RTP3000: НОВОЕ ПОКОЛЕНИЕ СИСТЕМ ДЛЯ УПРАВЛЕНИЯ И БЕЗОПАСНОСТИ НЕПРЕРЫВНЫХ ТП

Д.Э. Попов (ЗАО "Си Ай С - Контролс")

Рассмотрены архитектура, функциональные и технические особенности универсального комплекса технических средств RTP3000 компании RTP Corporation, предназначенного для решения задач управления и безопасности в составе АСУТП производств непрерывного типа.

Ключевые слова: АСУТП, комплекс технических средств, резервирование, безопасность, управление, отказоустойчивость, многопроцессорность.

На многих предприятиях нефтегазового комплекса АСУТП состоят из более или менее интегрированных подсистем управления и безопасности (включая ПАЗ, системы пожарной безопасности, контроль загазованности, системы управления горелками и др.). Высокий уровень критичности приложений, режим функционирования, нормативные требования определяют следующие особенности архитектуры систем безопасности: отказоустойчивость, надежность, полнота диагностики, аппаратная и программная избыточность. Следствием этого является, как правило, существенно более высокая стоимость, особенно с учетом обязательного резервирования компонентов систем безопасности на нефтеперерабатывающих и нефтехимических производствах.

RTP3000 – универсальный комплекс технических средств, предназначенный для эффективного решения задач управления и безопасности в составе АСУТП производств непрерывного типа. Комплекс разработан фирмой RTP Corporation на основе более чем 40-летнего опыта создания отказоустойчивых систем мониторинга, управления, критического управления и безопасности для различных отраслей промышленности.

Универсальный комплекс средств для управления и безопасности ТП

Международные стандарты в области функциональной безопасности IEC 61508, IEC 61511 существенно повлияли на все этапы жизненного цикла систем автоматизации и определили требования к техническим средствам, используемым для выполнения функций безопасности. Производство средств автоматизации, соответствующих этим требованиям и предназначенным для применения в составе систем безопасности, за последние годы существенно выросло.

Внимание к вопросам безопасности и роль систем безопасности в структуре автоматизации производства непрерывно возрастает. Формирование требований к системам безопасности (safety requirements specification) в соответствии со стандартом IEC 61511, а также отнесение к системам безопасности наряду с системами ПАЗ систем пожарной и газовой безопасности, систем управления горелками, систем критического управления существенно увеличивают число функций безопасности в составе АСУТП. Зачастую именно системы безопасности являются основным (иногда единственным) компонентом АСУТП.

АСУТП является важнейшим инструментом, обеспечивающим эффективное управление и безопасность ТП. Современный подход к реализации АСУТП сочетает противоположные тенденции: разделение процессов создания систем управления и безопасности, с одной стороны, и объединение этих систем в единую АСУТП, с другой. Усугубляет ситуацию необходимость использовать различные контроллеры для систем управления и безопасности. Контроллеры систем управления не могут использоваться в системах безопасности, поскольку не обладают необходимым уровнем диагностики, отказоустойчивости и надежности. Функциональные возможности специализированных контроллеров безопасности обычно оптимизированы для выполнения функций безопасности и не позволяют эффективно реализовывать алгоритмы управления. Кроме того, в силу аппаратной, программной и информационной избыточности они, как правило, существенно дороже контроллеров управления.

Производители средств автоматизации стараются преодолеть указанные противоречия и снизить издержки, связанные с реализацией и последующей эксплуатацией АСУТП с помощью так называемых интегрированных систем управления и безопасности. Понятие «интегрированности» систем у разных производителей может подразумевать различные характеристики, облегчающие функционирование разнотипного оборудования в одной системе:

– поддержка системой безопасности одного из основных коммуникационных протоколов системы управления;

– использование общего ПО конфигурирования и диагностики для системы управления и системы безопасности;

– применение однотипных процессоров для реализации функций управления и безопасности с возможностью их комплектации “обычными” или ”безопасными” подсистемами ввода/вывода.

Система RTP3000 является универсальным решением, обеспечивающим высокий уровень технико-экономических показателей при реализации систем безопасности (SIL3), систем управления и интегрированных решений, обеспечивая 100 % унификацию программных и аппаратных средств для любых типов приложений.

Основные особенности системы:

– масштабируемая распределенная архитектура от небольших локальных систем до десятков распре-

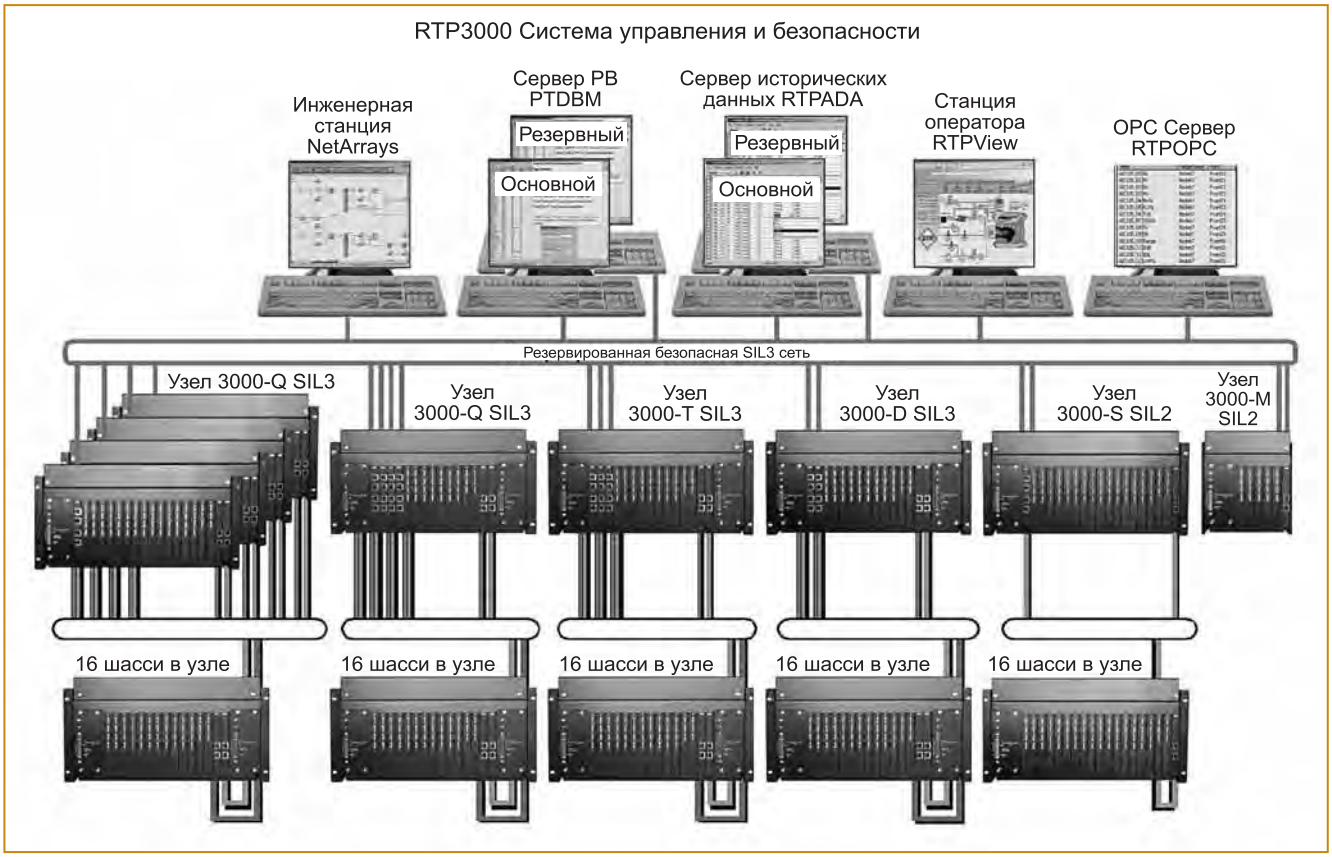

Рис. 1. Различные варианты архитектуры узлов системы управления и безопасности RTP3000

деленных узлов управления и безопасности, обрабатывающих десятки тысяч сигналов;

– универсальная платформа для систем управления и безопасности; уровень безопасности сертифицирован SIL1-SIL3 (IEC 61508, IEC 61511);

– интегрированный программный пакет конфигурирования, обслуживания, диагностики контроллеров и создания интерфейса оператора NetSuite;

– поддержка открытых промышленных протоколов Modbus RTU, Modbus TCP, OPC;

– поддержка разнообразных языков программирования: стандартные языки IEC 61131-3, нечеткая логика в соответствии с IEC 61131-7, поддержка C/C++ для реализации сложных, нестандартных алгоритмов управления;

– индивидуальный выбор схемы резервирования и уровня отказоустойчивости для любого компонента системы: 1oo1D (SIL2), 1002D (SIL3), 2oo2D (SIL3), 2oo3D (SIL3), 3oo4D (SIL3);

– размещение резервируемых модулей в разных шасси минимизирует возможность их одновременного отказа “по общей причине”;

– безопасные (SIL3) коммуникации по резервированной (дублированной или троированной) сети Fast Ethernet 100Mbit на базе стандартных компонентов;

– параллельная многопроцессорная архитектура, обеспечивающая цикл сканирования контроллера, не превышающий 5 мс, и время реакции системы до 12 мс независимо от информационной емкости ввода/вывода и размера прикладной программы;

– детальная диагностика благодаря высокой производительности системы, не приводящая к снижению скорости выполнения прикладных программ;

– замена компонентов системы, изменение аппаратной и программной конфигурации в режиме on-line;

– соответствие требованиям безопасности уровня SIL3 с периодом тестирования 10 лет.

Гибкая масштабируемая архитектура для управления и безопасности

Система управления и безопасности RTP3000 предназначена для автоматизации самых разных объектов: от небольших технологических установок до крупных производственных комплексов. В соответствии с особенностями производства формируются системы, различающиеся по структуре, функциональности, объему, уровню безопасности и отказоустойчивости: от небольших локальных систем, размещенных в одном шасси, до распределенных систем, объединяющих десятки узлов.

На рис. 1 представлены различные варианты архитектуры узлов системы:

– узел 3000-Q QMR (3oo4D, SIL3): отказоустойчивая система, состоящая из четырех процессоров узла, резервирующих друг друга по схеме 3oo4D; процессоры размещены в четырех отдельных шасси; мо-

дули ввода/вывода установлены в тех же шасси, что и процессоры узлов, а также в дополнительные шасси ввода/вывода; тип резервирования модулей ввода/вывода и размещение резервированных модулей определяются индивидуально для каждого модуля; шасси связаны безопасной (SIL3) отказоустойчивой (троированной) магистралью ввода/вывода на базе Fast Ethernet 100 Мбит/с;

– узел 3000-Q QMR (3oo4D, SIL3): в отличие от предыдущего варианта – процессоры размещены в одном шасси;

– узел 3000-T TMR (2oo3D, SIL3): в этом варианте три процессора узла резервируют друг друга по схеме 2oo3D; процессоры размещены в одном шасси;

– узел 3000-D (1oo2D, SIL3): два резервированных процессора узла в одном шасси;

– узел 3000-S (1001D, SIL2): один процессор узла; блоки питания и процессоры шасси не резервированы; магистраль ввода/вывода дублированная.

Все перечисленные узлы объединены безопасной (SIL3) отказоустойчивой сетью Fast Ethernet, соединяющей их с серверами данных (PB и историческим) и рабочими местами инженеров и операторов.

Каждый из узлов может выполнять функции системы управления и системы безопасности. На технологических объектах, где это не запрещено нормативными документами, допускается выполнение функций управления и безопасности на одном узле; при этом функции безопасности в соответствии с требованиями стандартов IEC 61508 и 61511 отделены от функций системы управления. Изменение параметров системы безопасности или какое-то иное деструктивное влияние на нее со стороны системы управления невозможно.

Незапланированный останов непрерывного производства связан с существенными экономическими потерями; межремонтный период безостановочной эксплуатации может достигать нескольких лет. В течение этого периода в связи с модернизацией существующих или вводом в эксплуатацию новых технологических узлов, может потребоваться внесение изменений в прикладную программу, а также расширение или изменение аппаратной части системы: подключение измерительных приборов и исполнительных устройств, удаление и установка модулей, шасси, дополнительных узлов системы управления и безопасности. RTP3000 позволяет вносить указанные изменения без каких-либо ограничений, а также осуществлять замену вышедших из строя компонентов, не останавливая работу системы.

Отказоустойчивость – основа надежности

Отказоустойчивость является одним из наиболее существенных параметров систем управления и систем безопасности на производствах непрерывного типа. Выход из строя любой из систем может привести к останову ТП и существенным экономическим потерям (не говоря уже о более серьезных последствиях). Не менее важна возможность гибкой, избирательной отказоустойчивости для различных компонентов АСУТП. Такой подход позволяет обеспечить необходимый уровень надежности в соответствии с уровнем критичности функции управления или функции безопасности, которые реализуются с помощью данного компонента и в то же время не приведет к неоправданному увеличению стоимости системы.

Резервирование модулей или каналов системы может не обеспечить желаемого уровня отказоустойчивости и надежности в случае одновременного выхода из строя резервирующих друг друга компонентов. Это происходит, как правило, вследствие отказов “по общей причине”, например, в случае выхода из строя шасси, в котором расположены резервирующие друг друга модули (или каналы) или при размещении резервирующих друг друга каналов на одном модуле (или на разных модулях в пределах одного шасси).

Механизм распределенной отказоустойчивости RTP3000 наряду с гибким, избирательным подходом обеспечивает также максимальную устойчивость к отказам по “общей причине”. Любые модули и отдельные каналы систем управления или безопасности, созданные на основе RTP3000, могут быть зарезервированы. Кратность резервирования в диапазоне 1...4 выбирается для каждого компонента произвольно, в зависимости от уровня ответственности реализуемых им функций. Резервирующие друг друга компоненты системы могут быть произвольным образом распределены по различным шасси в составе узла. Такой подход обеспечивает максимальный уровень надежности и отказоустойчивости.

Поскольку отказоустойчивость обеспечивается за счет аппаратной избыточности, то ее уровень непосредственно отражается на стоимости системы. Возможность гибко конфигурировать уровень отказоустойчивости компонентов в соответствии с уровнем критичности выполняемых ими функций позволяет оптимизировать технико-экономические показатели АСУТП.

Рис. 2. Структурная схема системы управления и безопасности RTP3000

Многопроцессорная архитектура с параллельной обработкой обеспечивает высокую производительность

Многопроцессорная архитектура и распределенная параллельная обработка данных в RTP3000 позволили достичь впечатляющих показателей производительности системы: минимизировать цикл процессора до значений ⩽5 мс и время реакции системы <12 мс. Высокая производительность является существенным преимуществом как для систем безопасности, так и для систем управления. Сокращается время реакции на отклонение процесса от нормального режима, что дает возможность применений RTP3000 на объектах с малым временем безопасности процесса (время от возникновения нарушения до развития аварийной ситуации). В системах управления появляется возможность эффективной реализации сложных ресурсоемких алгоритмов управления.

Сканирование и диагностика модулей ввода/вывода, регистрация последовательностей событий с высоким разрешением (1 мс) осуществляется процессорами шасси, число которых увеличивается при возрастании информационной емкости системы, поэтому производительность не падает с ростом объема ввода/вывода. Выполнение функций управления и безопасности осуществляется процессорами узла. Для управления очень быстрыми процессами, такими как турбины электрогенераторов или экзотермические реакции, скорость которых превышает возможности системы, используются специализированные модули, совмещающие функции управления и ввода/вывода и обеспечивающие время реакции системы < 1 мс.

Обычно уровень диагностики в системах управления существенно ниже, чем в системах безопасности. Выполнение диагностических процедур снижает скорость алгоритмов управления, а аппаратная, программная и информационная избыточность приводит к существенному увеличению стоимости. Высокий уровень производительности и особенности архитектуры RTP3000 позволяют реализовывать системы управления, уровень диагностики которых не уступает системам безопасности без потери скорости работы и увеличения стоимости.

Детальная диагностика – ключевой элемент безопасности

Диагностика работы всех компонентов системы является ключевым элементом безопасности; качество диагностики зависит от полноты охвата, детальности и скорости выполнения диагностических процедур. Чем быстрее обнаружена и устранена неисправность, тем безопаснее система. В RTP3000 диагностика каждого компонента и каждой системной функции проводится на каждом цикле сканирования; полнота диагностики является основой архитектуры системы, где каждый компонент диагностирует себя и все функционально связанные с ним элементы (рис. 2). Помимо компонентов и функций системы диагностируются также сигнальные линии между модулями ввода/вывода и полевыми устройствами. Контроль состояния сигнальных линий не влияет на функционирование полевых устройств. Проверка диагностических процедур осуществляется имитацией состояния неисправности компонентов и тестирования реакции диагностических механизмов.

Выделим следующие основные типы диагностических процедур RTP3000:

– проверка выполнения процессорами математических и логических функций; проверка каналов модулей ввода/вывода, гарантирующая способность канала изменить состояние;

– контроль целостности сигнальных линий между модулями ввода/вывода и полевыми устройствами; диагностика обрыва и короткого замыкания;

– резервные шины троированных сетей ввода/вывода используются для контроля работоспособности сети; помимо этого проводится дополнительный контроль целостности сообщений, пересылаемых по сети.

Модули ввода осуществляют контроль целостности входных цепей, проверку входных сигналов и контроль работоспособности самого модуля. По объединительной панели шасси входные сигналы из модулей ввода поступают в процессор шасси. Передача данных от модулей ввода к процессору шасси сопровождается целым рядом проверок:

– все сообщения, приходящие от входных модулей к процессору шасси, регенерируются процессором шасси и пересылаются обратно в модуль, где они сравниваются с исходным сообщением для контроля целостности;

– адрес получателя сообщения (в данном случае процессора шасси) повторяется в сообщении несколько раз для гарантии доставки по назначению;

– каждое сообщение пересылается два раза: второй раз в инвертированном виде (получатель сравнивает оба сообщения).

Входные данные пересылаются процессором шасси в процессор узла по троированной отказоустойчивой сети Fast Ethernet (100 Мбит/с). Уровень диагностики сети и контроля целостности сообщений соответствует уровню полноты безопасности SIL3. Контроль значений входных параметров резервированных каналов ввода проводится независимо каждым из резервированных процессоров узла; каждый процессор шасси обменивается данными с каждым из процессоров узла; нарушение работы одного из резервированных процессоров или модулей ввода сразу выявляется и не оказывает влияния на работу других модулей и системы в целом.

В случае реализации системы управления и системы безопасности в одном узле, в процессоре узла происходит разделение данных. Данные, относящиеся к системе безопасности, отделяются от данных системы управления и обрабатываются в процессоре узла приложением системы безопасности; они защищены от любых изменений со стороны других прило-

жений и интерфейса оператора. Данные, относящиеся к функциям управления, передаются приложению системы управления.

Каждый процессор узла выполняет приложение два раза и сравнивает результаты. Если результаты совпадают, то они пересылаются по троированной сети ввода/вывода в процессоры шасси. В процессоре шасси проводится диагностика и голосование (мажоритарная выборка) полученных результатов; тип голосования зависит от кратности резервирования процессоров узла. Передача данных от процессора шасси к модулям вывода осуществляется тем же способом, с теми же диагностическими процедурами, что обмен данными с модулями ввода, описанный ранее.

По результатам диагностических процедур формируются диагностические сообщения, позволяющие обслуживающему персоналу своевременно принять необходимые меры для восстановления уровня работоспособности и отказоустойчивости системы.

Интегрированная среда разработки NetSuite

RTP NetSuite – полностью интегрированная среда разработки, тестирования и обслуживания систем управления и безопасности на базе комплекса RTP3000. NetSuite включает все необходимые приложения для создания АСУТП: проектирование и разработка алгоритмов управления и защиты, тестирование и отладка прикладной программы на встроенном симуляторе, построение операторского интерфейса, включая серверы данных PB, рабочие места операторов, сервер исторических данных и ряд вспомогательных программных средств и утилит.

Основные компоненты NetSuite:

– NetArrays – графический пакет конфигурирования оборудования системы и создания алгоритмов управления на основе языков стандарта IEC 61131-3;

– PTDBM – сервер БД PB;

– RTPADA – исторический сервер данных и событий;

– RTPView – средство разработки графического интефейса оператора;

– RTPReport – генератор отчетов на основе данных исторического сервера, включающий библиотеку разнообразных функций статистической обработки данных, табличных и графических форм их представления.

Сервер данных PB и сервер исторических данных и событий поддерживают работу в режиме резервирования, распространяя концепцию максимальной отказоустойчивости RTP3000 на уровень интерфейса оператора. Поддержка открытого протокола OPC-DA обеспечивает взаимодействие с системами уровня управления производством, а также оборудованием и АСУТП других производителей.

Попов Дмитрий Эммануилович *– директор по развитию направления системы управления и ПАЗ*
ЗАО "Си Ай С – Контролс".
Контактный телефон (495) 961-12-71.
Http:// www.cis-controls.ru E-mail: dpopov@cis-controls.ru

Промышленные мониторы и панели Thin Clients в широкоэкранном формате

Департамент «Промышленная автоматизация» компании Siemens добавил новые промышленные мониторы и панели Thin Client в свою линейку устройств HMI в широкоэкранном формате. Они представлены в виде терминалов или устройств, управляющихся сенсорным экраном или клавишами на передней панели, с диагоналями дисплеев 12...22 дюймов. Устройства используются для установки непосредственно на пульте управления, а также для подключения к системе дистанционного управления или SCADA-системе. Мониторы Simatic Flat Panel подходят для подключения к промышленным ПК на расстоянии до 30 метров, в то время как Simatic Thin Clients могут использоваться для распределенных решений. Новая продукция получила награду iF product design award 2012 за лучший дизайн продукта 2012. Новые широкоэкранные устройства Simatic IFP и Simatic ITC рассчитаны на длительную эксплуатацию. Они оборудованы прочными литыми алюминиевыми передними стенками и рассчитаны на 24-часовую непрерывную работу, не требующую техобслуживания, а также работают при высокой температуре и вибрации, устойчивы к ударам и ЭМС. Энергосберегающая светодиодная фоновая подсветка может менять яркость в 100 % диапазоне, а при максимальной яркости может использоваться в хорошо освещенных рабочих средах. Широкоформатные мониторы имеют четкий контраст, высокое разрешение, широкий угол обзора.

Новая промышленная панель Simatic IFP подходит для использования в качестве производственного монитора с высоким быстродействием, например, для вывода видео и построения графиков. Панели представлены с размерами 15, 19 и 22 дюйма в качестве отображающих устройств или устройств с сенсорной функцией. Также имеется 15-дюймовая сенсорная версия с функциональными клавишами, портом USB, расположенным на фронтовой стороне, и клавиатурой. Устройства также рассчитаны на установку в вертикальном положении при работе в ограниченном пространстве. Они подключаются через DVI-D или новый интерфейс DisplayPort к промышленному ПК, который может располагаться на расстоянии до 30 м. Мониторы прошли сертификацию по Atex. Ожидается одобрение от компании Marine.

Панель Thin Client Simatic ITC для клиент-серверных архитектур не имеет изнашиваемых механических частей, таких как вентилятор или жесткий диск. Сенсорное устройство с диагоналями дисплеев 12, 15, 19 или 22 дюйма может быть сконфигурировано для подключения к одному или нескольким серверам, таким как Simatic IPC. Дисплей Thin Client оборудован процессором Intel Celeron с частотой 1,2 ГГц для приложений ЧМИ.

ПО Setup Wizard обеспечивает быстрый ввод устройств в эксплуатацию и интеграцию их в существующие сети. ПО настройки удаленного доступа обеспечивает центральное управление панелями Thin Clients через сеть, например, для параллельного обновления встроенного аппаратного обеспечения.

Http://iadt.siemens.ru