Сетевые многофункциональные контроллеры

С.Л. РОГОВ, А.А. СТЕПАНОВ, В.В. ДЬЯЧЕНКО (ООО "ТРЭИ ГмбХ")

Выбор аппаратных средств автоматизации для построения систем безопасности промышленных объектов

Предлагается информация о российском оборудовании, прошедшем процедуру сертификации в центре T‹ V, которое может быть использовано для построения систем противоаварийных защит и блокировок.

The paper informs about Russian equipment certified by T‹ V that can be used in anti-wreck protection and interlock logic.

Общая характеристика нормативной базы

В настоящее время в России не существует единой нормативной базы, регламентирующей требования к заказчику, проектировщику и инжиниринговой организации по выбору технических средств построения систем безопасности промышленных объектов.


BESCHEINIGUNG

Сразу акцентируем внимание читателя на том, что построение системы безопасности опасных промышленных объектов не ограничивается только мероприятиями, связанными с обеспечением взрывобезопасности применяемого оборудования.

Существуют не связанные друг с другом нормативные документы Ростехрегулирования, Ростехнадзора, Госпожнадзора, отраслевые документы РАО ЕЭС, Газпрома, корпоративные стандарты крупных компаний, таких как ТНК ВР, Сургутнефтегаз и др.

- Ростехрегулирование обязывает собственника опасного объекта, при наличии измерительных приборов в составе системы безопасности, провести испытания для утверждения типа измерительной системы и зарегистрировать его в Государственном реестре средств измерений.
- Ростехнадзор обязывает провести экспертизу проекта и применять технические средства, разрешенные к применению в соответствии с категорией опасности объекта.
- Госпожнадзор также обязывает провести экспертизу проекта и применять технические средства пожарного контроля и пожаротушения, разрешенные к применению.
- Отраслевые нормативные документы акционерных компаний, как правило, имеют юридически выверенные ссылки на государственные нормативные документы в сфере их компетенции, но в отличие от последних пытаются дополнить требованиями, вытекающими из специфики их производств, требований собственника, опыта применения импортного оборудования, опыта общения с системными интеграторами зарубежных фирм.

Примером могут служить руководящие документы РАО ЕЭС [1] и [2]. В перечисленных документах сформулированы требования к структуре систем, сетевой организации, резервированию контроллерного оборудования. К требованиям данных РД привыкли и проектанты, и системные интеграторы, и руководители, и технические специалисты служб ТАИ и АСУТП энергообъектов. Но в требованиях этих документов существует неопределенность в выборе способов и объемов резервирования технических средств, порождающая различные критерии в выборе технических средств.

Специалисты, разработчики корпоративных документов некоторых компаний, пошли еще дальше и внесли в требования по выбору оборудования обязательное соответствие средств автоматизации противоаварийных защит и блокировок требованиям европейского стандарта EN 61508 [3]. Они приводят классифицирование своих производственных объектов по уровням потенциальной опасности, в случае аварии: с 1-го по 8-й согласно DIN V 19250 [4] (классы опасности объектов 7-й и 8-й и соответствующий им уровень требований к оборудованию – SIL4 в данной статье не рассматриваются, это объекты ядерной энергетики, производства, утилизации ядерного и химического оружия. По этому роду деятельности существуют специальные нормативные документы Госатомнадзора и Минобороны).

Почему EN 61508?

В Еврозоне разработаны и функционируют стандарты, формирующие требования к оценке уровня потенциальной опасности объекта и оценке соответствия оборудования автоматизации систем безопасности уровню опасности объекта. В данной статье мы не будем подробно анализировать систему стандартизации безопасности Евросоюза, остановимся только на общих вопросах.

Стандарт, определяющий требования к электрическим/электронным/программируемым системам обеспечения безопасности (EN 61508), есть в библиотеке Госстандарта на английском языке, объем этого документа

www.asucontrol.ru

вместе с приложениями около 600 печатных листов. В таком виде он находится в библиотеке уже 5 лет, и перспектив его перевода на русский язык по инициативе Госстандарта не видно. Но зона действия этого стандарта (с переводом его на национальные языки) подошла уже к границам России. Вступление Прибалтики в Евросоюз, начавшийся процесс гармонизации национальных стандартов Украины, Казахстана и других республик бывшего СССР обуславливают интерес к этому документу и у отечественных системных интеграторов и собственников опасных объектов.

Последние 5 лет активной работы фирмы TREI на рынках автоматизации СНГ, Балтии, Польши привели к необходимости сертификации производимого фирмой оборудования на соответствие мировым стандартам качества и безопасности.

Практически все тендеры, в которых нам приходится участвовать на объектах нефтехимии, нефтегазодобычи, энергетики и др. отраслей, проходят с участием ведущих мировых фирм-производителей оборудования автоматизации. Собственники объектов также в ряде случаев иностранцы. Эти два обстоятельства предопределяют наличие в тендерных требованиях к поставляемому оборудованию обязательной сертификации оборудования на соответствие мировым стандартам в общепризнанных мировых лабораториях и испытательных центрах. Именно по этим причинам фирма TREI первой из Российских производителей средств автоматизации провела сертификацию контроллеров серии TREI-5B:

- 2002 г. – сертификация в двух испытательных Европейских центрах на соответствие нормам 73/23/EEC [5], 89/336/EEC [6], 93/68/EEC [7], 93/465/EEC [8] и получила право маркировки продукции знаком CE;
- 2004 г. – сертификация в немецком центре T‹ V на соответствие требованиям Европейских стандартов оборудования для взрывоопасных производств, EN 50014 [9], EN 50020 [10];
- 2006 г. – сертификация в немецком центре T‹ V на соответствие требованиям стандарта для оборудования автоматизации систем безопасности промышленных объектов, EN 61508.

Критерии выбора уровня опасности оборудования системными интеграторами и собственниками опасных объектов

Приведем основные критерии выбора по степени их релевантности.

1. На данное предприятие ранее поставлялось оборудование иностранного производителя с обозначенным уровнем опасности.

2. Аналогичную по уровню опасности технологию для данного предприятия проектировала иностранная фирма и в проектных документах указывала уровень опасности.

3. Иностранный собственник, опираясь на национальные стандарты и опыт использования аналогичного оборудования, определял экспертным или расчетным способом уровень опасности.

4. Специалисты предприятия информировались о существовании уровней опасности.

5. Отечественный проектировщик технологии в описательной части проекта указывал предполагаемый или расчетный класс опасности производства и соответствующий уровень оборудования.

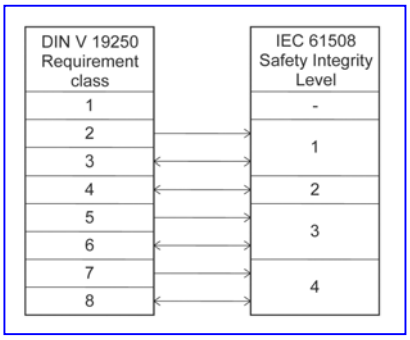

Рис. 1. Соответствие между классом опасности по DIN V 19250 и уровнем безопасности по IEC 61508

6. Проектный отдел предприятия проводил анализ производственных объектов и ранжировал их по классу опасности. Полный перевод стандарта EN 61508 или выдержки из него внесены в стандарт предприятия.

Анализ показывает, что два последних критерия являются наиболее правильными и, к сожалению, наиболее редкими при выборе оборудования. Как же поступить проектировщику или собственнику промышленного объекта? Специалисты фирмы TREI оказывают заказчику услуги по определению класса опасности объекта и правильному подбору средств автоматизации на базе широкой номенклатуры оборудования собственного производства. Как указывалось выше, практически все производственные объекты, в том числе объекты тепловой энергетики, по уровню потенциальной опасности могут обслуживаться оборудованием уровня SIL3. Таким образом, беспроигрышный вариант – это применение для автоматизации контроллеров TREI-5B-02(04) в сертифицированной для этого уровня опасности конфигурации – 100 % резервированная структура контроллера.

Опираясь на опыт сертификации, можно утверждать, что затраты на экспертное обследование объекта сертифицированным центром (по имеющейся у авторов информации, ни один из Российских центров не имеет такой аккредитации, поэтому в качестве сертифицированного центра могут выступать только Европейские лаборатории) намного превышают возможные финансовые потери из-за увеличения стоимости оборудования при выборе уровня опасности более высокого, чем реальный. Например, экспертиза оценит часть технологии по классу опасности 6 – уровень оборудования SIL3, часть по классу 4 – уровень оборудования SIL2 и часть технологии по классу 2 – уровень оборудования SIL1. То есть, применяя оборудование уровня SIL3, вы экономите на экспертизе и гарантированно обеспечиваете безопасность объекта. Для того чтобы у читателя не возникало путаницы между терминами “класс опасности производства, технологии, объекта” и “уровень требований к оборудованию обеспечения безопасности”, приведем рисунок соответствия (рис. 1). Направление стрелок указывает однозначность соответствия.

www.asucontrol.ru

Требования к оборудованию автоматизации уровня SIL3

Приведем основные требования к оборудованию на примере контроллера TREI-5B-02 с комментариями.

1. Дублирование 100 % контроллеров, для систем с контурами регулирования допускается 100 % резервирование.

Комментарии: прежде всего, отметим, что дублирование подразумевает одновременное, активное выполнение функций контроллера. Дублирование может быть синхронное и асинхронное. Резервирование подразумевает, что активным в данный момент времени может быть только основной контроллер, только он может выполнять управляющие воздействия на объект; резервный контроллер ведет опрос входных каналов и по каналу межконтроллерной связи производит зеркализацию базы данных основного контроллера. Зеркализация необходима для безударного перехода регуляторов с основного контроллера на резервный. Примеры реализации дублирования (рис. 2) и резервирования (рис. 3).

2. Дублирование 100 % магистралей передачи данных между составными частями контроллера.

Комментарии: в связи с тем, что контроллер TREI-5B-02 имеет сетевую структуру передачи данных между составными частями контроллера, задача дублирования магистралей передачи данных решается дублированием внутреннего межмодульного интерфейса ST-BUS. Физически – это дублированный RS-485 (2,5 MBod), по протоколу – это ModBus с добавлением функций определения повреждения линии и взаимного контроля. Данное решение позволяет создавать распределенную систему с соблюдением требований дублирования магистралей передачи данных (рис. 4).

3. Контроль достоверности передачи данных между составными частями контроллера.

Комментарии: все процедуры передачи данных в контроллере осуществляются с программно-аппаратным контролем достоверности. В случае обнаружения ошибки контроллер до 3 раз повторяет процедуру и в специальных, доступных оператору регистрах ведет статистику ошибок для принятия решений о правильности выбора скорости передачи данных и технологии прокладки кабеля связи.

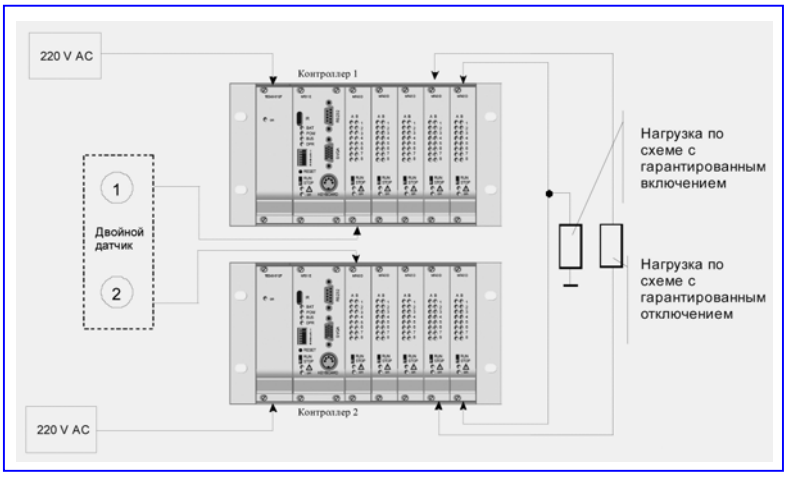

Рис. 2. Структура системы на базе контроллера TREI-5B-02 со 100 % дублированием

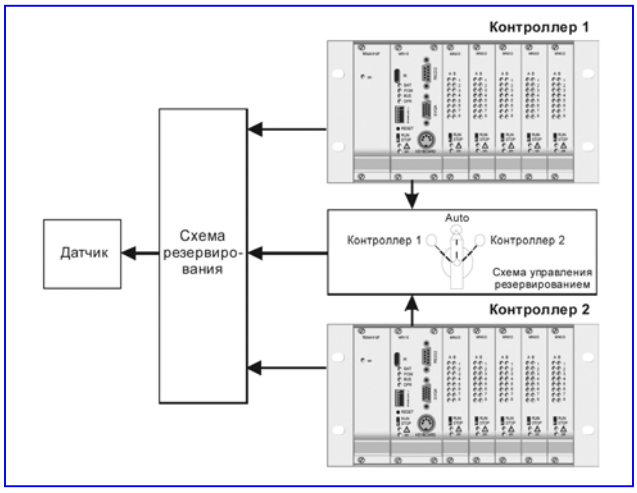

Рис. 3. Структура системы на базе контроллера TREI-5B-02 со 100 % резервированием

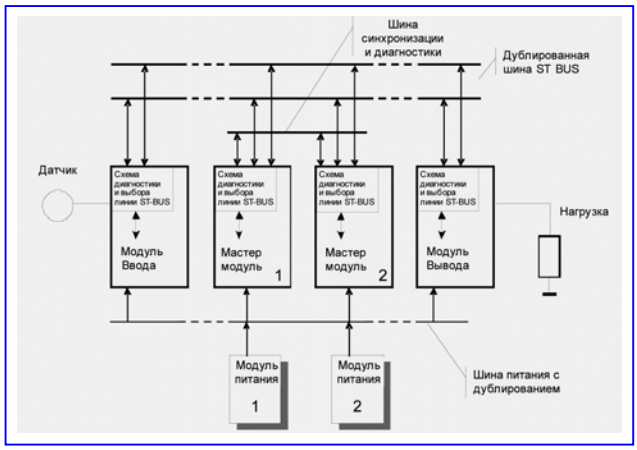

Рис. 4. Структура системы на базе контроллера TREI-5B-02 с дублированием 100 % магистралей передачи данных

4. Диагностика аппаратного отказа всех функциональных частей контроллера, в т.ч. любого из каналов ввода/вывода.

Комментарии: диагностика аппаратных отказов является одним из самых важных критериев, определяющих выбор аппаратных средств. Важно не только само наличие диагностики (что декларируется многими производителями средств автоматизации) визуальной или звуковой. Важно наличие программного анализа диагностики, наличие возможности расстановки приоритетов и уровней критичности, обнаруженных ошибок для принятия решения процессорным модулем (мастер-модулем) о невозможности продолжения работы, выдачи диагностического сигнала резервному контроллеру и перевода в неактивное состояние всех управляющих модулей.

5. Аппаратная индикация неисправности функциональной части контроллера.

Комментарии: данное требование реализовано на всех функциональных модулях контроллера TREI-5B-02. Реализована не только обобщенная светодиодная индикация неисправного модуля, но и индикация

www.asucontrol.ru

неисправности каждого канала ввода/вывода, применяемого в системах безопасности.

6. Перекрестная диагностика контроллерами состояния работоспособности.

Комментарии: согласно требованиям стандарта, каждый из работающих контроллеров должен иметь информацию о состоянии дублирующего или резервного контроллера. Например: в системе блокировок и защит применены контроллеры TREI-5B-02 в режиме дублирования. Каждый из контроллеров независимо друг от друга проводит анализ работоспособности своих модулей, интерфейса и процессорного модуля и формирует информационное слово состояния аппаратной части контроллера. Это слово передается по межконтроллерному интерфейсу в дублирующий контроллер, и таким же образом принимается слово состояния дублирующего контроллера. Имея данную информацию, каждый из контроллеров передает ее на верхний уровень и самостоятельно анализирует полученную информацию. В случае, если по результатам анализа вырабатывается признак о том, что дублирующий контроллер не в состоянии полноценно выполнять свои функции, выдается информационное сообщение на верхний уровень и включается квитируемая оператором сигнализация о том, что система потеряла функции дублирования. Кроме перекрестного информационного контроля состояния, в контроллерах TREI-5B-02 осуществляется формирование аппаратного сигнала состояния контроллера, независимого от работоспособности процессорного модуля и работоспособности межконтроллерного обмена, который также перекрестно контролируется как в режиме дублирования, так и в режиме резервирования (рис. 5).

7. Диагностика обрыва, короткого замыкания линий связи с датчиками и исполнительными механизмами.

Комментарии: в номенклатуре модулей контроллера TREI-5B-02 имеется большое количество модулей ввода/вывода, но только часть из них обладает необходимыми для систем безопасности характеристиками. Это связано с желанием разработчиков контроллера максимально удовлетворить потребителя и в случаях неответственных применений сделать контроллер максимально доступным по цене. Требованиям стандарта удовлетворяют модули:

- аналогового ввода/вывода с функциями контроля безобрывности и короткого замыкания линии связи;
- дискретного ввода с контролем обрыва и короткого замыкания линии связи;
- дискретного вывода с контролем исправности ключевого элемента и постоянной проверкой его исполнительных функций без подачи управления в нагрузку, постоянного контроля безобрывности и короткого замыкания нагрузки.

Эти модули являются наиболее ответственными элементами и подвергаются специальным испытаниям в процессе сертификации.

8. Обеспечение невозможности вследствие ошибочных действий персонала изменения аппаратной и программной конфигураций контроллера.

Комментарии: данное требование состоит из нескольких частей, перечислю их и на примере контроллера TREI-5B-02 кратко опишу способы их реализации:

- невозможность изменения программной конфигурации. Реализация: в программе конфигурации после завершения процедуры программной компоновки контроллера пользователь при помощи пароля закрывает возможность ее несанкционированного изменения;
- невозможность случайной перестановки модулей в каркасе контроллера. Реализация: все модули контроллера имеют аппаратный, механический ключ-код установки, данный ключ для систем безопасности устанавливается производителем, и пользователю по его запросу дается специальная инструкция по его модификации. Наличие данного ключа делает невозможным установку модуля на “не свое” место в каркасе контроллера, тем самым страхует систему от ошибочных действий персонала;
- невозможность несанкционированного изменения аппаратной конфигурации модулей ввода/вывода. Реализация: даже если в модуле контроллера TREI-5B-02 совпадает механический ключ-код, но была изменена аппаратная конфигурация модуля (произведена несанкционированная замена мезонинов, изменены метрологические уставки каналов и др.), после установки модуля в каркас контроллера мастер-модуль сравнит конфигурацию установленного модуля с конфигурацией в своей базе данных и в случае несовпадения выдаст диагностическое сообщение и включит аппаратную индикацию; квитировать это сообщение можно специальными действиями оператора, подтверждающими санкционированность замены.

9. Обеспечение “горячей замены” модулей контроллера.

Комментарии: каждый из заменяемых модулей контроллера должен иметь возможность изъятия и замены без остановки программы и выключения питания, контроллер TREI-5B-02 различает ситуации изъятия модуля и его отключения или выхода из строя, при произведении процедуры изъятия в мастер-модуль посылается специальное диагностическое сообщение. В контроллере применены специальные аппаратные решения, позволяющие плавно подавать напряжение на вновь устанавливаемый модуль, что повышает надежность работы всего контроллера в целом. В “горячем” режиме можно производить замену, в том числе и мастер-модуля (предварительно переведя его в неактивное состояние, режим “Stop”), и блоков питания, без опасения кратковременных изменений характеристик питания.

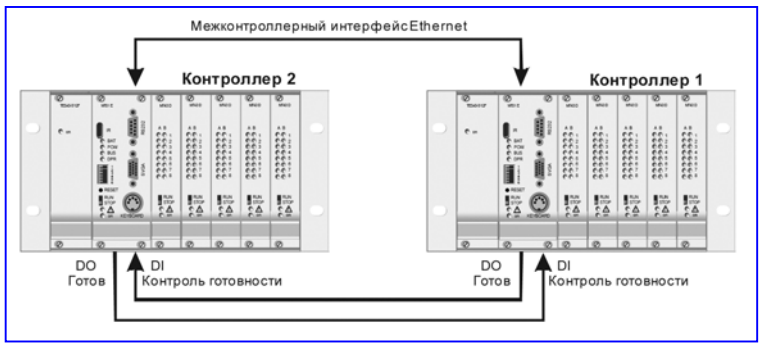

Рис. 5. Структура системы на базе контроллеров TREI-5B-02 с перекрестной диагностикой состояния работоспособности

www.asucontrol.ru

10. Обеспечение метрологических характеристик дублируемых измерительных каналов.

Комментарии: отличительной особенностью контроллеров серии TREI-5B является наличие сертифицированных схем дублированных и резервированных измерительных каналов, что не реализовано ни в одном из отечественных контроллеров и в большей части импортных. В методике поверки контроллеров есть специальный режим проверки метрологических характеристик аналоговых каналов при параллельном или последовательном подключении каналов к источникам сигнала. Многие даже не задаются вопросом, что точность измерения при таком подключении меняется. Поэтому разработчиками контроллера были применены специальные методы обеспечения точности и методики ее проверки.

11. Обеспечение характеристик взрывозащиты дублируемых измерительных каналов и каналов дискретного ввода/вывода.

Комментарии: предметом особой гордости фирмы TREI является наличие в составе контроллеров встроенных искробезопасных каналов, что позволяет создавать полноценные системы безопасности в режиме дублирования каналов. Приведем пример стандартной схемы дублирования (резервирования) с использованием контроллера с общепромышленными цепями ввода/вывода и внешним барьером искрозащиты (рис. 6).

В данной структуре мы видим, что усилия по созданию резервированной структуры сводятся на нет наличием общего для резервируемых цепей барьера искрозащиты. Включение по схеме (рис. 7) недопустимо, т.к. это меняет энергетические параметры цепи и требует специальных измерений и разрешений производителя барьера. В стандартных рекомендациях по

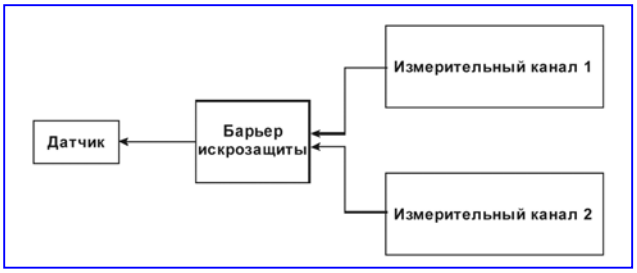

Рис. 6. Стандартная схема дублирования (резервирования) с использованием контроллера с общепромышленными цепями ввода/вывода и внешним барьером искрозащиты

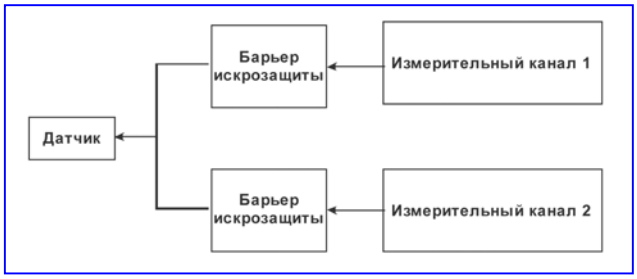

Рис. 7. Схема дублирования (резервирования) с использованием контроллера с общепромышленными цепями ввода/вывода и внешними барьерами искрозащиты

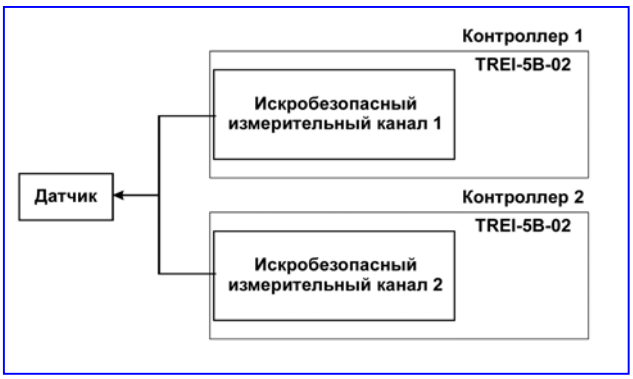

Рис. 8. Схема дублирования (резервирования) с использованием контроллера TREI-5B-02 с встроенными искробезопасными измерительными каналами

использованию барьеров искрозащиты такое включение не предусмотрено.

В отличие от двух ранее рассмотренных вариантов включения контроллер TREI-5B-02 позволяет производить резервирование искробезопасных каналов ввода/вывода без дополнительных технических “премудростей” (рис. 8). Схемы резервированного и дублированного включения прошли специальные испытания и сертификацию и подтверждены Российским сертификатом и сертификатом T‹ V.

Достаточность соблюдения требований

Казалось бы, требования известны, достаточно производителю приложить усилия к их программной и аппаратной реализации и можно де-факто декларировать соответствие своей продукции. Но это не так.

Сертификация в пользующемся мировой известностью и авторитетом центре T‹ V ñ это целый комплекс испытаний и процедур, проведение которых гарантирует потребителю получение продукции с гарантированными характеристиками и качеством.

Приведем лишь основные этапы сертификации, которые фирма TREI прошла за 2 года напряженной работы со специалистами испытательного центра.

- Предоставление всей информации о производственной структуре фирмы.
- Отчет о наличии сертифицированных поставщиков комплектующих.
- Свидетельство о сертификации системы качества производителя в системе стандартов ISO 9000.
- Проведение внешнего аудита специалистами центра системы качества предприятия.
- Предоставление экспертам центра принципиальных схем и конструкторской документации на сертифицируемое оборудование с расчетами всех электрических, тепловых и динамических параметров схем.
- Предоставление общих технических заданий и частных технических заданий на функциональные модули оборудования и все функциональные модули программного обеспечения.

www.asucontrol.ru

- Предоставление актов и протоколов испытаний независимых лабораторий на соответствие требований МЭК на данный вид продукции.
- Предоставление и совместный аудит актов и протоколов испытаний аппаратных и программных средств.
- Предоставление исходных текстов и описаний используемого программного обеспечения.
- Корректировка схемных, конструкторских и программных решений по замечаниям специалистов центра сертификации.
- Разработка и изготовление тестовой системы на базе контроллера TREI-5B-02 обеспечения безопасности промышленного объекта. Тестовая система должна обеспечивать возможность внесения преднамеренных разрушающих и неразрушающих воздействий на систему с целью проверки всех требований по диагностике и резервированию функций системы.
- Передача системы в сертификационный центр в Германию и проведение испытаний экспертами центра без присутствия специалистов производителя.
- Согласование технического отчета о проведении испытаний и выдача сертификата.

Выводы

1. Использование в системах автоматизации опасных производств оборудования, сертифицированного на соответствующий уровень опасности, является необходимым, но не достаточным условием. Из сказанного выше, читатель понял, что обязательным является соблюдение определенных компоновочных требований и архитектурных решений при создании системы. Именно поэтому в сертификатах на оборудование фирма T‹ V пишет, что построение систем безопасности на базе сертифицированной техники должно производиться изготовителем (заявителем) оборудования или другой фирмой, прошедшей обучение и получившей специальное разрешение изготовителя на право построения систем безопасности с применением ее техники. Фирма TREI на базе производственного предприятия в г. Пенза проводит обучение специалистов фирм-проектантов, эксплуатационников, системных интеграторов для ознакомления их с требованиями при построении систем безопасности на базе средств автоматизации, выпускаемых фирмой TREI.

2. Обязательным условием применения сертифицированной техники является применение программного обеспечения, на базе которого эта техника проходила сертификацию. Современные контроллеры (и контроллеры фирмы TREI не исключение) позволяют работать с ними на разных программных платформах с применением целевых задач разных производителей, но системы безопасности можно строить только с применением сертифицированного ПО. Производитель средств автоматизации должен предоставить пользователю весь набор библиотечных функций, обеспечивающий выполнение требований стандарта. В противном случае производитель не имеет права маркировать свою продукцию знаком соответствия уровню опасности.

3. Наличие у программируемого контроллера сертификата на соответствие оборудования уровню опасности не означает, что пользователь может применять данное оборудование в любой комплектации из всей номенклатуры модулей данного контроллера. Сертификацию и разрешение на применение проходит конкретный набор модулей в конкретной компоновке.

4. Построение систем автоматизации опасных объектов – комплексная задача. Здесь смыкаются интересы нескольких надзорных органов, в сферу деятельности которых входит обеспечение безопасности в пределах предоставленной им компетенции. Именно поэтому фирма TREI, единственная из отечественных производителей средств автоматизации, разработала и поставляет на рынки России, центральной Азии и стран восточной Европы технику, сертифицированную по всем направлениям обеспечения безопасности. А именно:

- контроллеры TREI-5B-02(04), сертифицированные на соответствие требования уровня SIL3 опасности промышленных объектов;
- контроллеры TREI-5B-02(04), сертифицированные для применения на взрывоопасных производствах с видом взрывозащиты Exia IIC;
- приборы приемно-контрольные управления пожаротушением на базе контроллеров TREI-5B, сертифицированные для пожарного и охранного контроля и активного пожаротушения объектов всех типов.

Сергей Львович Рогов – генеральный директор, Александр Александрович Степанов – начальник бюро электронного конструирования, Вера Владимировна Дьяченко – инженер-электронщик БЭК ООО "ТРЭИТ ГмбХ".
Телефоны: (8412) 55-58-90, 49-95-39, факс 49-85-13.
E-mail: trei@trei-gmbh.ru
http://www.trei-gmbh.ru

Список литературы

1. *РД* 153-34.1-35.137-00. Технические требования к подсистемам технологических защит, выполненных на базе микропроцессорной техники.
2. *РД* 153-34.1-35.127-2002. Технические требования к программно-техническим комплексам для АСУТП тепловых электростанций.
3. *EN* 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems.
4. *DIN* V 19250 Messen, Steuern, Regeln; Grundlegendo Sicherheits-Betrachtungen.
5. *73/23/EEC* Low voltage.
6. *89/336/EEC* Electromagnetic compatibility.
7. *93/68/EEC* Marking Directive.
8. *93/465 EEC* Marking Falsification Directive.
9. *EN* 50014 Electrical apparatus for potentially explosive atmospheres ñ General requirements.
10. *EN* 50020 Electrical apparatus for potentially explosive atmospheres ñ Intrinsic safety 'i'.

www.asucontrol.ru