ПРОТИВОАВАРИЙНАЯ ЗАЩИТА: ТЕОРИЯ, СТАНДАРТЫ И ПРАКТИКА ПОСТРОЕНИЯ СИСТЕМ НА ОСНОВЕ ПЛК

С.Л. Рогов (ООО "ТРЭИ ГМБХ")

Проводится анализ текущего состояния практики построения систем ПАЗ, выявляются несоответствия с ГОСТ Р МЭК 61508-2007. Предлагается структура системы ПАЗ, реализованной на ПЛК, удовлетворяющей требованиям стандарта функциональной безопасности электрических, электронных, программируемых электронных систем, связанных с безопасностью (ГОСТ Р МЭК 61508-2007).

Ключевые слова: контроллеры, системы безопасности, противоаварийные защиты.

Надежность функционирования систем обеспечения безопасности опасных объектов промышленности целиком зависит от состояния электронных и программируемых электронных систем, связанных с безопасностью. В соответствии с РД 153-34.1-35.137-00 "Технические требования к подсистеме технологических защит, выполненных на базе микропроцессорной техники" эти системы называются "системами блокировок и защит". Рассмотрим главные задачи, возлагаемые на такие системы:

- предотвращение аварий и минимизация последствий аварий – задача, возлагаемая на системы противоаварийной защиты (ПАЗ).

- блокирование (предотвращения) намеренного или ненамеренного вмешательства в технологию объекта, могущего привести к развитию опасной ситуации и инициировать срабатывание ПАЗ – задача системы блокировок.

В современных системах эти две задачи неразделимы, поэтому будем называть системы, решающие эти задачи, системами ПАЗ, что в терминах стандарта (ГОСТ Р МЭК 61508-2007. Функциональная безопасность электрических, электронных, программируемых электронных систем, связанных с безопасностью) обозначается E/E/EP, то есть системы, связанные с безопасностью.

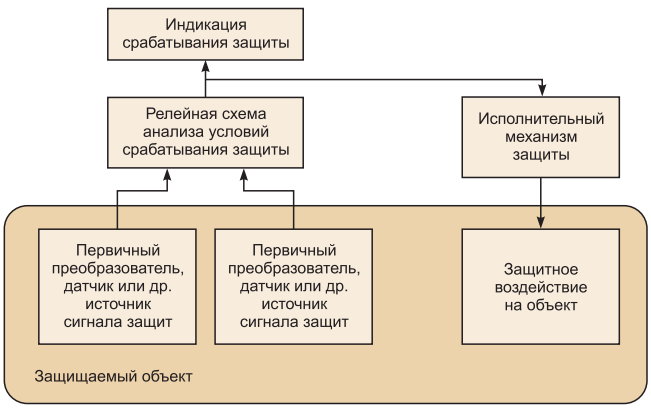

Рис. 1. Структура релейной системы ПАЗ

Главным критерием безопасности оборудования, применяемого в E/E/EP системах, является интегральный уровень безопасности SIL (Safety Integrity Level) (EN 954-1: 2001E). Самый низкий уровень безопасности – SIL1, самый высокий – SIL4.

Чтобы проанализировать текущее состояние систем ПАЗ, обратимся к истории развития сначала электрических, потом электронных и затем программируемых электронных систем ПАЗ. Они не случайно перечислены в ГОСТ Р МЭК 61508-2007 в последовательности своего эволюционного развития.

Первыми электрическими системами ПАЗ были релейные схемы защит, применяемые с начала XX века, и до сих пор работающие на многих отечественных объектах. Разработка и выпуск таких систем прекратились только в 60-е годы прошлого века. Функциональная структура системы релейной защитой представлена на рис. 1.

Массовое внедрение транзисторов и появление транзисторных логических элементов (электронные модули серии "Логика-Т") привело к удешевлению, снижению массы и значительному повышению надежности ПАЗ, но функционально эти системы остались аналогичными релейным. То же самое можно сказать и про внедрение в системы ПАЗ интегральных логических схем. До сих пор эти системы работают и обладают самой высокой надежностью, но функционально они также соответствуют релейным системам.

Основной недостаток релейных систем ПАЗ очевиден – это жесткая привязка схемы ПАЗ к конкретному объекту и конкретному набору датчиков и исполнительных механизмов защиты.

Следующим этапом развития систем ПАЗ стало внедрение в промышленность в 70-х годах XX века ПЛК (рис. 2). Возможность реализации на базе одного ПЛК нескольких зависимых и независимых схем и алгоритмов защиты позволила в разы улучшить массогабаритные характеристики ПАЗ, но поставила надежность всей системы ПАЗ в зависимость от одного вычислителя (процессорного модуля контроллера) и

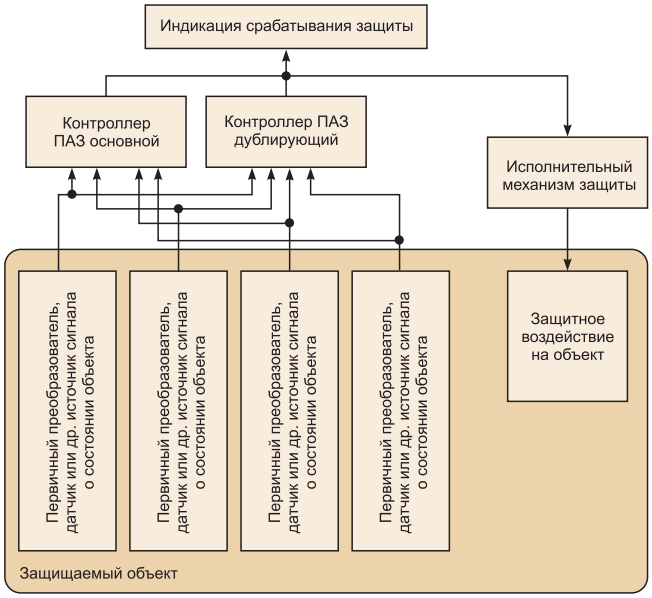

Рис. 2. Структура дублированной, контроллерной системы ПАЗ

прикладной программы. Именно на этой стадии развития систем ПАЗ было применено дублирование, а впоследствии и резервирование контроллеров.

Развитие контроллерных интерфейсов, появление электронных систем отображения информации, SCADA-систем и внедрение модульного принципа построения ПЛК привело к трансформации структуры контроллерной ПАЗ в привычную для специалистов структуру (рис. 3). Основной особенностью таких систем стала интеграция ПАЗ в АСУТП объекта управления как составной части информационно-управляющей структуры.

Реальные АСУТП, интегрированные с ПАЗ, могут отличаться составом ПЛК, числом станций оператора, наличием серверов, архивных станций, сложного интерфейса верхнего уровня и др., но по функции безопасности эти системы можно привести к структуре, изображенной на (рис. 3).

Проанализируем структуру системы ПАЗ (рис. 3) и выявим ограничения и несоответствия с требованиями стандарта ГОСТ Р МЭК 61508-2007.

1. *Сложность верификации алгоритмов ПАЗ.* В одном контроллере (дублированном) объединены все схемы и алгоритмы защит и блокировок объекта. Это приводит к необходимости перепроверки всех схем и алгоритмов при изменении в одном из них или при замене типа датчика или исполнительного механизма.

2. *Наличие в процессорном модуле контроллера ПАЗ ОС*, что значительно упрощает процесс разработки целевых задач процессора и приложений пользователя. С другой стороны, наличие ОС повышает инвариантность реакции логических и вычислительных алгоритмов на тестовое воздействие, проводимое при проверке ПАЗ. Иными словами, представитель надзорной организации, проводя проверку, руководствуется тестовыми комбинациями входных сигналов ПЛК, которые составлялись для релейных или электронных схем. Такая проверка не может дать гарантии повторяемости результатов тестов, так как состояние памяти процессора под управлением ОС при всех одинаковых условиях тестирования не будет одинаково в разные моменты времени. В подтверждение этого вывода в таблице приведен перечень ограничений для ПО ПЛК (ГОСТ Р МЭК 61508-2007. Ч. 3. с.34).

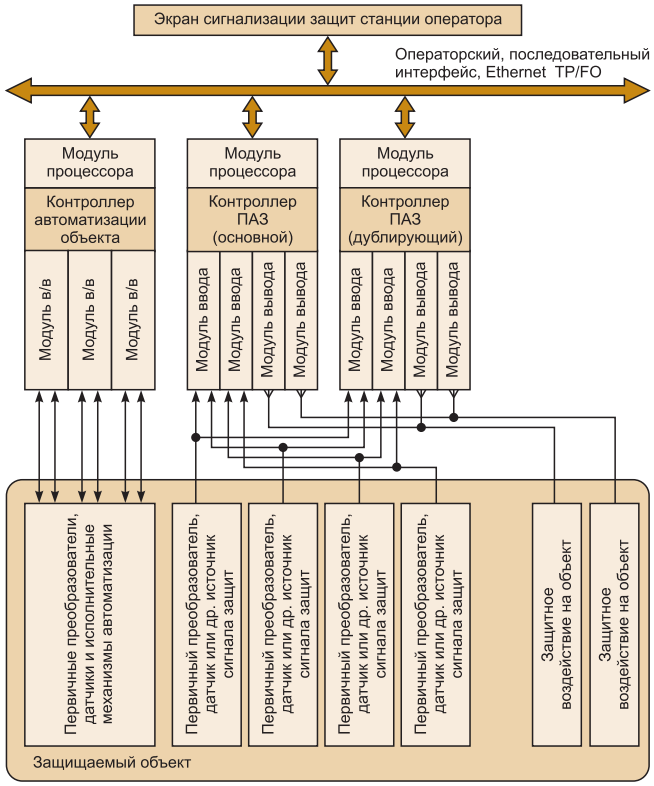

Рис. 3. Структура контроллерной, дублированной, модульной системы ПАЗ, интегрированной в АСУТП

Таблица

Метод/средство	Уровень безопасности SIL			
	SIL1	SIL2	SIL3	SIL4
1. Использование стандартов кодирования	HR	HR	HR	HR
2. Не использовать динамические объекты	—	HR	HR	HR
3. Не использовать динамические переменные	—	R	HR	HR
4. Ограничение использование прерываний	R	R	HR	HR
5. Ограничение использования указателей	—	R	HR	HR
6. Ограничение использование рекурсии	—	R	HR	HR
7. Не использовать безусловные переходы в программах, написанных на языках высокого уровня	R	HR	HR	HR
- R уровень независимости, определяемый как рекомендуемый - HR уровень независимости, определяемый как настоятельно рекомендуемый				

3. *Сложность подтверждения надежности.* Основным критерием безопасности систем E/E/EP и ПАЗ является интенсивность отказов λ. Этот критерий применяют при расчете доли безопасных отказов SIF[1] [2],

[1] *Ландрини Г.* Интегральные уровни безопасности в соответствии со стандартами МЭК 61508 и 61511 и анализ их связи с техническим обслуживанием // Современные технологии автоматизации. № 1. 2009.

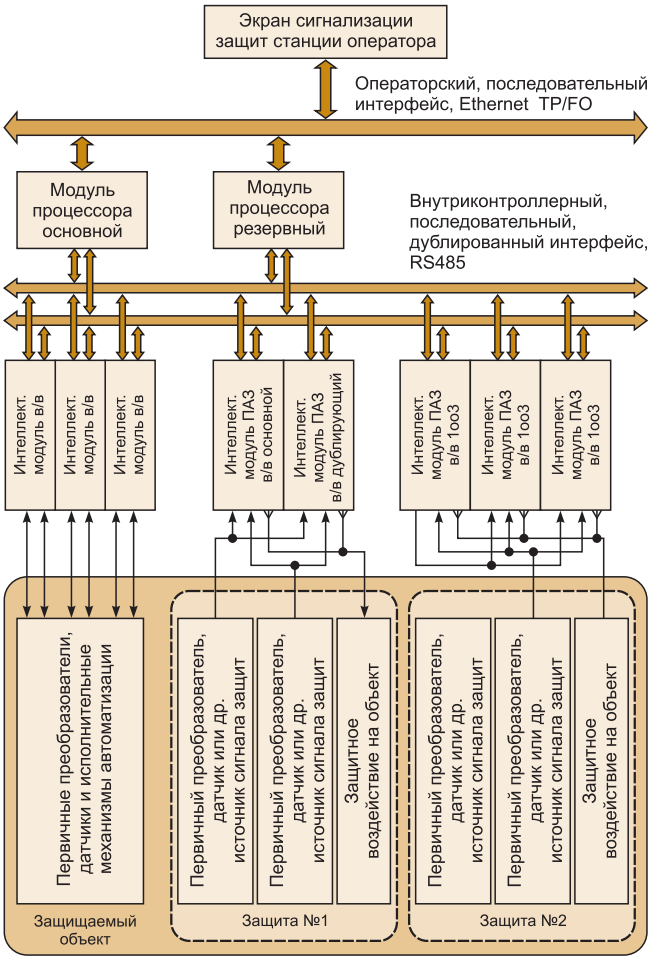

Рис. 4. Модифицированная структура дублированной, контроллерной, модульной системы ПАЗ, интегрированной в АСУТП

по которой определяют допустимый уровень SIL. В формулах используется суммарное значение интенсивности отказов последовательных цепочек управления, то есть $\Sigma \lambda_i$. Таким образом, минимизировать интенсивность отказов последовательной цепи, состоящей из модулей ввода сигналов защит, процессорного модуля, модуля вывода сигнала защит для стандартного ПЛК, достаточно сложно. Это связано с тем, что аппаратное обеспечение модулей ввода/вывода, интерфейса модулей ПЛК, процессорного модуля требует большого числа дискретных и интегральных элементов, разъемных, коммутационных и мультиплексируемых элементов схемотехники, что снижает расчетные показатели надежности системы в целом. Таким образом, чем сложнее и аппаратно избыточнее ПЛК, тем выше интенсивность отказов и тем ниже уровень SIL, на который может претендовать компонент системы ПАЗ. За подтверждением этого вывода опять обратимся к ГОСТ Р МЭК 61508-2007: "Избыточные функциональные возможности, пропускная способность или производительность могут быть вредными для безопасности системы, если существующие системы чрезмерно усложнены или имеют неиспользуемые возможности" (ГОСТ Р МЭК 61508-2007. Ч. 1. с.12).

4. *Сложность проверки систем после модификации в процессе эксплуатации*. Выполнить функциональное тестирование или тестирование методом "черного ящика" многоканальных систем ПАЗ невозможно или практически невозможно, так как число тестовых комбинаций в таких системах может стремиться к бесконечности. Обязательность такого тестирования – требование стандарта (ГОСТ Р МЭК 61508-2007. Ч. 3. с.32).

Сформулируем задачи по модернизации структуры ПАЗ:

- уменьшение объема задач ПАЗ, решаемых одним ПЛК (оптимально – 1 задача, максимально – 4 задачи);
- применение ПЛК без ОС: исполняемая задача должна иметь вид конечного откомпилированного кода в командах микропроцессора. ПО ПЛК должно выполнять функции *микропрограммного автомата*;
- ПЛК должен быть оптимизирован по набору функций, оснащен только тем программно-аппаратным инструментом, который необходим ему для выполнения задач ПАЗ. В конструкции ПЛК нежелательно применение внутренних интерфейсов, шинной адресации ввода/вывода, разъемных соединений между основными системными блоками ПЛК;
- для сохранения функций дублирования один из двух (1оо2) или два из двух (2оо2) необходимо, чтобы каналы ввода/вывода ПЛК имели возможность работы в параллельном для функции ввода/вывода сигналов и последовательном режиме для функции вывода. Обязательным условием является утверждение типа измерительных каналов ввода (в том числе и в параллельном режиме работы), так как в соответствии с требованиями ГОСТ Р 8.596-2002 "ГСИ. Метрологическое обеспечение измерительных систем. Основные положения" измерительные каналы систем безопасности должны быть утвержденного типа и подлежат периодической поверке согласно утвержденным методикам.

Для решения этих задач предлагается новая структура АСУТП с интегрированными функциями ПАЗ, минимизированный вариант которой представлен на рис. 4.

Рассмотрим основные функциональные отличия модифицированной структуры (рис. 4) от предыдущих:

1. *Приведенная структура позволяет создавать распределенную систему ПАЗ* с применением интеллектуальных модулей ввода/вывода (ИМВВ) как составную часть системы АСУТП.

2. *Дублирование функции ПАЗ* реализовано меньшими программно-аппаратными средствами при увеличении надежности. В то же время, сохранен основной критерий отказоустойчивости программно-аппаратных средств разных уровней безопасности SIL1...4: N=1 (Ч. 2, с.15), то есть любая одиночная неисправность не может привести к потере функции безопасности. Отказоустойчивость N означает, что N+1 отказ приведет к потере функции безопасности.

3. *Возможность изменения уровня безопасности индивидуально для каждой задачи ПАЗ.* В данной структу-

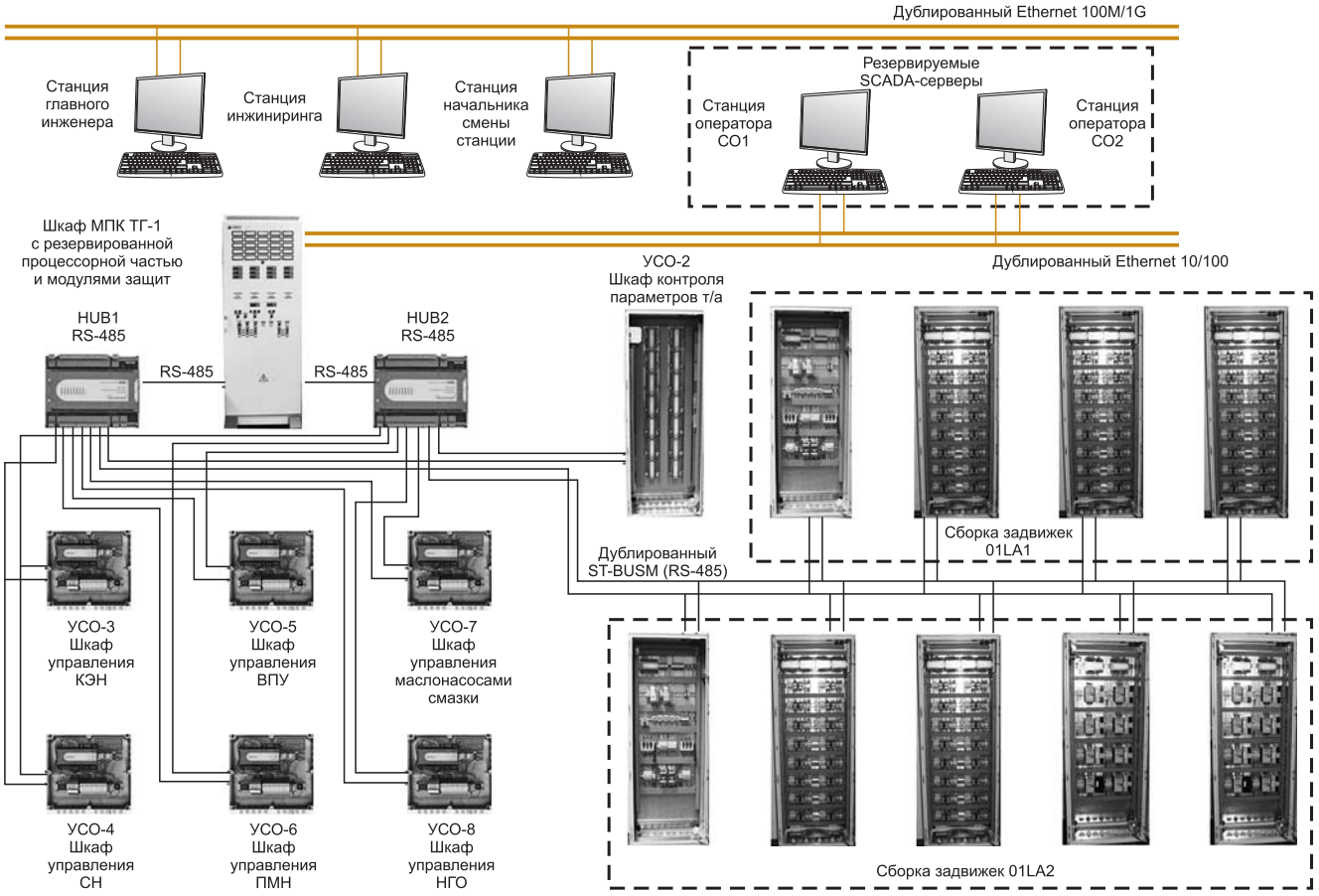

Рис. 5. Структурна схема АСУТП турбоагрегата ТГ-1 Топарской ГРЭС

ре, меняя долю безопасных отказов ИМВВ от 60% до 99%, можно менять уровень безопасности применительно к выполняемой ИМВВ функции ПАЗ от SIL1 до SIL4. Если трактовать выше сказанное упрощенно, то, достигая разного уровня надежности ИМВВ, можно достичь разных уровней безопасности ПАЗ.

Пример. Какая-либо из функции ПАЗ требует более высокого уровня безопасности, чем все остальные на автоматизируемом объекте (например, все имеющиеся функции ПАЗ требуют уровня SIL2 и лишь одна – уровня SIL3). В структуре (рис. 4) не меняя долю безопасных отказов (надежность) ИМВВ, можно для одной функции построить локальную систему с отказоустойчивостью N=2, то есть применить троирование функции ПАЗ на трех ИМВВ, включенных по схеме 1оо3 (один из трех). Данное включение допускает внесение двух одиночных неисправностей без потери функции безопасности (Ч. 2, табл. 3).

4. *Процессорные модули ПЛК в данной структуре не влияют на функцию безопасности.* Для функции ПАЗ они выполняют коммуникативную роль, а именно: загрузка приложения ИМВВ, диагностика, передача информации о состоянии защит в операторскую станцию для отображения на экране сигнализации защит.

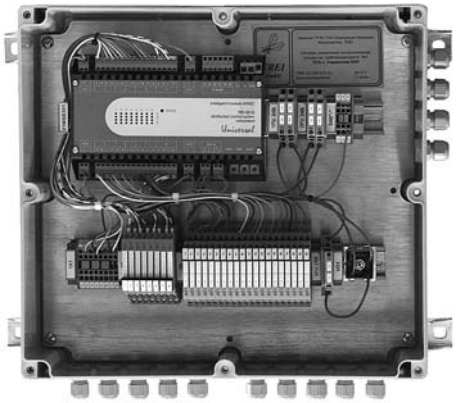

Рис. 6. Пример реализации удаленного УСО на базе интеллектуального модуля M932C контроллера TREI-5B-05

В существующей системе процессорные модули ПЛК выполняют алгоритмы сложного регулирования. Для реализации этих алгоритмов требуется информация от разных ИМВВ, не связанных с ПАЗ. Процессорные модули также выполняют каскадирование регуляторов, когда локальные регуляторы выполнены на ИМВВ. По этой причине процессорные модули не дублированы, а резервированы. Синхронизация БД процессорных модулей может проводиться или через операторский интерфейс, если он дублирован, или через отдельный интерфейс синхронизации. Синхронизация БД позволяет безударно переводить процесс регулирования с основного процессорного модуля на резервный и обратно.

5. *Реализована функция микропрограммного автомата на ИМВВ.* Пользовательское приложение, работающее на ИМВВ ПАЗ, – это программный TIC код, который исполняется без ОС и не использует функционала динамической адресации. Загрузочный модуль пользовательского

приложения формируется с помощью среды разработки приложения, которая функционирует на операторской станции АСУТП или на специально выделенной инженерной станции АСУТП.

Рассмотрим пример практической реализации децентрализованной АСУТП с интегрированными функциями ПАЗ на интеллектуальных модулях ввода/вывода. Специалистами фирмы ТРЭИ в 2009 г. была спроектирована, изготовлена и введена в строй АСУТП турбоагрегата К-55-90 Топарской ГРЭС корпорации Казахмыс (республика Казахстан). Рассмотрим подробнее структуру АСУТП (рис. 5).

Верхний уровень системы реализован по стандартной клиент-серверной архитектуре с резервированными серверами, совмещающими функции станций оператора оперативного персонала. Операторские станции неоперативного персонала (инженера АСУТП, главного инженера станции, начальника смены станции) подключены к серверам по дублированному независимому от контроллера интерфейсу Ethernet TP 100M/1G, который частично реализован на оптическом кабеле. Основной шкаф контроллера (МПК ТГ-1) подключен к серверным станциям по дублированному интерфейсу Ethernet TP 10/100.

Рис. 7. Пример реализации интеллектуальной сборки РТЗО для 16-ти реверсивных задвижек на базе интеллектуального модуля M932C контроллера TREI-5B-05

Контроллерный уровень системы реализован на контроллерах TREI-5B-05 по комбинированной архитектуре. Функции ПАЗ реализованы централизованно в шкафу МПК, а все остальные подсистемы построены по архитектуре РСУ с децентрализованными функциями сбора и обработки информации. Связь с интеллектуальными удаленными УСО осуществляется по дублированному интерфейсу ST-BUSM(RS-485) на скорости 1,25 MBod. Обращаем внимание читателей на реализацию топологии интерфейса ST-BUSM. Известно, что стандарт интерфейса RS-485 требует последовательного подключения абонентов интерфейса. Выполнение данного требования существенно снижает надежность системы и зависимость от целостности линии связи даже при наличии дублированного интерфейса. Но благодаря применению модуля M930H, выполняющего функцию HUB интерфейса RS-485, было реализовано радиальное подключение УСО для ответственных исполнительных механизмов (УСО-4...8) (рис. 6).

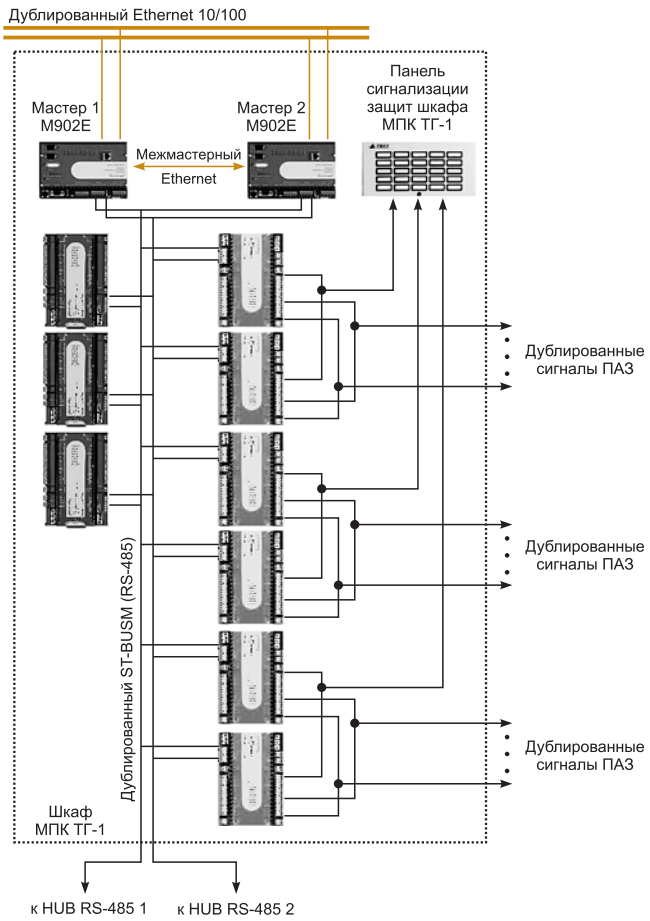

Рис.8. Структура шкафа МПК ТГ-1

Информационная подсистема реализована в УСО-2, конструктивно выполненного в виде отдельного шкафа, сбор и обработка информации в котором осуществляется на интеллектуальных модулях ввода/вывода серии M900.

Система дистанционного управления (ДУ) арматурой (≥ 100 ед.) осуществляется посредством интеллектуальных сборок задвижек (РТЗО) (рис. 7). Интеллектуальные модули управления арматурой M932C расположены непосредственно в шкафах с пускателями управления двигателями арматуры. В этих же модулях реализованы все алгоритмы управления.

Перейдем к рассмотрению структуры шкафа МПК, в котором и реализованы функции ПАЗ АСУТП ТГ-1 (рис. 8). Шкаф МПК реализован в соответствии с подходом, представленным на рис. 4.

Отметим качества, влияющие на функцию безопасности:

- процессорные модули M902E контроллера TREI работают в резервированном режиме и выполняют коммуникационную роль в АСУТП и не выполняют функций, влияющих на безопасность;

- все алгоритмы управления и обработки информации, не связанные с функцией безопасности, структурированы по подсистемам и реализованы в интеллектуальных модулях УСО и интеллектуальных РТЗО;

- подсистема ПАЗ реализована в дублированных, интеллектуальных модулях контроллера M932C. Дублирование организовано по схеме 1oo2 (один из двух);

- все измерительные каналы подсистемы ПАЗ, подключенные к дублированным модулям, зарегистрированы в Государственном реестре средств измерений. В описании типа средства измерения контроллеров TREI-5B отдельно нормированы метрологические характеристики измерительных каналов с резервированием, то есть в дублированном режиме. Испытания на полигоне изготовителя АСУТП, поверка системы поверителем на объекте проводилась в дублированном режиме;

- алгоритмы ПАЗ в ИМВВ разработаны с помощью инструментальной CASE-системы UNIMOD. Система позволяет использовать языки программирования ST, FBD и LD стандарта МЭК 61131-3, что соответствует требованиям к ПО стандарта [1]. Конечным продуктом системы программирования является исходный код, загружаемый по интерфейсу ST-BUS в ИМВВ, выполняющий в цикле алгоритмы ПАЗ без применения ОС;

- программирование, отладка, испытание, модификация и верификация алгоритмов ПАЗ проводится вне зависимости от технологических алгоритмов управления, регулирования и задач функционально-группового управления (ФГУ), реализованных на других ИМВВ и процессорных модулях контроллера;

- число тестовых испытаний и проверочных комбинаций входов для каждого ИМВВ ПАЗ конечное, что позволяет проводить проверку методом "черного ящика" индивидуально по каждой задаче ПАЗ или по группе задач внутри зоны ответственности одного ИМВВ.

Заключение

Развитие микроэлектронной элементной базы позволяет создавать новые, высоконадежные АСУТП с интегрированными в них функциями безопасности. Реализация систем ПАЗ по предлагаемой структуре, позволяет решить несколько, казалось бы, противоречивых задач:

- создать всю систему на базе одного контроллера с резервированными процессорными модулями;

- не допускать совмещения в одном контроллере функций безопасности и функций, не связанных с безопасностью;

- разделить задачи ПАЗ на отдельные законченные программно-аппаратные модули;

- значительно повысить надежность системы ПАЗ;

- удешевить всю разрабатываемую АСУТП.

Рогов Сергей Львович *– ген. директор ООО "ТРЭИ ГМБХ".*
Контактные телефоны: (8412) 55-58-90, 49-95-39.
E-mail: rogov@trei-gmbh.ru http://www.trei-gmbh.ru