудования и потерю оборудования или продукции: • Функциональная безопасность относится к части общей безопасности, которая зависит от правильного функционирования системы, связанной с обеспечением безопасности.

	• .Функциональная безопасность применяется к изделиям, а также к организациям.

H

HALT	High accelerated life tests, высокоускоренные испытания на долговечность
HFT	Hardware fault tolerance, коэффициент отказоустойчивости Коэффициент отказоустойчивости N означает, что N + 1 отказов могут вызвать потерю функции безопасности, например: • HFT = 0: 1-й отказ может вызвать потерю функции безопасности • HFT = 1: 2 отказа в сочетании могут вызвать потерю функции безопасности. (Существует два пути к безопасному состоянию. Потеря функции безопасности означает, что безопасное состояние не может быть введено.)
HMI	Human-machine interface, человеко-машинный интерфейс
HSBY	Hot Standby, горячий резерв

I

IEC	International Electrotechnical Commission, Международная электротехническая комиссия
IEC 61508	Стандарт IEC 61508 является международным стандартом, который разрабатывает функциональную безопасность электрических/электронных/программируемых электронных систем, связанных с обеспечением безопасности. Он применяется к любой системе, связанной с безопасностью, в любой отрасли промышленности, где нет стандартов на продукты.
IL	Instruction list, язык списка инструкций Язык программирования IEC 61131-3 для пользовательской логики ПЛК.

L

LCD	Liquid crystal display, жидкокристаллический индикатор
LD	Ladder diagram, язык лестничной логики

	Язык программирования IEC 61131-3 для пользовательской логики ПЛК.

M

MTBF	Mean time between failures, среднее время наработки на отказ
MTTF	Mean time to failure, средняя наработка до отказа
MTTR	Mean time to repair, средняя наработка до ремонта

N

NFPA	National Fire Protection Association, Национальная ассоциация пожарозащиты Стандарт США для пожарозащиты.
Модули, не влияющие на уровень безопасности	Модули, не влияющие на уровень безопасности – это модули, которые не используются напрямую для управления функцией безопасности. Они не мешают модулям безопасности (как во время обычной работы, так и при отказе).

P

PELV	Protected extra low voltage, защищенное сверхнизкое напряжение
PES	Programmable electronic system, программируемая электронная система Система контроля, защиты или наблюдения, основанная на одном или нескольких программируемых электронных устройствах, включая элементы системы, такие, как источники питания, датчики и другие устройства ввода, магистральные шины данных и другие каналы связи, а также пускатели и другие устройства вывода. PES является другим термином автоматизированной системы управления или ПЛК.
PFD	Probability of failure on demand, вероятность отказа (по требованию)

Для одноканальной системы средняя вероятность отказа по требованию вычисляется следующим образом:

$$PFD(t)_{Av} = \frac{1}{2} \lambda_{DU} \bullet t$$

Для двухканальной системы средняя вероятность отказа по требованию вычисляется следующим образом:

$$PFD(t)_{Av} = \lambda_{DUCH1} \bullet \lambda_{DUCH2} \bullet t^2 + CC$$

Для двухканальной системы должен также учитываться эффект общей причины. Значение эффекта общей причины лежит в диапазоне от 1% до 10% PFD_{CH1} and PFD_{CH2}.(=1/RRF).

PFH Probability of failure per hour, вероятность отказа в час

ПЛК Programmable logic controller, программируемый логический контроллер (ПЛК)

проект Проект – пользовательское приложение в Unity Pro XLS.

Периодичность контрольных испытаний Периодичность контрольных испытаний – это интервал времени между контрольными испытаниями. Контрольные испытания – это периодические испытания, выполняемые для обнаружения отказов в системе, связанной с обеспечением безопасности с тем, чтобы при необходимости система могла бы быть восстановлена в подобное новое состояние или близкое к обычному для этого состояния.

PRT PLC reaction time, время отклика ПЛК
Время отклика ПЛК – это время, которое проходит между обнаружением сигнала на терминале входного модуля и откликом, установленном на терминале выходного модуля.

PS Power supply, Питание

PST Process safety time, безопасная продолжительность процесса
Безопасная продолжительность процесса определяется как период времени между отказом, произошедшим в EUC (Equipment Under Control, оборудование под контролем) или системой контроля EUC (с потенциалом для порождения опасного события) и присутствием опасного события, если функция безопасности не выполняется. (Источник: IEC 61508, часть 2, 7.4.3.2.5)

Q

QSE Qnvironment system qualification, оценка среды системы

R

RAM Random access memory, ОЗУ

RIO Remote input/output, удаленный ввод/вывод

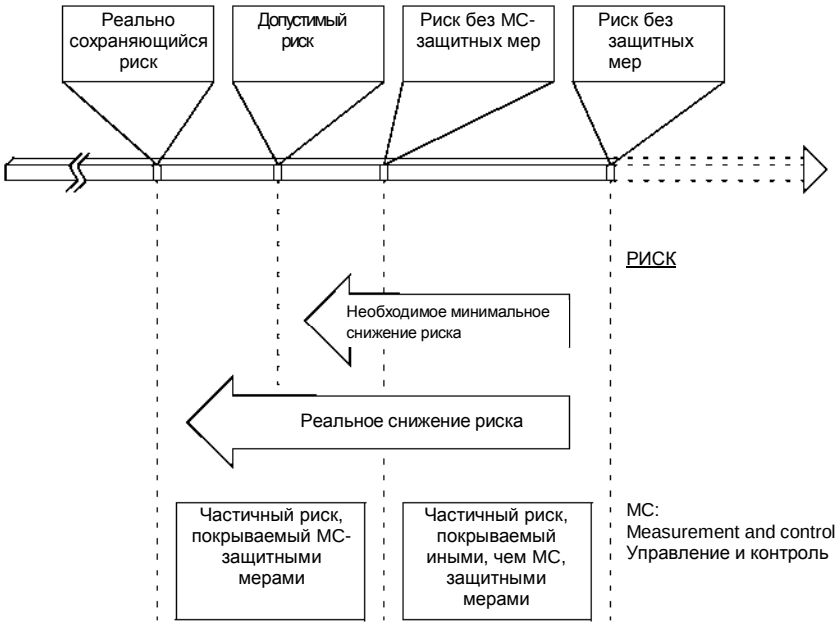
Риск Риск – это комбинация вероятности возникновения ущерба и его серьезностью.
Риск вычисляется с помощью уравнения: R=S*H
где

Буква	Описание
R	Риск
S	Степень ущерба
H	Частота возникновения ущерба

RM Requirements management, контроль исходных требований

RRF Risk reduction factor, коэффициент снижения риска

Коэффициент снижения риска равен 1/PFD.



Часы реального времени (RTC) Real-time clock, часы реального времени

S

система, связанная с обеспечением безопасности Этот термин обозначает систему, которая
- выполняет требуемые функции безопасности, необходимые для достижения или поддержки безопасного состояния для EUC и
- предназначена для достижения, по-своему или с помощью других электрических/электронных/программируемых электронных систем, связанных с обеспечением безопасности, или средств снижения внешнего риска, необходимой эксплуатационной безопасности для требуемых функций безопасности.

SFC Sequential function chart, язык последовательных функций
Язык программирования IEC 61131-3 для пользовательской логики ПЛК.

SFF Safe failure fraction, коэффициент безопасных отказов

SFR Safety functional requirement, функциональное требование безопасности
Функциональные требования безопасности получаются из анализа опасности и определяют, что функция делает, например, функцию безопасности, которая должна быть выполнена.

SIL Safety integrity level, уровень эксплуатационной безопасности
Дискретный уровень (1 из возможных 4) для определения требований эксплуатационной безопасности, который должен быть назначен электрическим/электронных/программируемых электронным системам, связанных с обеспечением безопасности, где уровень эксплуатационной безопасности 4 является высшим, а уровень 1 – низшим.
Эксплуатационная безопасность – это вероятность систем, связанных с обеспечением безопасности, удовлетворительно выполнять требуемые функции безопасности при всех заявленных условиях в заданном интервале времени.
Ниже определены **4 уровня**:
- уровень 4: защита оборудования и общества (ядерная)
- уровень 3: защита людей
- уровень 2: защита собственности и производства
- уровень 1: защита предприятий

SIR Safety integrity requirement, требование эксплуатационной безопасности
Требования эксплуатационной безопасности получаются из оценки риска и описывают правдоподобие удовлетворительно выполняемой функции безопасности, например, уровень степени, необходимой для проведения функции безопасности.

SRS Safety requirements specification (IEC 61508), system requirements, характеристики требований безопасности (IEC 61508), системные требования Функциональное описание высокого уровня системы безопасности.

SSC System safety concept, концепция системной безопасности
Подробное описание системной архитектуры, конфигурации и средств диагностики, требуемых для достижения функциональной безопасности.

St Structured text, структурированный текст
Язык программирования IEC 61131-3 для пользовательской логики ПЛК.

T

TÜV Technischer Überwachungsverein
(Ассоциация технической инспекции (нем.))

U

UMA Unrestricted memory area, свободная область памяти
Особо выделенная область памяти для битов и слов, которые не защищены от записи.

V

VDE Verband Deutscher Elektroingenieure
Германский аналог IEEE.

W

горячий пуск Горячий пуск означает перезапуск компьютера без выключения питания.