## **1** ОБЗОР ЛИТЕРАТУРЫ

## **1.1** Обзор существующих аналогов

На этапе проектирования системы были тщательно изучены существующие аналоги. Одним из наиболее приближенным примером является система автоматизации «DESIGO™» (см. рисунок 1.1).

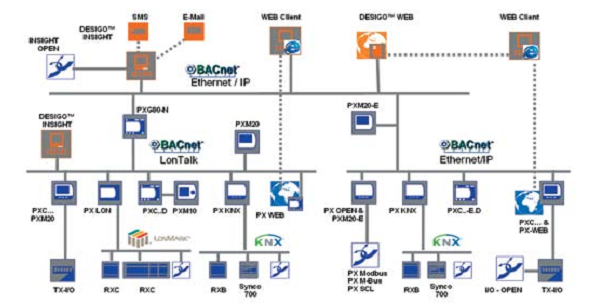


Рисунок 1.1- Система автоматизации «DESIGO™» [7]

Система автоматизации DESIGO™ построена на основе открытого протокола BACnet. Основным компонентом построения системы автоматизации зданий DESIGO™ являются свободно программируемые контроллеры DESIGO™ PX. Семейство контроллеров DESIGO™ PX содержит ряд компактных контроллеров с фиксированным набором точек ввода-вывода и модульных контроллеров, состоящих из процессорной части и модулей ввода-вывода (TX-I/O). Возможность написания прикладных программ для контроллеров DESIGO™ PX позволяет реализовать гибкие алгоритмы управления для любого технологического оборудования зданий.

Для организации автоматизации отдельных помещений используются стандартные контроллеры семейства DESIGO™ RX.

Контроллеры DESIGO™RX могут иметь коммуникацию по различным протоколам полевого уровня – LonWorks (RXC) или KNX (RXB) и могут легко интегрироваться в общую систему автоматизации.

В качестве средства контроля и управления могут быть использованы как специализированные панели оператора (PXM20 и PXM20-E), так и система диспетчеризации и управления зданиями DESIGO™ INSIGHT. Система диспетчеризации DESIGO™ INSIGHT представляет собой современную SCADA-систему с широкими возможностями организации локального и удаленного (Terminal Server) мониторинга и анализа данных, оперативного уведомления о неполадках (sms, e-mail, fax) и управления системами жизнеобеспечения здания. При использовании современных информационных технологий (Internet), можно также организовать мониторинг и управление при помощи WEB-браузера на основе решений PX™ WEB или DESIGO™ WEB.

Все системы жизнеобеспечения здания представляют собой единый комплекс, требующий организации единого мониторинга и управления. Система автоматизации, построенная на основе DESIGO™, предоставляет широчайшие возможности по интеграции различных систем в единую систему управления. Интеграция может осуществляться посредством специализированных модулей ввода-вывода I/O OPEN (Modbus, M-BUS, WILO, GRUNDFOS, SED), при помощи системных контроллеров PX OPEN(LonWorks, KNX, MODBUS, M-BUS) и в систему диспетчеризации INSIGHT™ OPEN(BACnet, OPC, MODBUS).

Основные моменты:

* свободно программируемые контроллеры – возможность реализации самых сложных алгоритмов.
* полноценная встроенная реализация протокола BACnet, протестированная независимой лабораторией.
* масштабируемое решение с использованием различных топологий
* широкие возможности по удаленному программированию, мониторингу и управлению
* современная динамично развивающаяся система

## **1.2** Протокол BACnet

BACnet (Building Automation and Control Networks) – это открытый сетевой протокол передачи данных, предназначенный для систем автоматизации зданий и сетей управления. Специализация протокола – инженерные системы зданий. Основная концепция BACnet – осуществление и стандартизация связи и взаимодействия различных устройств и программного обеспечения систем автоматизации от различных производителей.

Начало разработки нового протокола обмена данными припало на 1987 год. Целью разработки, как уже было отмечено выше, стало желание создать единый унифицированный и самостоятельный, вне зависимости от производителя железа ли программного обеспечения, стандарт сетей передачи данных в системах автоматизации и диспетчеризации зданий. Разработчик протокола, кампания ASHRAE пришла к заключению, что использование закрытых протоколов обмена данными в системах автоматики делает невозможным существование и комфортное использование устройств и программных продуктов от разных производителей. С 2003 года протокол BACnet имеет стандарт ISO (16484-5).

Суть технологии BACnet и принцип ее функционирования состоит в том, что физическая форма устройств в системе автоматики не имеет никакого значения, потому что BACnet – это не что иное, как набор правил, по которым устройства системы автоматизации взаимодействуют между собой. Таким образом, есть возможность выбрать оптимальное оборудование от каждого производителя и соединить их в одну систему. Вместо привязанности к определенному бренду, появляется свобода в компоновке оборудованием, как новых систем управления, так и уже функционирующих. Новые устройства легко интегрируются с ранее установленными.

Под понятием BACnet устройство понимается устройство системы автоматизации, будь то контроллер, датчик или еще что-то, поддерживающее протокол BACnet.

Для осуществления взаимодействия между устройствами, что гарантируется технологией BACnet, необходимо, что бы все алгоритмы работы этих устройств были описаны с помощью стандартных функциональных блоков BIBB (BACnet Interoperability Building Block). Эти блоки легко взаимодействуют между собой, что упрощает работу инженеров, программистов и прочих специалистов. Все поддерживаемые блоки BIBB, свойства их взаимодействия, детальное описание типа для каждого из устройств BACnet описаны в специальном документе – PICS (Protocol Implementation Conformance Statement).

Поскольку протокол BACnet построен на объектно-ориентированном принципе, каждое устройство BACnet описывается как стандартный объект или их набор. Количество элементов в наборе не ограничено.

В стандарте определены следующие объекты и типы:

* аналоговый вход (AI);
* аналоговый выход (AO);
* аналоговое Значение (AV);
* двоичный Вход (BI);
* двоичный Выход (BO);
* двоичное Значение (BV);
* вход Со Многими Состояниями (Multi-State Input);
* выход Со Многими Состояниями (Multi-State Output);
* календарь (Calendar);
* регистрация события (Event-Enrollment);
* файл (File);
* класс уведомления (Notification-Class);
* группа (Group);
* цикл (Loop);
* программа (Program);
* расписание (Schedule);
* команда (Command);
* устройство (Device);
* HVAC;

Все в том же стандарте, описаны прикладные задачи, которые выполняют объекты BACnet. Среди них представлены:

* доступ к файлам;
* доступ к объектам;
* создание и обработка событий;
* удаленное управление устройствами;
* виртуальный терминал;

Поскольку BACnet построен на модели «клиент-сервер», сообщения протокола являются по сути сервисными запросами. Поддерживаются 35 видов сообщений, которые подразделяются на 5 групп (или классов).  
BACnet поддерживает 5 типов локальных сетей:

* Ethernet (IEEE 802.3/ISO 8802-3)
* ARCNET (ANSI/ATA 878.1)
* MS/TP-a
* PTP
* LonTalk

## **1.3** Системы SCADA

SCADA (*supervisory control and data acquisition*, диспетчерское управление и сбор данных) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. SCADA может являться частью АСДУ ИС, системы экологического мониторинга, научного эксперимента, автоматизации здания и т. д. SCADA-системы используются во всех отраслях хозяйства, где требуется обеспечивать автоматическое управление технологическими процессами в режиме реального времени. Данное программное обеспечение устанавливается на компьютеры и, для связи с объектом, использует драйверы ввода-вывода или OPC / DDE-серверы. Программный код может быть как написан на языке программирования (например на C++), так и сгенерирован в среде автоматизированного проектирования.

Иногда SCADA-системы комплектуются дополнительным ПО для программирования промышленных контроллеров. Такие SCADA-системы называются интегрированными и к ним добавляют термин SoftLogic.

Термин «SCADA» имеет двоякое толкование. Наиболее широко распространено понимание SCADA как приложения, то есть программного комплекса, обеспечивающего выполнение указанных функций, а также инструментальных средств для разработки этого программного обеспечения. Однако, часто под SCADA-системой подразумевают программно-аппаратный комплекс. Подобное понимание термина SCADA более характерно для раздела телеметрия.

Значение термина SCADA претерпело изменения вместе с развитием технологий автоматизации и управления технологическими процессами. В 80-е годы под SCADA-системами чаще понимали программно-аппаратные комплексы сбора данных реального времени. С 90-х годов в связи с тем, что всё большая часть функций автоматического управления решается не аппаратными, а программными средствами, термин SCADA больше используется для обозначения только программной части человеко-машинного интерфейса АСУ ТП.

**1.3.1** Основные задачи, решаемые SCADA-системами

SCADA-системы решают следующие задачи:

* + обмен данными с «устройствами связи с объектом», (то есть с промышленными контроллерами и платами ввода/вывода) в реальном времени через драйверы.
  + обработка информации в реальном времени.
  + логическое управление.
  + отображение информации на экране монитора в удобной и понятной для человека форме.
  + ведение базы данных реального времени с технологической информацией.
  + аварийная сигнализация и управление тревожными сообщениями.
  + подготовка и генерирование отчетов о ходе технологического процесса.
  + осуществление сетевого взаимодействия между SCADA-станциями (компьютерами).
  + обеспечение связи с внешними приложениями (СУБД, электронные таблицы, текстовые процессоры и так далее). В системе управления предприятием такими приложениями чаще всего являются приложения, относимые к уровню MES.

SCADA-системы позволяют разрабатывать АСУ ТП в клиент-серверной или в распределённой архитектуре.

**1.3.2** Основные компоненты SCADA

SCADA-система обычно содержит следующие подсистемы:

* Драйверы или серверы ввода-вывода – программы, обеспечивающие связь SCADA с промышленными контроллерами, счётчиками, АЦП и другими устройствами ввода-вывода информации.
* система реального времени – программа, обеспечивающая обработку данных в пределах заданного временного цикла с учетом приоритетов.
* человеко-машинный интерфейс (HMI, англ. Human Machine Interface – инструмент, который представляет данные о ходе процесса человеку оператору, что позволяет оператору контролировать процесс и управлять им. Программа-редактор для разработки человеко-машинного интерфейса.
* система логического управления – программа, обеспечивающая исполнение пользовательских программ (скриптов) логического управления в SCADA-системе. Набор редакторов для их разработки.
* база данных реального времени – программа, обеспечивающая сохранение истории процесса в режиме реального времени.
* система управления тревогами – программа, обеспечивающая автоматический контроль технологических событий, отнесение их к категории нормальных, предупреждающих или аварийных, а также обработку событий оператором или компьютером.
* генератор отчетов – программа, обеспечивающая создание пользовательских отчетов о технологических событиях. Набор редакторов для их разработки.
* внешние интерфейсы – стандартные интерфейсы обмена данными между SCADA и другими приложениями. Обычно OPC, DDE, ODBC, DLL и так далее.

**1.3.3** Концепции систем

Термин SCADA обычно относится к централизованным системам контроля и управления всей системой, или комплексами систем, осуществляемого с участием человека. Большинство управляющих воздействий выполняется автоматически RTU или ПЛК. Непосредственное управление процессом обычно обеспечивается RTU или PLC, а SCADA управляет режимами работы. Например, PLC может управлять потоком охлаждающей воды внутри части производственного процесса, а SCADA система может позволить операторам изменять уста для потока, менять маршруты движения жидкости, заполнять те или иные ёмкости, а также следить за тревожными сообщениями («алармами»), такими как – потеря потока и высокая температура, которые должны быть отображены, записаны, и на которые оператор должен своевременно реагировать. Цикл управления с обратной связью проходит через RTU или ПЛК, в то время как SCADA система контролирует полное выполнение цикла.

Сбор данных начинается в RTU или на уровне PLC и включает показания измерительного прибора. Далее данные собираются и форматируются таким способом, чтобы оператор диспетчерской, используя HMI мог принять контролирующие решения – корректировать или прервать стандартное управление средствами RTU/ПЛК. Данные могут также быть записаны в архив для построения трендов и другой аналитической обработки накопленных данных.

**1.3.4** Некоторые распространенные SCADA

На мировом рынке представлено более 50 продуктов, которые можно отнести к SCADA-системам, продукты различаются:

* + по требуемой операционной системе, наиболее распространена Windows (Linux, Mac OS встречаются намного реже для данного продукта);
  + по количеству поддерживаемого оборудования, протоколов (почти все SCADA поддерживают Modbus, LonWorks, BACnet, OPC, DDE, реже протоколы специфического оборудования, со своим нестандартным протоколом типа счётчика электрической энергии Меркурий 230ART, климатического контроллера Danfoss ECL-300, приборы фирмы Овен и т. п.);
  + по цене, по соотношению цена/качество, в общем случае на рынке представлены как полностью бесплатные SCADA, недорогие SCADA с ценой лицензии на 60 тегов от $100 (DATARate), так и SCADA ценой порядка $100 тыс., при максимальной комплектации – при количестве тегов более 5000, нескольких АРМ диспетчера (WinCC, InTouch, Citect);
  + частный случай условно-бесплатные SCADA, c ограничением по времени работы без перезапуска (обычно 1 час), или по количеству тегов (обычно 8-50), или по количеству одновременно поддерживаемых протоколов (обычно 1);
  + по наличию и типу ключа аппаратной защиты (программный ключ файл, аппаратный USB или LPT-ключ, программная «привязка» к оборудованию), среди прочих факторов ключ платной SCADA в любом случае замедляет первоначальное развертывание и замену вышедшего из строя сервера;
  + по наличию прочих функций (поддержка резервирования, генераторы отчетов, удаленный доступ, веб-интерфейс и тому подобное).

Полностью бесплатные SCADA: OpenSCADA, Rapid SCADA, FreeSCADA, SCADA-ГИНЭС, Inductive Automation Ignition.

Условно-бесплатные SCADA, достаточные для автоматизации малого технологического процесса и изучения без покупки лицензии, возможность работы в течение неограниченного времени:

* + Simp Light Free – ограничение 8 тегов;
  + MasterSCADA – ограничения 32 тега для MasterSCADA RT32 без дополнительных возможностей или 1 час полнофункциональной работы для MasterSCADA Demo;
  + IGSS – ограничение 50 объектов (ориентировочно 150 тегов) и выбор одного протокола передачи данных (IGSS FREE50), по другому типу лицензии ограниченно время работы без перезапуска на 1 час и 1000 объектов (DEMO Mode);
  + Контар АРМ – поддерживает только с контроллеры производства ОАО «МЗТА»;
  + IntegraXor свободна для 128 Modbus I/O;
  + Каскад. Демо-версия имеет ограничение на 32 физических канала ввода/вывода и 2 часа непрерывной работы, включает себя полную справочную систему, SQL-сервер Firebird 2.5, WEB-модуль (реализация WebSCADA) и ряд проектов, демонстрирующих возможности системы. SCADA интегрирована с SoftLogic-системой KLogic, и, как следствие, реализована сквозная технология программирования алгоритмов контроллеров и рабочих станций. При покупке лицензии время работы не ограничивается, лицензия выдается по числу каналов или устройств сервера доступа к данным и наличию дополнительных клиентских модулей;
  + Vijeo Citect – позволяет создать и отладить полноценный проект без приобретения лицензий, при отсутствии лицензий включается демо-режим, в котором проект запускается на ограниченное время, после истечения этого времени проект необходимо перезапустить. Лицензируется только среда исполнения (Runtime), среда разработки распространяется свободно. В комплекте идет стандартный набор драйверов для подключения к контроллерам и RTU разных производителей. Всего насчитывается более 100 типов устройств, без учета поддержки стандартных протоколов, таких как OPC, Modbus и так далее. В отсутствии контроллера или контроллеров проект можно разрабатывать и отлаживать благодаря эмуляции точек ввода-вывода конфигурируемых под конкретный контроллер.

Прочие SCADA: Simatic WinCC, Intouch Wonderware, Trace mode, Genesis, SCADA Infinity, PcVue Solutions, RSView, ClearSCADA, DATARate, Контур, Круг-2000, ZenOn, Winlog, iFix, InduSoft Web Studio SCADA, Wizcon, Vijeo Citect, Статус-4, Каскад, Энтек, Sitex, Elipse E3, Elvis, Realflex RealWin SCADA, Broadwin (Advantech) WebAccess, General Electric Proficy Cimplicity, WellinTech SCADA, Factory Link (с 2012 года не поддерживается разработчиком), Monitor Pro (базировалась на Factory Link, рекомендована замена на Vijeo Citect), Vijeo Look (рекомендована замена на Vijeo Citect).

**1.3.5** WebSCADA

Под термином WebSCADA, как правило, понимается реализация человеко-машинного интерфейса (HMI) SCADA-систем на основе web-технологий.

Это позволяет осуществлять контроль и управление SCADA-системой через стандартный браузер, выступающего в этом случае в роли тонкого клиента.

Архитектура таких систем включает в себя WebSCADA-сервер и клиентские терминалы – ПК, КПК или мобильные телефоны с Web-браузером. Подключение клиентов к WebSCADA-серверу через Internet/Intranet позволяет им взаимодействовать с прикладной задачей автоматизации как с простой web или WAP-страницей. Однако на данном этапе развития WebSCADA ещё не достигло уровня широкого промышленного внедрения, так как существуют сложности с защитой передаваемой информации. Кроме этого, реализация функций управления через незащищенные каналы связи противоречит соображениям безопасности любого промышленного объекта. В связи с этим, в большинстве случаев Web-интерфейсы используются в качестве удаленных клиентов для контроля и сбора данных.

**1.3.6** Уязвимость

SCADA-системы могут быть уязвимы для хакерских атак, так, в 2010 году с использованием вируса Stuxnet была осуществлена атака на центрифуги для обогащения урана в Иране. Таким образом, для защиты информационных комплексов, содержащих SCADA-системы, требуется соблюдение общих требований информационной безопасности.

## **1.4** Аналитический обзор АСДУ ИС

АСДУ ИС зданием представляет собой комплекс мероприятий и программно-технических решений, обеспечивающих снижение эксплуатационных расходов за счет безаварийной и экономически эффективной эксплуатации здания.

Как правило, в сложных автоматических системах управления, предназначенных для управления зданием, можно выделить следующую иерархию:

1. Инженерные системы (отопление, вентиляция, освещение, электроснабжение и другое);
2. Оборудование, обеспечивающее работу инженерной системы (котлы, вентиляторы, насосы и прочее);
3. Автоматика оборудования, позволяющая объединить отдельные устройства в целостный комплекс для выполнения поставленной задачи без участия человека;
4. Единая сеть автоматики объекта, позволяющая организовать обмен данными между контроллерами автоматизации;
5. Система диспетчеризации (включает в себя сеть автоматики оборудования, но также может быть дополнена различными приборами, предназначенными для сбора данных);
6. Система интеллектуального принятия решений и задания параметров работы оборудования (при наличии данного звена к системе применим термин «Интеллектуальное Здание»);
7. Человек или группа людей (технические специалисты, экономисты), корректирующие и управляющие работой систем здания в целом.

Существует заблуждение, что АСДУ ИС оборудования сама по себе и есть система управления зданием. В основу системы автоматики всего лишь заложен принцип исключения человека из цепи регулирования некоторых параметров в данном конкретном оборудовании. При этом сохраняется базовая посылка: «Если это нельзя сделать в ручном режиме, то это нельзя автоматизировать».

Нижний уровень АСДУ ИС зданием содержит различные датчики, исполнительные механизмы и контроллеры управления. Качественная работа инженерной системы невозможна без надежной и правильной работы оборудования, присутствующего в данной системе. Качество работы оборудования напрямую зависит от применяемых в контроллерах алгоритмов управления. Применяемые в автоматизации оборудования зданий контроллеры делятся на два основных типа: конфигурируемые и свободно-программируемые.

Конфигурируемый контроллер содержит в себе программу и конечный набор определенных алгоритмов, написанных производителем контроллера. Свободнопрограммируемые контроллеры содержат в себе только среду исполнения, а написание алгоритмов и программ предоставляется пользователю. В простых инженерных системах зачастую достаточно применять конфигурируемые контроллеры, так как заводские алгоритмы соответствуют алгоритмам, по которым функционирует оборудование. Если же система сложная, то может сложиться ситуация, когда, казалось бы самое элементарное действие не может быть выполнено из-за ограниченности алгоритма.

Свободнопрограммируемые контроллеры позволяют реализовать любой сколь угодно сложный алгоритм работы оборудования и, как правило, их применение единственный способ организовать совместную работу различного оборудования или даже нескольких систем.

Вне зависимости от сложности, АСДУ ИС должна получать «уставки» (задания на поддержание тех или иных параметров) от человека, либо от системы автоматики другой единицы оборудования, либо от (или с помощью) системы более высокого уровня (например, рабочей станции диспетчера).

Без организующей АСДУ высокого уровня система автоматики объекта остается лишь разрозненным набором оборудования, а обеспечение взаимодействия между элементами данного набора ложится на плечи человека (иными словами, инженеру придется бегать по объекту с блокнотом и нажимать кнопки, стараясь ничего не упустить).