# Программно-технический комплекс СМ СИКОН для систем автоматизации высокой надежности

**В.Л. Зиновьев (ООО "Компьютерные комплексы"),**
**А.В. Фрейдман (НЦ "Науцилус")**

*ПТК СМ СИКОН для АСУТП высокой надежности предназначен для приложений АСУТП, где серьезный сбой системы управления чреват катастрофическими последствиями. ПТК разработан в Институте электронных управляющих машин (ИНЭУМ) в сотрудничестве с компаниями "Науцилус" и "Компьютерные комплексы". Для обеспечения отказоустойчивости архитектура ПТК использует активно резервируемые конфигурации ключевых элементов, а все ПО, включая SCADA систему, разработано на базе ОС РВ.*

Аппаратная часть ПТК СМ СИКОН включает на нижнем уровне комплекс технических средств (КТС) СМ СИКОН, а на верхнем – серверы БД РВ OPUS и станции операторов (СТО) – SCADA Phocus для сбора данных и непрерывного мониторинга процессов. Структура ПТК СМ СИКОН представлена на рис. 1.

КТС СМ СИКОН (Сетевых Индустриальных Контроллеров) предназначен для работы в качестве низового звена системы, осуществляющего связь со средствами измерения параметров ТП, приборами промышленной автоматики и исполнительными механизмами.

КТС СМ СИКОН – полнофункциональный набор унифицированных модулей для создания распределенных сетевых АСУТП по заказной спецификации, включающий:

- управляющие контроллеры, ранжированные по уровню обеспечения надежности (одинарный, дублированный);
- контроллеры УСО, различающиеся по числу обрабатываемых информационных каналов и по уровню обеспечения надежности;
- набор модулей ввода/вывода сигналов (аналогового, дискретного ввода/вывода, блок компенсации холодного спая термопар (БКХ) и блок релейной коммутации (БРК)).

КТС СМ СИКОН реализует функции:

- измерения аналоговых выходных сигналов датчиков в виде напряжения и силы постоянного тока, электрического сопротивления; выходных сигналов термопар и термопреобразователей сопротивления;
- выдачи управляющих сигналов на объект;
- преобразования и обработки информации о состоянии объекта;
- цифрового регулирования и логического управления;
- внутренней диагностики и оперативной сигнализации возникших неисправностей;
- передачи информации верхнему уровню управляющей системы и приема управляющей информации от верхнего уровня системы.

Число каналов ввода/вывода (в том числе резервных) определяется требованиями заказчика. При этом одна стойка УСО позволяет разместить до 124 канала ввода или до 64 каналов вывода аналоговых сигналов в любом сочетании плюс до 256 каналов ввода/вывода дискретных сигналов в любом сочетании. Интерфейс между стойками УСО и управляющим контроллером – CAN (дублированный). Интерфейс между КТС СМ СИКОН и станциями оператора – Ethernet (дублированный).

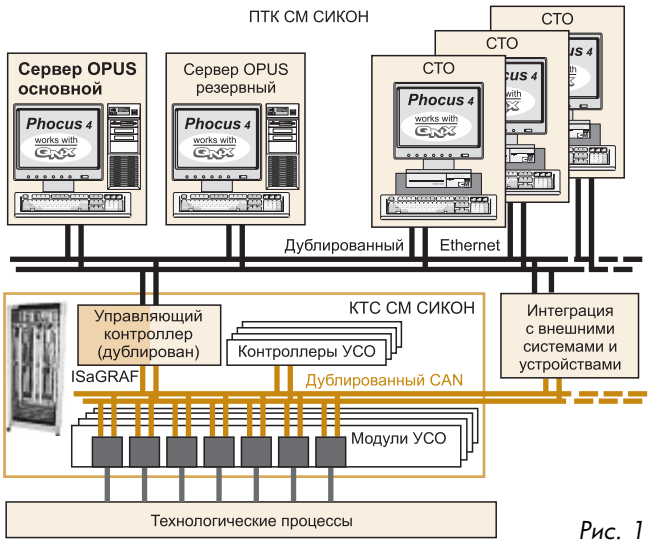


Рис. 1

Рис. 2

## Обеспечение надежности и отказоустойчивости

Для обеспечения надежности системы применено резервирование наиболее важных элементов и систем. К ним относятся: ЛВС Ethernet подсистемы взаимодействия с персоналом (ПВП), сетевые средства связи CANbus для подсистемы управления и взаимодействия с объектом (ПУВО), а также аппаратные средства подсистем технологического оборудования (дублирование). Применена дублированная система питания 24В с аккумуляторной поддержкой.

Повышенная надежность и отказоустойчивость системы обеспечивается: диагностикой состояний линий связи; резервированием управляющих контроллеров и интерфейсов связи; возможностью замены неисправных модулей в "горячем" режиме.

Взаимодействие основного контроллера с резервным обеспе-

чивает "безударное" переключение между основным и резервным оборудованием. Гальваническая развязка входных/выходных сигналов достигается за счет схемотехнических решений модулей аналого-частотных преобразователей и модулей дискретного ввода/вывода сигналов. Для обеспечения искробезопасности цепей входных/выходных сигналов применены изолирующие аналого-частотные и частотно-аналоговые преобразователи с видом защиты "искробезопасная электрическая цепь" ExibIIC.

В функции контроллера УСО входит сбор и обработка сигналов от объекта и представление их значений в форме, удобной для передачи на дублированный управляющий контроллер по локальной дублированной сети CAN. На основании полученной информации управляющий контроллер формирует сигналы, которые передаются на выходные модули УСО только с одного контроллера (ведущего). В случае неисправности ведущего контроллера происходит безударное переключение на резервный контроллер.

***Контроллер УСО*** включает процессорный модуль Сикон ТС1775.30, модуль питания ввода/вывода дискретных сигналов и модуль ввода/вывода частотных сигналов. Процессорный модуль построен на базе 32-разрядного микроконтроллера SAK TC1775 (INFINEON Technology), программируемой логической интегральной схемы (ПЛИС) XC 9500 (XILINX) и двух контроллеров Ethernet – CS 8900A (Cirrus LOGIC).

Функциональные характеристики определяются параметрами используемого микроконтроллера. Его производительность – 40 млн. операций/с, он имеет встроенную функцию цифровой обработки сигналов (DSP), специализированный процессор для работы с периферией, внутреннюю RAM объемом 72 Кбайт, 32-канальный АЦП, 64-канальный блок обработки частотных сигналов, последовательные интерфейсы RS-232 и Twin CAN. Использует внешнюю память в виде RAM с батарейной поддержкой емкостью до 8 Мбайт, быструю RAM емкостью до 1 Мбайт и FLASH-память объемом до 8 Мбайт. Микроконтроллер использует часы РВ с батарейной поддержкой и синхронным параллельным интерфейсом (SPI).

Имеется возможность взаимодействия через внешние интерфейсы: TWIN CAN (дублированный интерфейс для связи по сети CAN с внешними устройствами со скорость передачи до 1 Мбит/с); Ethernet реализован в виде дублированного интерфейса (применяется для связи с сетями персональных и промышленных компьютеров со скоростью передачи до 10 Мбит/с); два последовательных порта могут использоваться как два канала RS-232/485 в любом сочетании.

***Управляющий контроллер*** выполнен в том же конструктиве, что и контроллер УСО, но содержит два процессорных модуля (ПМ), выполняющие управляющие функции в дублированном режиме. Реализованный *способ резервирования* использует соединение ПМ управляющего контроллера через линии GPTA (General Purpose Timer Array) микроконтроллеров. Управление потоком данных по этим линиям осуществляется периферийным процессором PCP (Peripheral Control Processor). Такое решение позволяет существенно разгрузить центральный процессор, а также упростить логику работы всего ПО контроллера в целом, повысив тем самым его надежность.

### Состав ПО ПТК СМ СИКОН

ПО ПТК можно условно разделить на группы: системное, инструментальное и прикладное.

Системное ПО включает ОС, интерфейсные программные модули и программы взаимодействия с аппаратными средствами и является базовым для инструментального и прикладного ПО. В ПТК СМ СИКОН в качестве основы для системного ПО на нижнем и верхнем уровнях АСУТП используется ОС РВ. На нижнем уровне для контроллеров КТС СМ СИКОН используется встроенная, оптимизированная для применяемого процессора (Tricore TC 1775) ОС РВ, не имеющая интерфейсов для конечного пользователя; на верхнем уровне – ОС РВ QNX 4.25.

Инструментальное ПО входит в состав как нижнего (пакет ISaGRAF), так и верхнего уровня (SCADA пакет Phocus 4) ПТК СМ СИКОН. Система ISaGRAF применяется в КТС СМ СИКОН в качестве инструментального ПО для ПУВО. Помимо стандартных языков стандарта IEC 61131-3 ISaGRAF позволяет использовать распространенный *графический язык Потоковых Диаграмм (FC – Flow Chart)*, который используется для описания последовательных операций. Функционально пакет ISaGRAF состоит из средств: разработки (Workbench) и исполнения (Target).

Прикладное ПО создается по техническому заданию заказчика с помощью средств разработки пакетов ISaGRAF и Phocus и может модернизироваться в процессе эксплуатации самим заказчиком самостоятельно.

### ПО управляющего контроллера

Основой ПО управляющего контроллера КТС СМ СИКОН служит целевая задача ISaGRAF для процессора Tricore TC1775, разработанная в Научном центре "Науцилус". Она включает следующие программы: ядро целевой задачи (исполнение пользовательских алгоритмов); средство связи с системой разработки; средство обеспечения внешнего доступа к БД ISaGRAF. Чтобы повысить время реакции целевой задачи ISaGRAF, она разделена на два процесса: прикладная целевая задача ядра и программа связи, которые выполняются параллельно и независимо друг от друга.

Задача доступа к БД ISaGRAF обеспечивает возможность доступа к данным ISaGRAF из SCADA-системы.

Благодаря возможности разрабатывать процедуры на языке С для ПТК СМ СИКОН в компании Науцилус были созданы различные функции диагностики и управления. К первым относятся функции диагнос-

*Надежность оборудования обратно пропорциональна числу и положению лиц, за ним наблюдающих.*
Закон Уатсона

тики сетей CAN и Ethernet, проверки жизнеспособности УСО, дублирующего ПМ, а также диагностики связи с объектом управления. Ко вторым – такие широко используемые алгоритмы управления, как ПИ-, ПДД- и ПИД-регуляторы. Все эти функции доступны технологу при разработке системы управления ТП, например, в виде функциональных блоков для программирования на графическом языке FBD.

Помимо этого, ПО управляющего контроллера содержит задачу управления РВ, которая может использоваться, например, для управления МЭО (механизмов электрических однооборотных), предназначенных для перемещения рабочих органов запорно-регулирующей трубопроводной арматуры поворотного принципа действия (шаровые и пробковые краны, поворотные дисковые затворы, заслонки и пр.). Так как эта задача не связана с циклом ISaGRAF, она способна обеспечить выдачу управляющих сигналов с точностью 20 мс, что позволяет получить высокую точность дозировки жидкостей и высокую производительность.

### Функции основного и резервного ПМ управляющего контроллера на уровне ISaGRAF

Каждый из ПМ управляющего контроллера может быть основным либо резервным. Задача ISaGRAF основного ПМ управляющего контроллера работает в режиме РВ, задача ISaGRAF резервного ПМ управляющего контроллера работает в поцикловом режиме исполнения.

Основной ПМ получает данные по шине CAN от контроллеров УСО, определяет в соответствии с технологическим алгоритмом необходимые управляющие воздействия и посылает их контроллерам УСО. В конце каждого цикла целевой задачи ISaGRAF делается копия областей данных целевой задачи ISaGRAF, включающая кроме значений переменных, описывающих непосредственно состояние управляемого объекта, также и состояния всех функциональных блоков регуляторов и таймеров. Эта копия (зеркало) используется для быстрого доступа к данным драйвера SCADA-системы. Другая аналогичная копия переписывается в память периферийного процессора и запускается программа передачи этих данных на резервный ПМ.

Как только завершается передача текущего состояния целевой задачи ISaGRAF основного ПМ управляющего контроллера на резервный, задача ISaGRAF резервного ПМ исполняет на полученных данных один цикл алгоритма и переходит в режим ожидания следующей порции данных. Принципиальное различие в функциях основного и резервного ПМ состоит в том, что резервный не опрашивает контроллеры УСО и не посылает им команды управления. Все остальные функции резервным ПМ управляющего контроллера выполняются: в конце цикла делается зеркало для связи со SCADA, продолжает работать задача связи Ethernet и задача арбитража, отслеживающая жизнеспособность основного ПМ управляющего контроллера.

***Старт и передача функции основного ПМ контроллера.*** В состав ПО контроллера входит задача арбитража, которая распределяет роли ПМ управляющего контроллера при старте системы и следит за состоянием ПМ в процессе работы. Каждому ПМ управляющего контроллера выделена линия GPTA, на которой он периодически меняет уровень сигнала, при этом каждый фронт вызывает прерывание центрального процессора дублирующего ПМ. В режиме работы при отсутствии потока прерываний от резервного ПМ к основному последний прекращает перекачку данных на резервный до тех пор, пока прерывания не возобновятся. При исчезновении потока прерываний от основного ПМ к резервному в течение заданного промежутка времени резервный становится основным. При включении комплекса каждый из ПМ управляющего контроллера начинает генерировать прерывания на дублирующем ПМ и одновременно ожидает прерывания от дублирующего ПМ в течение заданного таймаута. Если прерываний нет, то ПМ становится основным. Если прерывания имеются, ПМ становится основным или резервным в зависимости от номера слота, в котором он установлен.

***Обмен данными на уровне периферийного процессора*** осуществляется за счет простого одностороннего протокола. Основной ПМ является передатчиком (функция приемника отсутствует), резервный – приемником (функция передатчика отсутствует). Передатчик начинает обмен данными, если на линии готовности приемника высокий уровень сигнала. В этом случае на одной из управляющих линий выставляется высокий уровень сигнала, что вызывает прерывание периферийного процессора и вызов канальной программы приемника. Высокий уровень сигнала на этой линии держится в течение передачи всего сообщения. Сброс сигнала сигнализирует приемнику о конце передачи. Другая управляющая линия передатчика используется для индикации, что очередной байт передан, и приемник может его забрать.

***ПО контроллера УСО*** осуществляет прием/передачу данных от модулей УСО и передачу их на верхний уровень. Оно разработано на языке С в ОС РВ для Tricore TC1775 и активно использует аппаратные функции, встроенные в данный микроконтроллер.

### Подсистема связи по сети CAN

Подсистема связи по сети CAN предназначена для сбора контроллером УСО данных от удаленных объектов, а также для связи контроллера УСО с управляющим контроллером. Две сети CAN функцио-

нируют в режиме дублирования. Максимальная скорость передачи по сети CAN составляет 1 Мбит/с. Взаимодействие между контроллерами осуществляется по типу Producer-Consumer. Для передачи данных между контроллерами используются широковещательные сообщения, существенно повышающие скорость обмена данными по сравнению со взаимодействием типа запрос/ответ. С одним контроллером УСО могут взаимодействовать несколько управляющих контроллеров и наоборот.

Для синхронизации ввода/вывода по сети CAN передается специальная синхронизирующая телеграмма, задающая начало цикла обмена данными. Возможна гибкая настройка режимов обмена данными, когда часть данных будет передаваться в синхронном режиме (каждый такт синхронизации, через такт и т.д.), а часть в асинхронном – по внутреннему событию (через определенные интервалы времени или по изменению).

В каждом контроллере УСО задаваются параметры: период опроса – время между синхронизирующими телеграммами; окно обмена данными – время между синхронизирующей телеграммой и окончанием обмена данными ввода/вывода (синхронные телеграммы ввода/вывода, принятые после истечения этого времени, игнорируются). Если контроллер УСО не получает синхронизирующую телеграмму в течение N периодов опроса (например, в случае обрыва обеих линий CAN), он переводит свои выходы в состояние по умолчанию или в специальное предустанавливаемое состояние, задаваемое отдельно. Кроме того, все контроллеры передают через определенный интервал времени (задается на стадии конфигурации системы) специальную телеграмму, подтверждающую работоспособность данного контроллера. При помощи данного механизма возможно определение выхода из строя конкретного контроллера или отдельной сети CAN (участка сети).

### ПО верхнего уровня

Для создания системы сбора данных и ЧМИ в ПТК СМ СИКОН используется SCADA-система Phocus 4 для ОС РВ QNX4.25. Применение ОС РВ QNX и архитектурные особенности Phocus делают его чрезвычайно эффективным и надежным средством для разработки ответственных приложений с большим числом точек данных для малоресурсных и бездисковых систем.

Пакет Phocus своей мощностью и структурой обязан ОС QNX, которая имеет врожденные качества одноранговой сети со встроенной отказоустойчивостью, обеспечивающей удаленную загрузку и работу резервируемых систем. QNX включает POSIX-совместимую, устойчивую, многонитевую дисковую файловую систему, делающую тренды предыстории и запись данных о событиях надежными и безошибочными. QNX имеет свои собственные средства для работы в сети, обеспечивающие быструю связь, устойчивую к отказам (FLEET), равномерную загрузку и избыточность сети. Phocus идеально реализует возможности, предоставляемые современными процессорами, так как прикладные программы в среде Phocus работают в защищенном режиме, целиком используя 32-битовый код. Наконец, POSIX-образная надежная файловая структура диска делает данные более защищенными.

Пользовательский интерфейс Phocus разработан под графической оболочкой Photon microGUI, что делает его легким для изучения и интуитивно понятным в эксплуатации. Мощные функции визуализации обладают высокой производительностью и надежностью, что гарантирует отсутствие мерцаний и задержек. Несколько окон (отображения событий предыстории, статистики сервера ввода/вывода, серверов и др.) могут быть открыты одновременно и обновляться в режиме РВ. Стандартное меню операторского интерфейса включает таблицу данных для просмотра БД РВ. Отображатель мнемосхем способен выводить мнемосхемы, имеющие индивидуальный размер и такие характеристики, как минимальный уровень доступа пользователя, доступность к узлу и управление стилем окна. Данные трендов предыстории просматриваются через просмотрщик или как тренд, встроенный в пользовательскую мнемосхему. Точные значения в известное время могут быть показаны в режиме курсора. Генератор отчетов, используя предварительно составленный формат отчета, получает и форматирует данные для отображения и/или печати.

Утилита просмотра событий позволяет просматривать события, записанные задачей регистрации тревог/событий Phocus, и выбирать тревоги/события для просмотра по начальному и конечному времени, по их типу, имени сервера или группы, имени и типу записи, приоритету. Абсолютные приоритеты делают возможной параллельную обработку, например, в одном окне можно следить в РВ за трендом на дисплее, отображающем реальный процесс, и в то же время проводить модификацию БД в режиме on-line.

Помимо элементов интерфейса оператора разработчику доступны:

- построитель БД – средство описания групп и точек, которое задает предельные значения тревог, временной интервал записи данных предыстории, масштаб единиц и др.;
- построитель пользовательских мнемосхем – редактор векторной графики, включающий также средства динамизации при подключении к БД. С его помощью создаются стандартные объекты – прямоугольники, окружности, трубы, текст и др. Несколько объектов могут быть сгруппированы в составные пользовательские объекты. Имеются библиотеки групп векторных объектов (измерительные устройства, насосы, двигатели, здания) и символов bitmap. После создания каждого графического объекта его атрибуты могут быть соединены (можно несколькими связями) с полями записей БД на любом сервере сети. Например, объект может менять цвет, положение или может мерцать в случае тревоги;

• построитель трендов позволяет задать формат нескольких полей, на каждом из которых могут выводиться по несколько графиков;

• построитель отчетов позволяет задать форматы отчетов в виде шаблонов, в которые должны выводиться данные для анализа;

• вспомогательные инструменты, необходимые для конфигурации системы, включают менеджер доступа для управления пользовательским доступом, утилиту конфигурации сервера ввода/вывода для задания и управления работой сервера ввода/вывода, редактор сообщений, используемый для редактирования пользовательских сообщений, журнал системных ошибок и утилиту конфигурации сообщений тревог. В версии Phocus/OPUS 4.x имеется и модуль рецептов.

### Сервер БД РВ OPUS

В SCADA-пакете Phocus ядром системы является сервер БД РВ OPUS, который автоматически запускается в ядре Phocus. Эта ключевая часть пакета имеет очень небольшой (около 70 Кб) размер кода. OPUS способен работать непрерывно без остановки и перезагрузки. Этим достигается непрерывность мониторинга процессов.

С точки зрения программной архитектуры основу OPUS составляют несколько серверов (БД, ввода/вывода, предыстории и быстрой предыстории) и администраторов (доступа, управления, сообщений, исходных данных). Под сервером здесь понимается программная компонента, а не отдельный компьютер. Каждый сервер в OPUS может поддерживать одновременно работу нескольких серверов ввода/вывода. Каждая компонента, а также драйверы ввода/вывода реализованы как отдельные процессы в ОС. Один из процессов следит за состоянием всех остальных компонентов системы, и в случае сбоя перезапускает отказавшую программу. При этом ошибка не сказывается на работе системы в целом. Все процессы Phocus обмениваются данными через внутренние очереди и системные сообщения.

OPUS содержит технически совершенный сервер распределенной БД РВ. Эта резидентная в памяти БД РВ содержит упорядоченные группы записей данных, которые, в свою очередь, могут быть привязаны к внешним устройствам сбора данных и управления. Сервер OPUS управляет расположенными в памяти именованными записями, которые могут обновляться от внешних устройств таких, как ПЛК, модулей сбора данных или дискретного управления и распределяет их присоединенным к нему клиентам. Также сервер БД РВ OPUS обеспечивает управление пользовательским доступом, распределением тревог, обновлением данных пользователя, сервером ввода/вывода и интерфейсом управления.

Первоначально пользователь создает БД проекта для отображения ввода/вывода с присоединенных физических устройств ввода/вывода. Каждая точка БД затем присоединяется к серверу ввода/вывода посредством уникального идентификатора сервера ввода/вывода. Сервер ввода/вывода отвечает за связь с физическим устройством ввода/вывода, получение необходимых данных и запись их на сервер OPUS. Принятые сервером данные проходят внутреннюю обработку. Сначала проверяется изменение значений данных, если это происходит, то данные передаются в очередь для записи предыстории. Затем проверяются тревоги. Если любой флаг тревоги установлен или сброшен, то об этом сообщается менеджеру тревог, который создает сообщение тревоги и помещает данные в свой внутренний буфер.

Изменение данных передается менеджеру обновления. Он будет проверять наличие зарегистрированного клиента, связанного с этой точкой, и, если есть, добавляет заголовок данных записи в список клиентских обновлений. Данные будут прочитаны при ближайшем контакте клиента с сервером.

***Достоинства пакета Phocus:***

• использует все преимущества ОС РВ QNX, результатом чего является его высокая производительность, надежность и компактность;

• может работать с дублированными сетями, одна из которых – общая магистраль TCP/IP, а другая – детерминированная отказоустойчивая сеть QNX (Qnet или Fleet), обеспечивающая мгновенное переключение управления с основного сервера БД на сервер активного резерва;

• доступны все программы двусторонней передачи данных между платформой QNX и MS Windows, включая такие интерфейсы, как OPC (OPC сервер и клиент для OPUS) и HTML. Таким образом, задача интеграции с общекорпоративными системами предприятия могут быть легко решены;

• экономически выгоден и по цене сравним с другими SCADA, включая пакеты на платформе MS Windows.

Каждый сервер в Phocus может поддерживать одновременно работу нескольких серверов ввода/вывода, доступных для многих распространенных плат ввода/вывода, контроллеров и датчиков.

### Резервирование серверов Phocus в ПТК СМ СИКОН

Для обеспечения надежного и непрерывного мониторинга в составе ПТК СМ СИКОН Phocus конфигурируется исключительно с функцией активного резервирования. Сервер активного резерва предоставляет в сравнении с другими видами резервирования наиболее прогрессивный алгоритм для безотказной работы. Каждый сервер снабжается источником бесперебойного питания. Информация о работе этих источников также может стать доступной для операторов системы Phocus.

Главный и активный резервный серверы имеют единое имя и выполняемый набор задач. Все изменения данных отражаются на обоих серверах. В случае сбоя основного сервера происходит практически мгновенное переназначение в качестве главного сервера актив-

ного резерва. При восстановлении работы главного сервера он вновь становится резервным. Соединение главного и резервного серверов с ПЛК осуществляется по дублированным каналам Ethernet, обеспечивая надежную доставку данных в SCADA-систему.

### Заключение

ПО ПТК СМ СИКОН создано на базе ОС РВ, что позволяет использовать данный ПТК в проектах с высокими требованиями к надежности и отказоустойчивости системы управления. Исходные коды ПО систем как нижнего, так и верхнего уровня полностью контролируются отечественными разработчиками, так что при необходимости возможно их исследование и сертификация для применения в самых ответственных приложениях. ПТК СМ СИКОН с успехом применяется на ответственных объектах производства карбамида и аммиака (Таджик Азот), а также для испытания ракетных двигателей (НИИХиммаш). Планируется его адаптация для объектов энергетики.

ПТК СМ СИКОН можно рекомендовать к применению на ответственных участках опасных объектов химической, атомной и др. отраслей промышленности, требующих катастрофоустойчивости.

***Зиновьев Валерий Леонидович*** *– зам. директора ООО "Компьютерные комплексы",*
***Фрейдман Андрей Витальевич*** *– зам. директора Научного центра "Науцилус".*
*Контактные телефоны (495) 135-35-91, (495) 939-58-72.*
*E-mail: zin@kompex.ru freydman@nautsilus.ru*

## Системы противоаварийной автоматической защиты и "критического" управления на базе отказоустойчивых средств автоматизации Triconex

**Д.Ю. Свечников, П.Н. Кирюшин (Компания "Инвенсис Системс")**

*Представлен обзор систем противоаварийной защиты и управления критическими с точки зрения безопасности объектами, реализованных на аппаратных средствах повышенной отказоустойчивости фирмы Triconex.*

Подразделение Трайконекс (Triconex) в составе ООО "Инвенсис Системс" представляет на рынках России, стран СНГ и Балтии ряд продуктов, решений и инженерных услуг для систем противоаварийной автоматической защиты (ПАЗ), отказоустойчивого управления промышленными объектами, а также средства и системы управления турбокомпрессорным оборудованием.

### Противоаварийная защита

Противоаварийная защита – особое звено в АСУТП. Российским специалистам известен краткий термин – ПАЗ. За рубежом принято обозначать соответствующий круг функций термином ESD (Emergency Shut-Down), а группу оборудования -SIS (Safety Instrumented System). ПАЗ – сфера исключительной ответственности и жесткой стандартизации, выработанная на основе тяжкого опыта промышленных аварий и катастроф.

В России нормативным документом, формулирующим основные требования к ПАЗ, являются "Общие правила взрывобезопасности для взрывопожароопасных химических, нефтехимических и нефтеперерабатывающих производств" ПБ 09-540-03. Эти правила устанавливают ряд обязательных инженерных решений и ограничений (независимость функционирования ПАЗ от системы управления, резервирование, диагностика и самодиагностика систем и др.). При этом, однако, в документе нечетко разделены функции между системами управления и ПАЗ, присутствует ряд терминологических неопределенностей, а самое главное – взрывоопасность рассматривается в отрыве от прочих производственных опасностей (пожарной, газовой, связанной с движущимися механизмами и др.). Наличие большого числа отраслевых руководящих документов не столько закрывает нормативную неполноту, сколько создает путаницу.

Стандарты США и Западной Европы, получившие мировое признание, отличаются комплексным подходом к промышленным опасностям и исчерпывающей четкостью формулировок. Они охватывают все вопросы, начиная от контроля технических средств ПАЗ в процессе их производства и заканчивая вопросами эксплуатации и технического обслуживания. Главным критерием допуска технических средств и инженерных решений в системы ПАЗ является общий уровень опасности объекта, оцениваемый по числу возможных человеческих жертв в случае аварии. Стандарт DIN V 19250 определяет восемь классов опасности объектов от наименьшего AK1 до наивысшего AK8. Стандарт Международного Электротехнического Комитета IEC 61508 устанавливает четыре уровня полноты безопасности (Safety Integrity Level, SIL) от минимального SIL1 до максимального SIL4. Для каждого из указанных классов определены требуемые показатели надежности систем ПАЗ.

Сертификацию технических средств ПАЗ осуществляет Ассоциация Технического Надзора Германии (TUV) – независимая организация, сертификат которой официально признан в настоящее время более чем в 40 странах мира. Компания Triconex ведет последовательное и плодотворное сотрудничество с международными контролирующими и сертифицирующими организациями. Контроллеры Tricon и Trident имеют сертификаты TUV. Контроллеры архитектуры TMR (Triple Modular Redundancy) являются универсальным и наиболее функциональным микропроцессорным средством для уровней до AK6 и SIL3.