БАЗОВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ "ЦИФРОВОЙ ПОДСТАНЦИИ"

Синицын Максим Анатольевич

магистрант, ФГБОУ ВО НИУ «МЭИ», РФ, г. Москва

«Цифровая подстанция» (ЦПС) – это сложный инфраструктурный объект, представляющий собой соединение как первичного технологического оборудования, осуществляющего прием, преобразование, распределение и передачу электроэнергии потребителям, так и систем и средств автоматизации с возможностью удаленного мониторинга, контроля и управления состоянием первичного оборудования. С технической точки зрения, ЦПС – это обычная подстанция с высоким уровнем автоматизации, построенная не на релейной логике, а с помощью микропроцессорных терминалов РЗА (интеллектуально-электронных устройств – ИЭУ), сетевых коммутаторов, преобразователей интерфейсов, серверов обработки и архивирования данных, автоматизированных рабочих мест (АРМ) оперативного персонала, устройств организации единого времени, устройств приема и передачи информации. Общая структурная схема ЦПС представлена на рис.1.

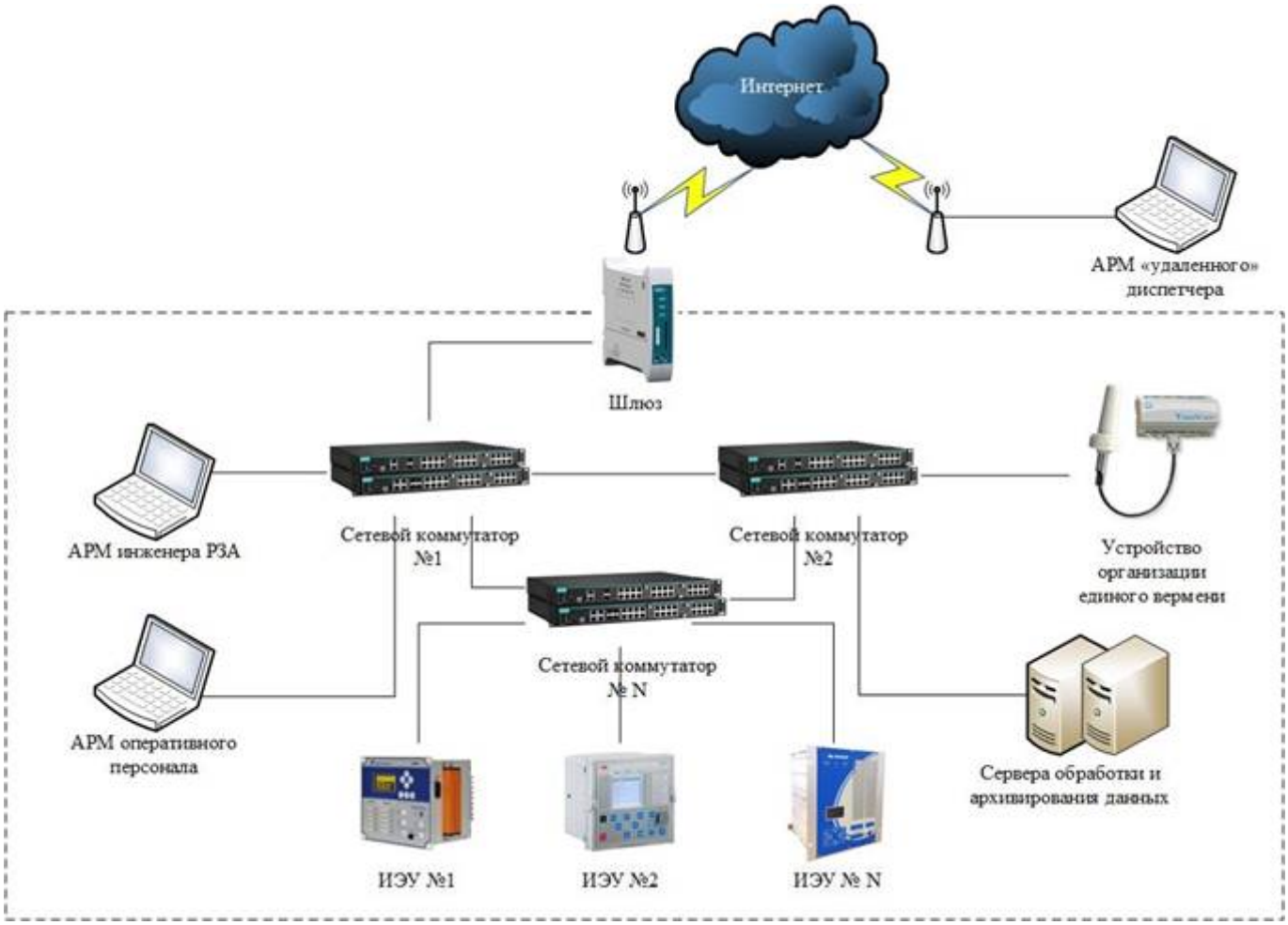

Рисунок 1. Общая структурная схема ЦПС

Синицын М.А. Базовые принципы построения "Цифровой подстанции" // Молодежный научный форум: Технические и математические науки: электр. сб. ст. по мат. LII междунар. студ. науч.-практ. конф. № 12(52).
URL: https://nauchforum.ru/archive/MNF_tech/12(52).pdf *(дата обращения: 08.09.2025)*

Устройства РЗА

В системе автоматизации ЦПС устройства РЗА осуществляют сбор информации о состоянии коммутационных аппаратов – от соответствующих блок-контактов, о токовой нагрузке – от трансформаторов тока, о напряжении на шинах ПС – от трансформаторов напряжения. Далее происходит обработка полученной информации и выдача управляющего воздействия – в виде подачи управляющего сигнала на электромагниты включения и отключения КА.

Конфигурирование микропроцессорных терминалов РЗА происходит в специальных программах-конфигураторах, которые разрабатываются производителями этих устройств. Например, для устройств SEPAM от компании Schneider Electric – это SFT, для устройств БМРЗ от компании Механотроника – это Конфигуратор-МТ, для устройств REC, REL, RET, REG, REF от компании ABB – это PCM600. С помощью программ-конфигураторов решаются вопросы задания уставок защит, параметрирование дискретных и аналоговых входных и выходных каналов, написание логики работы устройства. Внешний вид терминала РЗА представлен на рис.2.

Рисунок 2. Внешний вид терминала РЗА

Для микропроцессорных устройств существуют такие понятия как «интерфейс связи» и «протокол связи». Интерфейс – это физический канал для передачи данных, т.е. провод с несколькими токопроводящими жилами изолированными друг от друга. Наиболее распространены интерфейсы Ethernet, RS-485, RS-232 и другие. Протокол – это набор правил, которые управляют обменом информацией. Он определяет синтаксис и семантику сообщений, операции управления, синхронизацию и состояния при коммуникации. Для людей – алфавит, правила построения слов, предложений, текста, правильное произношение – это своеобразный протокол связи! По такому же принципу «общаются» между собой микропроцессорные терминалы, только для обмена информацией взаимодействующие устройства используют определенную последовательность сигналов логических нулей и единиц, и, естественно, для однозначного интерпретирования информации устройства

должны иметь одинаковый протокол обмена. Наиболее распространены промышленные протоколы Modbus, Profibus, OPC и другие. В частности, для автоматизации подстанций разработан стандарт МЭК-61850 со своим набором телекоммуникационных протоколов: MMS, GOOSE, SV.

Сервер обработки и архивирования данных

Сервер обработки и архивирования данных – это обычный компьютер (может быть в промышленном исполнении), на котором установлена SCADA-система (Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных). Основная его функция – это сбор, обработка и архивирование данных. В крупных проектах выделяют несколько серверных компьютеров под разные задачи – ввода/вывода данных и отдельно под архивирование данных. Архивирование чаще всего происходит с помощью баз данных, таких как MS SQL, Firebird, PostgreSQL, MySQL и других. Ввод и вывод данных осуществляет OPC-сервер. Его функция – это опрос микропроцессорных терминалов по определенному протоколу и предоставление информации в SCADA-систему по протоколу OPC. Зачастую, все SCADA-системы этот протокол OPC «понимают» и легко «общаются» с OPC-серверами. Ключевую роль в функционировании технологического процесса играет SCADA-система. Это своеобразный координатор, человеко-машинный интерфейс, «управляющий» системы автоматизации. SCADA-система обменивается данными с OPC-сервером, обрабатывает их, архивирует и с помощью средств визуализации предоставляет оператору в простой и понятной форме. Структура такой системы представлена на рис.3.

Рисунок 3. Структура компонентов сервера обработки и архивирования данных

АРМ оперативного персонала

Помимо серверов обработки и архивирования данных в системе автоматизации ПС присутствуют АРМы оперативного персонала. В зависимости от возложенных на них функций АРМы предоставляют доступ к текущим и архивным данным на сервере, возможность мониторинга и управления состоянием КА, анализа аварийных режимов работы электроустановки, изменения уставок технологических защит. АРМ оперативного персонала также представляет собой компьютер с установленной SCADA-системой, он «общается» с сервером обработки и архивирования данных, получая и передавая ему необходимую информацию. Структурная схема такого «общения» представлена на рис.4.

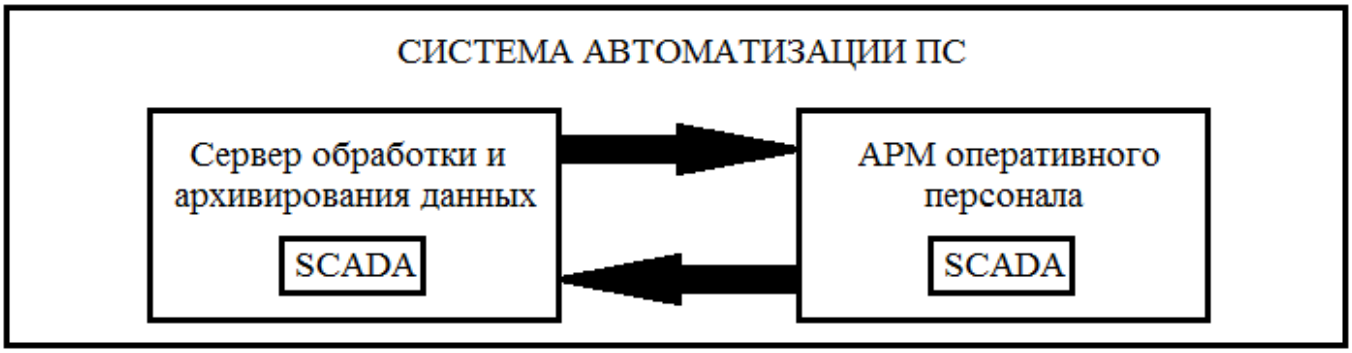

Рисунок 4. Обмен информацией в системе автоматизации ПС

Права доступа и полномочия оперативного персонала должны ограничиваться, чтобы максимально исключить влияние человеческого фактора на функционирование процесса, что достигается средствами самой SCADA-системы. Необходимо давать оператору только те права доступа, которые регламентированы его должностной инструкцией и другими правилами. Пример внешнего вида мнемосхемы, которую видит оператор, представлена на рис.5 [1, с. 43].

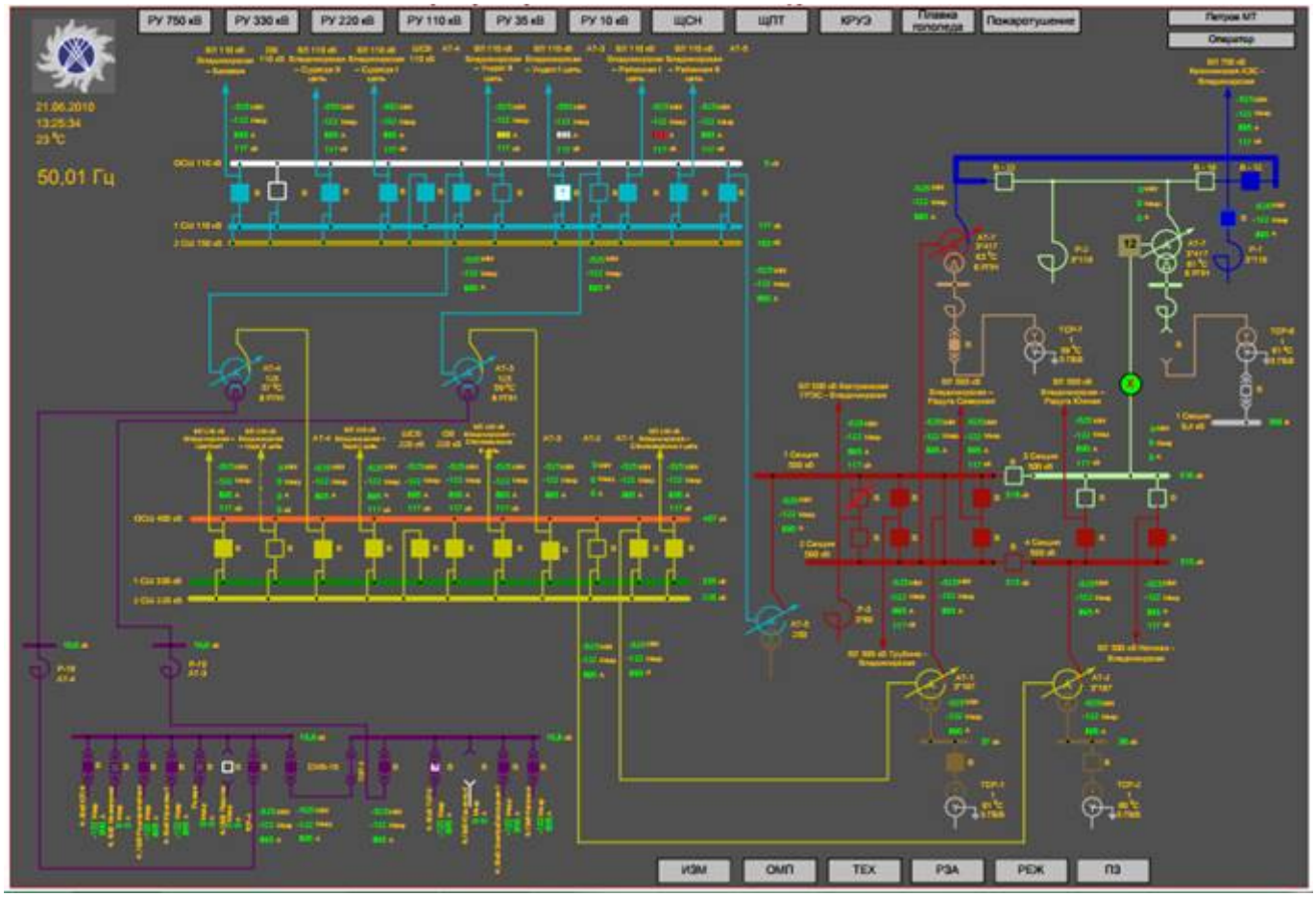

Рисунок 5. Пример внешнего вида главной мнемосхемы ЦПС

Устройства организации единого времени

Все микропроцессорные ИЭУ в системе автоматизации фиксируют события, происходящие на

объекте управления, с привязкой к метке времени. Для возможности анализа причинно-следственных связей событий все устройства должны работать синхронно. В самом простом варианте, для синхронизации работы может применяться один из компьютеров сети. Если необходима привязка к точному единому времени, то необходимо использовать устройство организации единого времени (рис.6)

Рисунок 6. Устройство организации единого времени

Устройство представляет собой антенну для связи с космосом и сервер точного времени, выдающий отметки точного времени по различным протоколам: NTP, PTP, PPS и другим.

Устройства приема и передачи информации «удаленному» диспетчеру

Для создания распределенных систем управления применяются промышленные модемы (рис.7), работающие по распространенным GSM/GPRS каналам связи. С помощью таких модемов осуществляется взаимодействие системы автоматизации, находящейся непосредственно на ПС, и «удаленного» диспетчера. С целью организации единой распределенной сети применяются VPN-технологии, позволяющие создать одну общую локальную сеть для взаимодействия всех компонентов системы автоматизации.

Рисунок 7. Внешний вид GSM/GPRS модема ПМ01 фирмы ОВЕН

Резервирование. Увеличение надежности ПС

С целью увеличения надежности любой системы автоматизации, в том числе и ЦПС, применяется резервирование. Резервируются сервера обработки и архивирования данных, OPC-сервера, физические каналы связи, вся система в целом. Принцип резервирования заключается в следующем: существуют два сервера обработки и архивирования данных, один – основной, другой – резервный. В нормальном режиме работы основной сервер производит опрос OPC-серверов, ведет обработку данных, выполняет вычисления и архивацию, отправляет резервному текущие и архивные данные, что обеспечивает их идентичность на обоих компьютерах. Резервный не производит опрос, не выполняет обработку, а только принимает данные от основного. При возникновении нештатной ситуации – отказ основного сервера, потеря связи основного и резервного серверов, ошибки связи с OPC-серверами, управление процессом переходит на резервный компьютер.

Существующие проблемы

Несмотря на высокую технологичность, кажущуюся защищенность, краеугольным камнем для разработчиков является защита от несанкционированного доступа в систему и кибератак на незащищенные телекоммуникационные протоколы.

В июне 2017 года были опубликованы результаты исследований вредоносного ПО, которое получило название CrashOverride/Industroyer. Эксперты компаний ESET, Dragos Inc. и ряд независимых специалистов пришли к выводу, что это вредоносное программное обеспечение

предназначено для нарушения рабочих процессов в промышленных системах управления (ICS), в частности, на электрических подстанциях. CrashOverride/Industroyer позволяет напрямую управлять выключателями и прерывателями цепи в сети электрических подстанций [3].

Зловред умеет работать с четырьмя промышленными протоколами, распространенными в электроэнергетике, управлении транспортом, водоснабжении и других критических инфраструктурах: IEC 60870-5-101 (aka IEC 101), IEC 60870-5-104 (aka IEC 104), IEC 61850, OLE for Process Control Data Access (OPC DA) [3].

Отправив устройствам специально сформированную последовательность данных, можно их отключить. Для последующего включения необходима их ручная перезагрузка [3].

В случае использования этой функции вредоносным ПО при критической ситуации в электросети физический ущерб может не ограничиться отключением электроснабжения – атака может привести к повреждению оборудования вследствие несрабатывания релейной защиты и автоматики. При особым образом спланированных перегрузках атака в одном месте может привести к каскадным отключениям электроснабжения на нескольких подстанциях [3].

Таким образом, CrashOverride/Industroyer — это настоящее кибероружие, нацеленное на промышленные системы [3].

В условиях необходимости удовлетворять комплексу требований по функциональной надежности, безопасности, быстродействию телекоммуникационных протоколов, а также по оптимальности затрат наиболее перспективно выглядит реализация концепции встраивания средств криптографической защиты информации в каждый элемент или в каждую подсистему цифровой подстанции [2].

Экономическая эффективность

Сложно однозначно оценить экономическую эффективность от внедрения ЦПС, ведь стоимость оборудования, программного обеспечения, работ по проекту чаще всего является конфиденциальной информацией. Несмотря на сокращение времени проектирования за счет типизации схемных и функциональных решений, сокращение объема монтажных и наладочных работ за счет монтажа оборудования, конфигурирования и тестирования устройств РЗА прямо на заводе, сокращение затрат на обслуживающий персонал, значительными остаются капитальные затраты на средства программной автоматизации ПС, затраты на пуско-наладочные работы.

На мой взгляд, экономическую эффективность от внедрения ЦПС можно увеличить при акцентировании внимания на интегрировании в нее системы диагностического мониторинга (СДМ), позволяющей видеть действительное текущее состояние оборудования, рационально организовывать систему текущего обслуживания и ремонта (ТО и Р), выявлять дефекты на ранних стадиях их развития и предотвращать крупные аварии, влекущие за собой замену дорогостоящего оборудования. Перспективной видится задача разработки алгоритма СДМ для ИЭУ в соответствии с теорией надежности и встраивания этого устройства в общую структурную схему автоматизации ПС, которое будет обрабатывать информацию о состоянии первичного оборудования и выдавать рекомендуемые меры воздействия на него.

Заключение

«Цифровая подстанция» – это новая ступень развития энергетики. С применением микропроцессорных устройств возрастают требования к квалификации и уровню знаний обслуживающего персонала. Базовое понимание принципов и назначения элементов системы автоматизации ПС дает возможность быстро проводить диагностику неработоспособных узлов, выявлять причины отказов, как оборудования, так и средств программной автоматизации.

В статье рассмотрены базовые принципы построения ЦПС, описана ее структура и функции входящих в нее технологических элементов.

Список литературы:

1. Правила оформления нормальных схем электрических соединений подстанций и графического отображения информации посредством ПТК и АСУ ТП // СТО 56947007-25.040.70.101-2011-ФСК ЕЭС.

2. http://www.fsk-ees.ru/upload/docs/STO_56947007-25.040.70.101-2011.pdf (дата обращения: 20.11.2017)

3. Зинин В.М., Подлесный А.М., Карантаев В.Г. Цифровая подстанция – объект критической инфраструктуры // Автоматизация и IT в энергетике.

4. http://insat.ru/articles/?id=51664 (дата обращения: 20.11.2017)

5. Kaspersky Lab ICS CERT. Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2017.

6. https://ics-cert.kaspersky.ru/reports/2017/09/28/threat-landscape-for-industrial-automation-systems-in-h1-2017/ (дата обращения: 20.11.2017)