X МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «АВТОМАТИЗАЦИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ЭНЕРГЕТИКЕ 2022» В РАМКАХ ДЕЛОВОЙ ПРОГРАММЫ «МЕЖДУНАРОДНОГО ФОРУМА «ЭЛЕКТРИЧЕСКИЕ СЕТИ РОССИИ 2022».

Обзор. Часть 1

А.А. ЕГОРОВ (Журнал “Автоматизация и IT в энергетике”)

АВТОМАТИЗАЦИЯ & IT в энергетике
научно-производственный журнал

В материале представлен обзор докладов Егорова А.А., Цветкова М.Ю., Литвинова П.В., Крюкова О.В., сделанных на X Международной научно-практической конференции “Автоматизация и информационные технологии в энергетике 2022”, проведенной в рамках деловой программы “Международного Форума “Электрические сети России-2022” 23 марта 2022 г.

Ключевые слова: *импортозамещение; сетевой комплекс РФ; интеллектуальное устройство; мониторинг энергоустановок; smartRTU; имитационное моделирование; IT инфраструктура; иммунитет; киберугрозы; свойство самовосстановления; инновационные возможности; мониторинг распределительных устройств; КТП “КАСКАД”.*

В Москве в павильонах 55 и 57 ВДНХ 22-25 марта 2022 года состоялся Международный форум “Электрические сети” (МФЭС) – мероприятие, включающее в себя выставку производителей комплектующих и оборудования для электроэнергетики и деловую программу. Напомним, что в связи с форс-мажорными обстоятельствами (неоднократными вспышками коронавируса Covid-19, созданием временных госпиталей в выставочных павильонах и введением запрета на проведение массовых мероприятий) даты и место проведения Международного форума “Электрические сети” с 2020 года менялись несколько раз. Таким образом, вместо уже ставшей традиционной для проведения этого мероприятия первой недели декабря, организатором (ЗАО “Электрические сети”) было принято решение провести Международный форум “Электрические сети” в марте 2022 года, организовав площадку в доступных на данное время павильонах ВДНХ. Разместить экспозицию в павильоне 75, как это было в последние годы, оказалось по ряду причин невозможным. Были выделены павильоны 55 и 57.

Рис. 1. Павильон 55 ВДНХ

Напомним, что павильон 55 ВДНХ (рис. 1) раньше назывался “Электрификация”, именно там много лет назад зародился МФЭС. А вот павильон 57 оказался необычным выбором – в нем постоянно размещается экспозиция “Россия – моя история”, но она находилась на техническом обслуживании, что позволило провести там выставку электросетевого оборудования.

Параллельно с выставкой в рамках МФЭС 2022 была проведена большая деловая программа в виде панельных дискуссий, научно-практических конференций и круглых столов. В этой программе были охвачены наиболее актуальные вопросы создания и эксплуатации сетевого хозяйства России.

Журнал “Автоматизация и IT в энергетике” традиционно поддержал мероприятие в качестве отраслевого партнера Форума МФЭС 2022, организовав X Юбилейную научно-

практическую конференцию на тему "Современное состояние и тенденции развития информационно-управляющих систем и телекоммуникаций в энергетике (контроль, учет, управление, телекоммуникации, безопасность, импортозамещение)".

X Юбилейная международная научно-практическая конференция проводилась при поддержке Академии военных наук РФ (научное отделение "Проблемы регионального развития"), Российского Национального Комитета СИГРЭ (Подкомитет D2 РНК СИГРЭ "Информационные системы и телекоммуникации") и "Института систем управления, информатики и электроэнергетики" Московского авиационного института (национального исследовательского университета). На конференции отмечалось, что одна из основных задач электросетевого комплекса состоит в повышении его надежности, наблюдаемости и управляемости, а соответственно, и эффективности. Информационно-технологические системы реального времени, включая системы технологического управления, телемеханики и связи, мониторинга и диагностики (АСТУ, АИИС КУЭ, АСДУ, РЗА, интеллектуальные активно-адаптивные сети Smart Grid, цифровые подстанции и т. п.) призваны эффективно решать эти задачи. При их решении возникают проблемы импортозамещения, безопасности и эксплуатации информационных и телекоммуникационных систем, применения "необслуживаемого" энергоэффективного оборудования.

Модераторами конференции выступили **Егоров Александр Александрович**, к. т. н., профессор АВН РФ, доцент МАИ, главный редактор журнала "Автоматизация и IT в энергетике" и **Никишин Константин Александрович**, к. т. н., ученый секретарь НИК D2 РНК СИГРЭ, директор по развитию бизнеса ООО "РТСофт-СГ".

В конференции приняли активное участие более 120 специалистов. Участники конференции сосредоточились на практических вопросах и методах автоматизации в области цифровой трансформации электроэнергетики и роли информационных технологий в создании "умной" и безопасной электроэнергетики, а также проблемах импортозамещения. После выступления докладчиков завязывались между специалистами оживленные дискуссии и обсуждения по затронутым темам.

Ниже представлен обзор по представленным на конференции докладам.

Егоров Александр Александрович, к. т. н., профессор АВН РФ, Главный редактор журнала "Автоматизация и IT в энергетике", доцент МАИ представил доклад на тему: **"Импортозамещение в электроэнергетике как новая реальность Российской Федерации"**.

В докладе была рассмотрена аргументация противников и защитников импортозамещения. Противники импортозамещения, назовем их пессимистами, отмечают следующее: запрет ограничит конкуренцию и, в перспективе, произойдет снижение качества программного обеспечения; бытует мнение, что импортозамещение у нас не настоящее, просто перешивают шильдики на западных продуктах и др.

Защитники импортозамещения, назовем их оптимистами, отмечают, что импортозамещение поднимет экономику нашей страны. Также отмечаются успешные примеры отечественных продуктов (Логос, 1С, SimInTech и др.), нельзя тратить бюджетные деньги на иностранное ПО. А, пожалуй, главное с западным ПО есть очень серьезные проблемы из-за санкций и поэтому крайне необходима технологическая независимость для эффективного развития нашей страны.

В докладе перечислялись зарубежные ИТ-компании, которые приостановили свой бизнес в России на 14.03.2022 года. К ним относятся AMD, Intel, NVIDIA, TSMC, Hewlett-Packard, Dell, Apple, Google, Xerox, Cisco, IBM, Microsoft, Oracle, Adobe, SAP и многие другие.

В связи со сложившейся обстановкой из-за санкций Президент России Владимир Путин подписал указ от 2 марта 2022 года № 83 о мерах поддержки ИТ-отрасли. В этом указе, в частности, правительство на три года освобождает ИТ-компании от уплаты налога на прибыль и от проверок контрольными органами. Компании смогут взять кредиты до 3 % годовых "на продолжение работы" и на новые проекты. Плюс – сотрудники ИТ-компаний смогут взять льготную ипотеку и получат отсрочку от армии до достижения 27 лет. Такое решение принимается, чтобы снизить отток кадров из страны. Кроме того, планируется расширение программы грантов на разработку отечественных решений.

Далее в своем докладе Егоров А.А. отметил большие успехи в области импортозамещения, проводимые в Росатоме. Отечественные разработчики систем CAD/CAE объединяются с Росатомом для обеспечения цифрового суверенитета и импортонезависимости промышленности нашей страны.

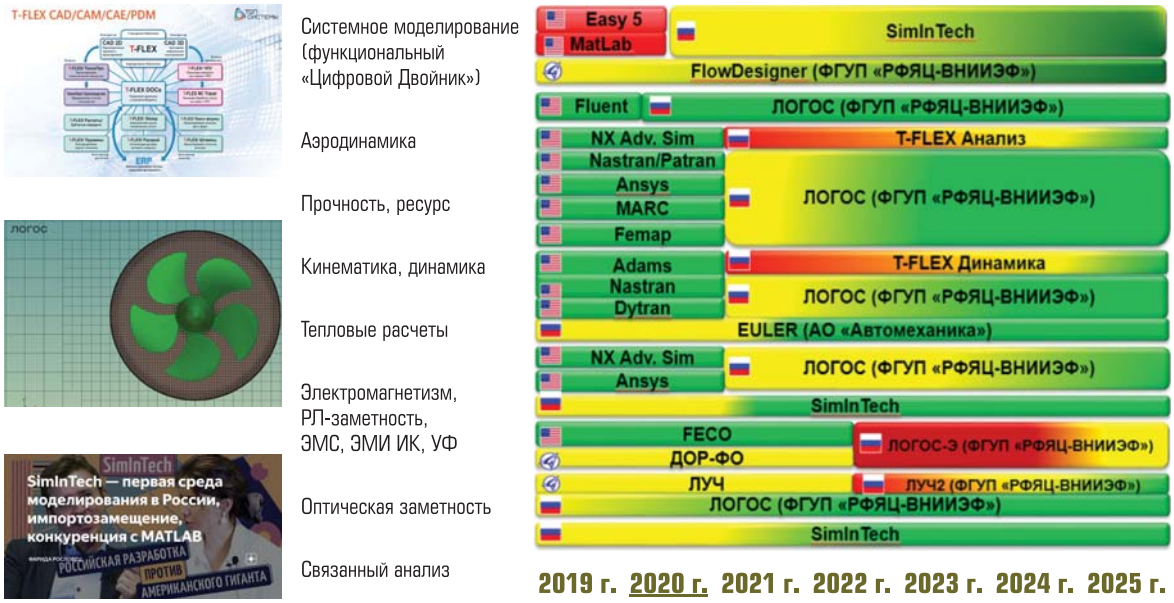


Рис. 2. Импортозамещение систем инженерного анализа CAE

В рамках Международной промышленной выставки “ИННОПРОМ2021” 6 июля 2021 года состоялось подписание Соглашения о создании Консорциума российских разработчиков систем CAD/CAE. Соглашение о создании CAD/CAE-консорциума подписали:

- генеральный директор ООО “Русатом – Цифровые решения” **Вера Гурова**;
- начальник отдела ФГУП “РФЯЦ-ВНИИЭФ” **Сергей Аксенов**;
- управляющий директор АО “Инженерно-технический центр “ДЖЭТ” **Алексей Ковалевич**;
- генеральный директор ЗАО “Топ Системы” **Сергей Кураксин**;
- генеральный директор ООО “3В Сервис” **Вячеслав Петухов** (разработчик SimInTech);
- заместитель генерального директора по продажам ООО “Фидесис” **Максим Соннов**.

Согласно подписанному документу, деятельность Консорциума будет направлена на обеспечение технологической независимости промышленных предприятий и научно-исследовательских организаций РФ в области систем суперкомпьютерного (математического) моделирования и инженерного анализа. Соглашение призвано объединить игроков рынка CAD/CAE для решения государственной задачи по обеспечению цифровой независимости российской экономики в области инженерного ПО (прежде всего, предприятий стратегических отраслей промышленности).

Положение с вопросом импортозамещения систем инженерного анализа CAE (Computer-Aided Engineering) отражено на рис. 2.

Далее докладчик остановился на отечественной программной среде **SimInTech** (Simulation In Technic). Это российская среда динамического моделирования технических систем, предназначенная для расчётной проверки работы систем управления сложными техническими объектами. SimInTech (рис. 3) позволяет эффективно осуществлять моделирование технологических процессов, протекающих в различных объектах, с одновременным моделированием системы управления, и позволяет повысить качество и надежность проектирования систем управления за счет проверки принимаемых решений на любой стадии проекта.

Первоначально SimInTech был предназначен для детального исследования и анализа нестационарных процессов в ядерных и тепловых энергоустановках, в системах автоматического управления, в следящих приводах и роботах, и в любых технических системах, описание динамики которых может быть представлено в виде системы дифференциально-алгебраических уравнений и/или реализовано методами структурного моделирования.

Основными направлениями использования SimInTech являются: создание моделей; проектирование алгоритмов управления, их отладка на модели объекта; автоматическая генерация исходного кода на языке Си для применяемых программируемых контроллеров (рис. 4).

ОТ МОДЕЛИРОВАНИЯ К СКВОЗНОМУ ПРОЦЕССУ СОЗДАНИЯ САУ

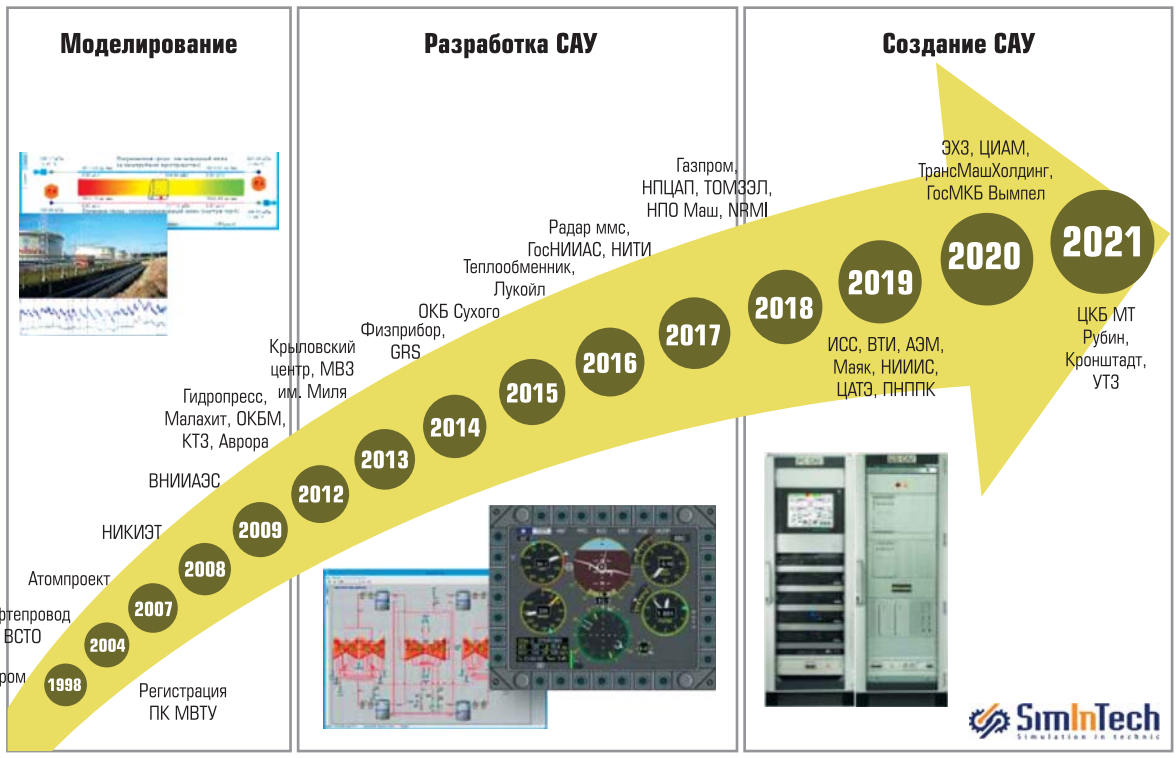


Рис. 3. Импортозамещение систем инженерного анализа CAE

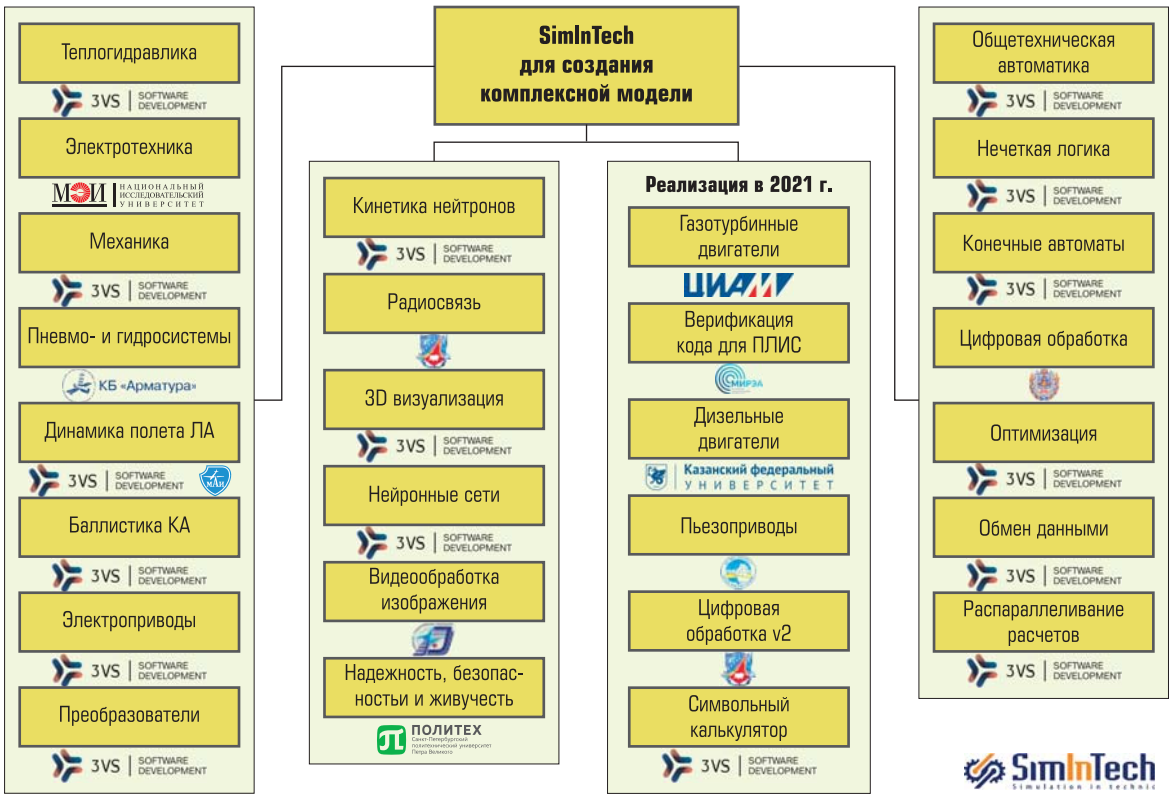


Рис. 4. SimInTech для моделирования сложных технических объектов

Логические и электрические схемы аппаратуры, средства разработки, BIOS, операционная система (ОС, ОПО) созданы/портированы в России, имеются в исходных кодах.

От 1-го поколения производительность выросла в 300 раз

Источник: Презентация новых российских процессоров Эльбрус: производительность выросла в 300 раз (trashbox.ru)

Рис. 5. Универсальные микропроцессоры "Эльбрус"

Среди предприятий оборонно-промышленного комплекса РФ, активно использующих SimInTech, следует перечислить: АО "КРОНШТАДТ", АО "Уральский турбинный завод", ЦИАМ, АО "ТрансМашХолдинг", Государственное машиностроительное конструкторское бюро "Вымпел" им. И.И. Торопова, Акционерное общество "Военно-промышленная корпорация "Научно-производственное объединение машиностроения", ФГУП "ГОСНИИАС", АО "Компания "Сухой", ПАО "ЛУКОЙЛ", АО "АТОМПРОЕКТ" и др.

15 декабря 2021 года на ежегодной конференции компании Байкал Электроникс был представлен процессор серверного класса **Baikal-S**. Пока широкая общественность бурно обсуждала отчёт о тестировании Сбербанком серверов на базе Эльбрус-8С, смакуя различные детали этой горячей истории, люди, чуть более погруженные в индустрию, с нетерпением ждали анонса Baikal-S. На рис. 5 представлены разработки универсальных микропроцессоров "Эльбрус".

Причем следует отметить, что логические и электрические схемы аппаратуры, средства разработки, BIOS, операционная система созданы/портированы в России, и что главное, имеются в исходных кодах.

Отказ крупнейшего в мире производителя полупроводников TSMC от сотрудничества с Россией означает, что российским компаниям будет сложно осуществить запланированную программу импортозамещения в области IT.

Производство чипов российской разработки осуществлялось как раз в этой тайваньской компании. Процессоры "Байкал" и "Эльбрус" были призваны стать альтернативой Intel и AMD, однако теперь их будущее туманно.

Безусловный интерес представляет Astra Linux – операционная система специального назначения на базе Linux-ядра, созданная для нужд органов государственного и военного управления и других учреждений, которые работают с информацией ограниченного доступа. Astra Linux обеспечивает защищенную обработку информации любого уровня конфиденциальности, будь то персональные данные, коммерческая, служебная или государственная тайна, вплоть до данных с грифом "совершенно секретно".

За последние три года штат "Астры" уже увеличился почти втрое, достигнув примерно 500 человек. В марте 2022 г. на фоне западных санкций, введенных после начала российской военной спецоперации на Украине, спрос на отечественные программные решения сильно возрос, поэтому в компании началось новое масштабное расширение коллектива. "*Сейчас у нас открыты вакансии по всем направлениям*, – сообщил CNews гендиректор "Астры" **Илья Сивцев**. – *Количество задач, которые мы должны решить в ближайшей перспективе, увеличилось в три раза. Для их реализации число наших разработчиков должно как минимум утроиться, а это значит, до конца года нам необходимо усилить команду до 1500 человек*".

Рис. 6. Цифровой суверенитет промышленности: Инженерная платформа Росатома

Далее докладчик отметил, что в рамках реализации цифровой стратегии в 2017 году "Роснефть" создала первый в Евразии промышленный симулятор гидравлического разрыва пласта (ГРП) "РН-ГРИД".

Импортозамещающая разработка обеспечивает технологическую независимость компании в области компьютерного моделирования, обязательного для применения технологии ГРП. Таким образом, "Роснефть" в кратчайшие сроки среагировала и сработала на опережение санкционных барьеров, ограничивающих продажи российским компаниям программного обеспечения (ПО) для моделирования гидроразрыва пласта (ГРП).

Программный комплекс "РН-ГРИД" обеспечивает выполнение всех операций и инженерных расчетов, необходимых для проектирования ГРП: загрузка и визуализация исходных данных большого объема, создание геомеханической модели пласта, анализ диагностических закачек, расчет дизайна и анализ фактически проведенных операций ГРП с использованием обширной базы данных технологических жидкостей и пропантов для ГРП.

Математическая модель симулятора "РН-ГРИД" базируется на самой современной концепции Planar 3D, которая позволяет наиболее точно описывать сложную геометрию трещины, возникающей в породе при проведении ГРП. Это выгодно отличает ее от западных коммерческих аналогов, большинство которых использует упрощенные подходы. Более подробно можно прочитать в статье Егоров А.А. "Отечественный флагманский продукт "РОСНЕФТЬ" – "РН–ГРИД" симулятор моделирования гидроразрыва пласта (ГРП)", журнал "Автоматизация и IT в нефтегазовой области" № 2, 2021 год, стр. 12-27.

В качестве другого примера докладчик привел программу "Цифровой суверенитет промышленности: Инженерная платформа Росатома" (рис. 6).

Импортозамещение в сфере высоких технологий в РФ потребует десятилетий. Такое мнение высказал вице-президент фонда "Сколково" **Алексей Беляков**.

"*Это точно долгосрочные стратегические программы. Это не год, не два – это десятилетия, поскольку цепочки поставок и взаимодействия большого количества партнеров, которые были разрушены, необходимо создавать заново*", – указал эксперт.

Цветков Максим Юрьевич, старший инженер-разработчик PLCnext, ООО "Феникс Контакт РУС" представил доклад на тему **"smartRTU – интеллектуальное устройство для мониторинга энергоустановок"**.

Максим Юрьевич остановился на области применения smartRTU 4:

- ПС низкого и среднего напряжения. Мониторинг и обработка состояния сети на вторичных подстанциях (например, измерения электрических параметров, положение КА и т.д.). ПС низкого и среднего напряжения.
- Первичное энергооборудование. Расширение контроля за счет функций управления коммутационными аппаратами или автоматическими выключателями, мониторинг параметров трансформаторов. ПС низкого, среднего и высокого напряжения.
- Подключение генерации. Мониторинг и обработка данных в точках подключения к сети, например, ветрогенераторов или СЭС. Дополнительно контроль реактивной мощности и управление инверторами в за-

Рис. 7. Внешний вид контроллера

висимости от требований сетевых операторов. ВЭУ, СЭС, локальные генерирующие установки.

К преимуществам системы докладчик отнес: ее гибкость и компактность, модульность, масштабируемость и расширяемость, интуитивно понятную и быструю настройку, конфигурирование вместо программирования через WEB интерфейс, эффективность и простой сервис, расширенную диагностику, информационную безопасность, надежность для применения в энергетическом секторе, индивидуальные решения под ключ и стандартные модули Axioline и SmartElemen.

Аппаратное обеспечение smartRTU AXC SG (Ord.N. 1110435):

- В основе контроллер AXC F 2152 (рис. 7).
- Специальное ПО.
- Реализация специфической коммуникации, функциональности и I/O-модулей для Axioline.
- ARM Cortex-A9 CPU 2×800 MHz.
- 512 Mb RAM (DDR3) / 512 Mb Flash.
- Слот для SD Flash card (2, 8, 32 Гб).
- ОС Linux.
- WEB сервер.
- 2 x RJ45, 10/100 Mb, коммутатор.
- Поддержка SmartElement и AXIOLINE I/Os.
- Слот расширения с левой стороны (+ Eth).
- Информационная безопасность: TPM, Firewall, OpenVPN, IPsec.
- Рабочий диапазон t: –25 °C ... +60 °C.

Модули ввода/вывода представлены на рис. 8.

Коммуникационная структура smartRTU представлена на рис. 9. Она позволяет подключать несколько Диспетчерских через RTU по сети Ethernet, а также Диспетчерскую через COM порт по интерфейсу IEC 60870-5-101. По сети Ethernet подключается ПК с WEB.

С другой стороны, к контроллеру smartRTU объекты и устройства по интерфейсу IEC 60870-5-104 или Modbus TCP (режим Server). В режиме Slave подключаются устройства, включая МП РЗА по интерфейсу IEC 60870-5-103 или Modbus TCP.

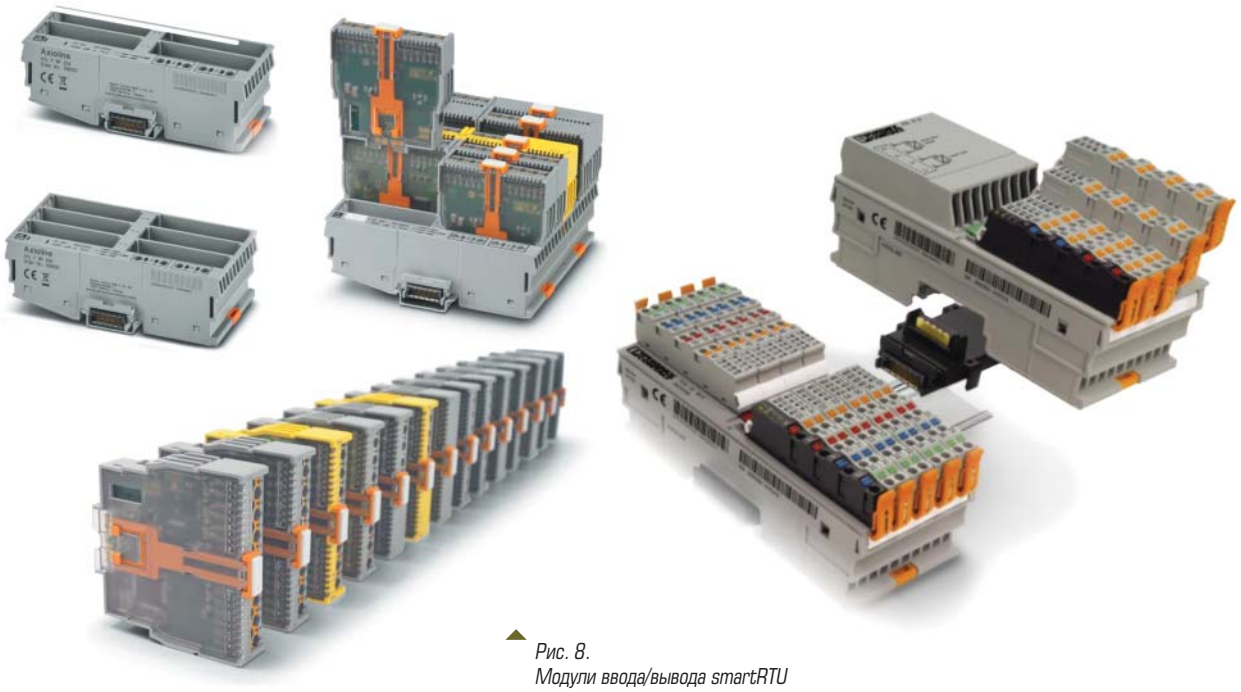


Рис. 8. Модули ввода/вывода smartRTU

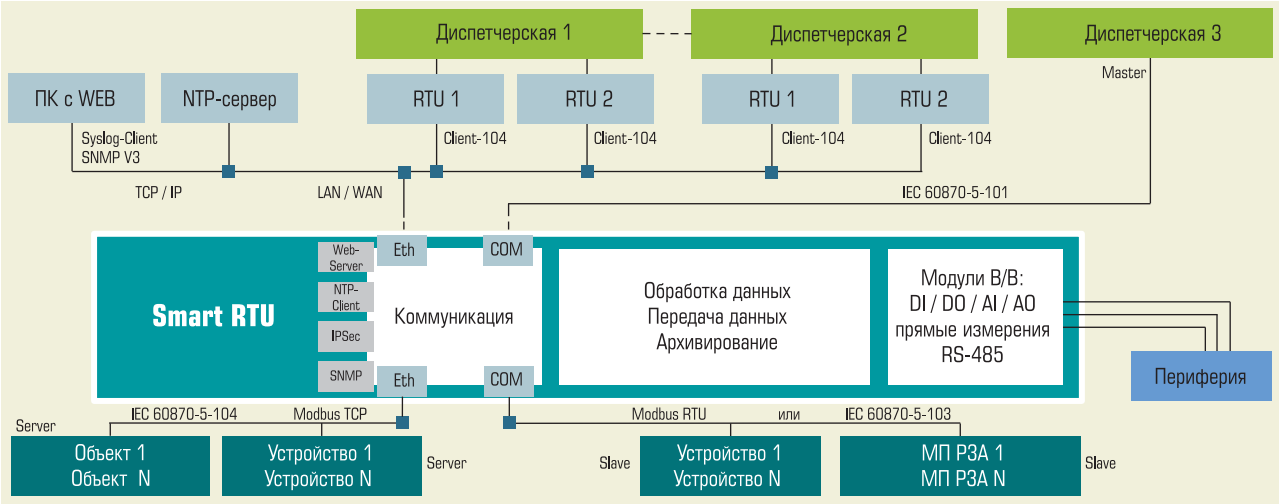


Рис. 9. Коммуникационная структура smartRTU

В таблице 1 перечислены протоколы, поддерживаемые smartRTU.

Основные функции, поддерживаемые контроллером приведены в таблице 2.

В заключение докладчик отметил, что областью применения контроллеров smartRTU является телемеханика энергообъектов (подстанции, трансформаторы и т. п.):

- Распределённые конечные потребители – понижающие трансформаторы 0,4 кВ.
- Городские электрораспределительные сети и ПС 6/10 кВ.
- Региональные электрические сети 35/110 кВ.
- Межрегиональные электрические сети 220 кВ и выше.
- Крупные промышленные предприятия – ПС 6/10 кВ.
- Производители высоковольтного оборудования.
- Альтернативная энергетика: ветро- и солнечная генерация.

Литвинов Павел Васильевич, начальник аналитического отдела АО РТСофт представил доклад на тему **“Проектирование и имитационное моделирование IT инфраструктуры, обладающей иммунитетом к киберугрозам и свойством самовосстановления”**.

Крупномасштабные взломы компьютерных сетей, произошедшие в 2020 году: эксплойты в решениях от Microsoft, SolarWinds и VMware, продемонстрировали уязвимость существующих методов защиты. Известны даже случаи, когда атака проходила с использованием антивирусного программного обеспечения. Когда была скомпрометирована инфраструк-

Таблица 1. Протоколы, поддерживаемые smartRTU

Функция	Описание
IEC 60870-5-101 Slave	Одно соединение со SCADA (RS-232)
IEC 60870-5-103 Master	Для подключения МП РЗА
IEC 60870-5-104 Server	Два независимых соединения со SCADA
IEC 60870-5-104 Client	Два независимых соединения
Modbus TCP Client	До 6 независимых соединения до 8 устройств каждое
Modbus RTU Master	Подключение до 16 устройств (RS-485)
NTP-Client	Два независимых соединения, до 4 NTP-серверов на каждое ПО
SNMPV3	Предоставление системной информации
syslog-Client	Передача на два сервера system/security уведомлений
МЭК 61850	GOOSE, MMS

Таблица 2. Основные функции, поддерживаемые контроллером smartRTU

Функция	Описание
Логические функции	Пользовательские логические операции (AND, OR, ...) и функции (RS-FF, impulse generator, ...)
Математические операции	MUL, DIV.ADD, ...
Функции для налоговых значений	• Определение min/max значений и пр., например, средних значений. • Масштабирование и нормализация. • Встроенные генераторы значений (по 16 точкам, пилообразная форма)
Сигнализация	Настраиваемая сигнализация
Выход за допустимые параметры	Мониторинг и сигнализация по измерениям
Архивация	Данные процесса, метки качества и времени
Конфигурирование	Через WEB интерфейс

тура McAfee ePolicy Orchestrator (ePO) для распространения вредоносного программного обеспечения. Концепция киберустойчивости базируется на 14-ти методах, три из которых: Ограничение привилегий; Резервирование; Сегментация получили наибольшее распространение в энергетике в силу их относительной простоты, эффективности и наличия специализированных аппаратных и программных решений. Вертикальная и Горизонтальная сегментация с использованием межсетевых экранов – это классическое решение чрезвычайно эффективное в прошлом.

Далее докладчик остановился на проникновении CPS и трендов IIoT в электроэнергетику. Все составляющие концепции Индустрии 4.0 нашли свое отражение в электроэнергетике: – "Интернет вещей", будет активно использоваться новыми потребителями – просьюмерами. "Умное предприятие" – это управление производственной деятельностью и активами. "Интернет услуг" – новые сервисы и способы продажи. "Киберфизические системы" станут доминирующей архитектурной основой отраслевых систем управления и контроля. Реальность такова, что выделенные DMZ и защищенные сегменты в любой момент могут получить доступ к сети интернет. Причин может быть множество. Например: ошибка в конфигурации межсетевого экрана или его взлом; подключение USB модема или роутера по незнанию, в нарушение инструкции или как результат обмана или воздействия методов социального инжиниринга на сотрудника; современные интеллектуальные устройства и даже сенсоры часто снабжаются модулями Wi-Fi и потенциально могут подключиться к бесплатному хот-споту.

Необходимо учитывать вероятность и просчитывать последствия того, что любой узел сети может получить нелегитимный доступ к незащищенному интернету или другому узлу. И стать точкой, с которой начинается атака или заражение.

Далее докладчик привел описание узлов агентов модели:

- Regular_node – программные и аппаратные элементы инфраструктуры, не обладающие специальными свойствами в аспекте информационной безопасности.
- Secure_node – узлы чрезвычайно устойчивые ко всем видам взлома. В качестве объективного критерия устойчивости можно использовать правило: "стоимость взлома должна многократно превышать сумму потенциальной выгоды хакера или возможного ущерба". Реализация возможна с использованием ОС, основанных на микроядре. Или использование принципов теории конечных автоматов.
- Cure_node – узлы, обладающие способностью быстрого восстановления нормального состояния. Это может быть перезагрузка или восстановление из хранилища резервных копий. Помимо возможности "самолечения" может поддерживаться функциональность активного лечения обычных узлов в случае заражения.
- Stop_node – узлы предназначенные для остановки распространения угроз. Например, может использоваться прекращение выполнения одной или нескольких функций, вплоть до отключения. Простейшим аналогом таких узлов, получивших широкое применение, можно считать дата диоды.
- Sensor_node – детекторы угроз. Решают задачи диагностики состояния инфраструктуры. Команды сенсора являются триггерами для перевода в другое состояние узлов cure_node и stop_node. Важно обеспечить "stealth mode" для таких узлов. Прототипы уже существуют. Это и реализация Deep Packet Inspection и устройства, не имеющие IP адреса в сети. Особенностью этого вида узлов является вариативность масштаба. От простейшей утилиты детектирования DoS атаки до полноценного Security Operations Center.

Результаты моделирования, проведенные в АО "РТСофт", позволили сделать следующие выводы:

- Концепция иммунной инфраструктуры и 'secure by design' адекватна современным вызовам в области информационной безопасности и завоевывает все большую популярность в разных странах, в том числе и в России.
- Использование различных методов имитационного моделирования хороший способ получить необходимые оценки и понизить размерность задачи.
- Заказчик не готов оперировать многомерными пространствами – его интересуют ответы на вопросы: какова защищенность моей инфраструктуры от APT атак по шкале от одного до ста? Сколько времени уйдет на восстановление? Риски растут или снижаются и как быстро?

Есть еще несколько причин, по которым моделирование – это хороший выбор:

- мы не можем полагаться на статистические методы. К счастью, количество успешных атак на энергокомпании невелико;
- натурные эксперименты и приемы penetration testing также нельзя использовать вне рамок испытаний и сертификации;
- результаты анализа защищенности и рекомендации для реальных объектов всегда или секретны или находятся под строгим “Соглашением о неразглашении” и не могут быть опубликованы в научной статье.

В заключение докладчик отметил, что основная сложность практического применения результатов моделирования в калибровке. Как показывает практика, почти всегда можно доверять выявленным зависимостям и форме кривой. К численным значениям до калибровки следует относиться с осторожностью.

Серьезным препятствием при оценке защищенности объекта является появление матриц большой размерности. Чтобы обеспечить полноту рассмотрения, в качестве первого шага мы должны анализировать пересечение каждого вида угроз с известными уязвимостями для всех элементов IT инфраструктуры. Для примера по состоянию на 10 января 2022 г. “Банк данных угроз и уязвимостей” (*https://bdu.fstec.ru/threat*) содержит 222 вида угроз и 36 838 известных уязвимостей.

В планах продолжить работу, объединить методы агентного моделирования с перебором всех вариантов, порождаемых пересечением информацией об известных уязвимостях и способов атак, изложенных в матрице MITRE ATT&CK®. Математический аппарат для понижения размерности разреженных матриц хорошо проработан. Он продолжает совершенствоваться в наши дни благодаря популярности рекомендательных систем, где существует та же проблема. Предполагается, что полученные результаты можно будет использовать для калибровки имитационных моделей.

Крюков Олег Викторович (полная версия доклада представлена на стр. 4.), д. т. н., заместитель директора по науке ООО “ТСН-электро” представил доклад на тему **“Инновационные возможности мониторинга распределительных устройств КТП “КАСКАД”**. Докладчик отметил, что технология Smart Grid трактуется сегодня как концепция инновационного преобразования электроэнергетики, включая малую энергетику, которая оптимизирует энергозатраты, позволяя рационально распределять электроэнергию.

Рис. 10. Структура концепции Интеллектуальной электроэнергетики

Структура концепции Интеллектуальной электроэнергетики представлена на рис. 10.

Далее докладчик остановился на вопросах, решаемых цифровой ПС:

- Унификация информационных протоколов обмена данными.
- Обеспечение способности к взаимодействию устройств.
- Сокращение кабельного хозяйства вследствие применения необслуживаемых волоконно-оптических соединений.
- Обеспечение наблюдаемости каналов сбора, передачи информации и управления.
- Снижение метрологических потерь во вторичных цепях.
- Упрощение способов тиражирования первичной информации.
- Применение устройств с обновляемым программным обеспечением.
- Унификация механизма конфигурации подстанции.
- Формирование единой системы диагностики. Переход к выполнению удаленной диагностики.
- Переход к необслуживаемым подстанциям.
- Критерии цифровой подстанции.
- Наблюдаемость параметров и режима работы силового оборудования и вторичных систем.
- Управляемость всеми технологическими процессами в режиме реального времени посредством цифровых систем связи и оборудования, обеспечивающего поддержку протоколов, утвержденных стандартами МЭК.

Рис. 11. Низковольтные комплектные устройства распределения и управления НКУ "КАСКАД"

- Самодиагностика всех силовых аппаратов и вторичных систем.
- Цифровой обмен данными между всеми технологическими системами.
- Интеллектуальное адаптивное управление режимом работы силового оборудования и вторичных систем с учетом режимов работы прилегающей электрической сети и внутренних технологических процессов.
- Упрощение вторичных соединений (применение волоконно-оптических кабелей) снижение затрат на обслуживание, упрощение вопроса электромагнитной совместимости.

Далее докладчик рассмотрел основные преимущества и недостатки цифровых подстанций.

К экономическим преимуществам было отнесено следующие:

- Диагностика оборудования и ремонт по фактическому состоянию, снижение затрат. Автоматическое управление подстанцией без участия оперативного персонала с АРМ диспетчера – снижение затрат на обслуживание до 35 %.
- Сокращение длительности перерывов в электроснабжении потребителей в аварийных режимах работы – уменьшение недоотпуска электрической энергии.
- Увеличение точности измерений (особенно при токах менее 10-15 % Iн) и увеличение благодаря этому точности учета электроэнергии и точности определения мест повреждения.
- Уменьшение потребления по цепям переменного тока и напряжения (в результате применения оптических ТТ и ТН).
- Самодиагностика и дистанционная.

К технологическим преимуществам было отнесено:

- Типизация и автоматизация проектных решений – снижение времени на проектирование.
- Поставка оборудования в полной заводской готовности – снижение времени на СМР и ПНР.
- Отсутствие электрической связи между первичным и вторичным оборудованием – повышение безопасности.
- Сокращение возможности появления дефектов типа "земля в сети постоянного тока" (сокращение размерности СОПТ ввиду использования цифровых оптических связей).
- Исключение ошибочных действий персонала, производящих оперативные переключения на ПС – уменьшение травматизма.
- Видеоконтроль операций на подстанции – обеспечение безопасности.
- Обеспечение контроля всех действий на подстанции в журнале событий.

В качестве недостатков в докладе отмечались следующие:

- Отсутствие единой НТД на проектирование.
- Вопросы информационной безопасности.
- Производители применяют собственные профили сигналы диагностики по 618508.1, которые требуют адаптации.

Далее докладчик остановился на низковольтных комплектных устройствах распределения и управления НКУ "КАСКАД" (рис. 11).

В докладе были рассмотрены классы средств регулирования в рамках технологии Smart Grid в электрических сетях 0,4-20 кВ. Технологии D-FACTS используют энерго-

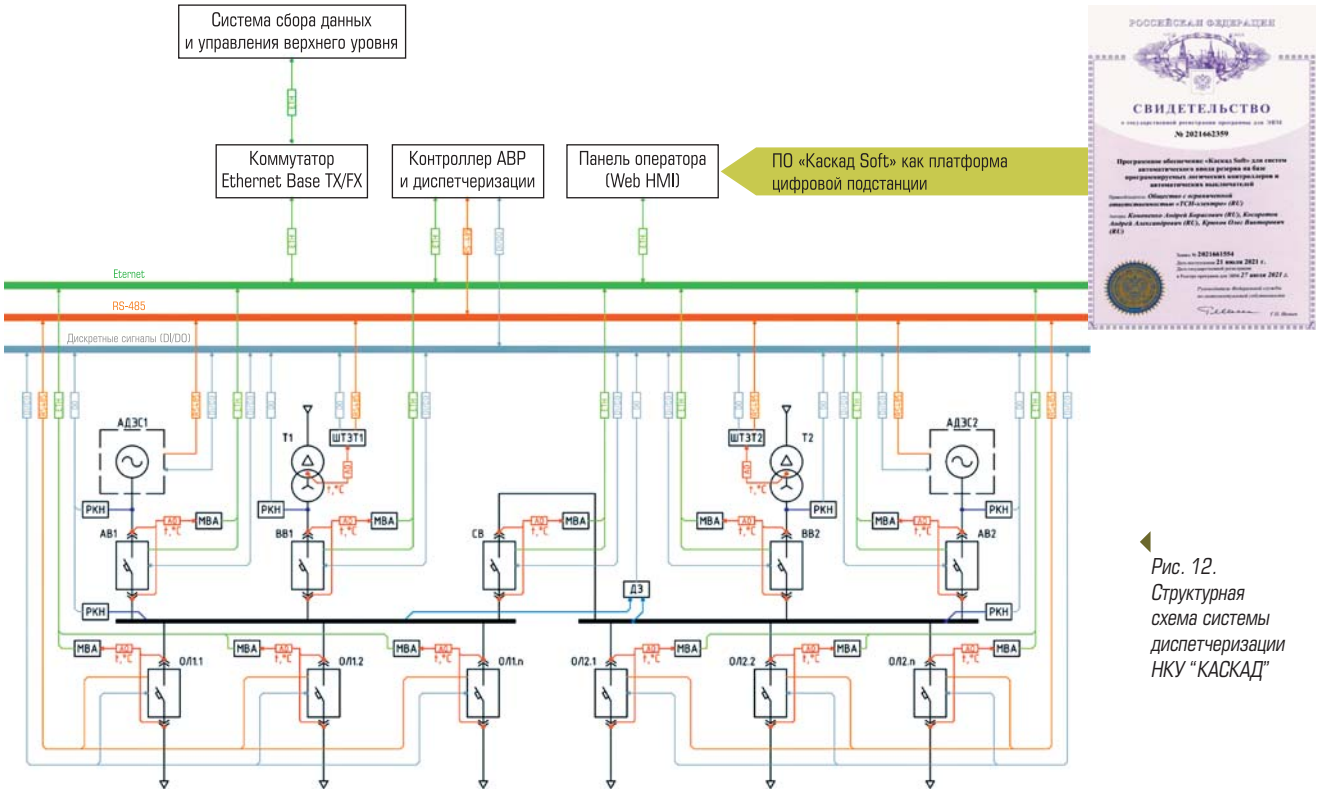


Рис. 12. Структурная схема системы диспетчеризации НКУ "КАСКАД"

эффективные трансформаторы, устройства регулирования потока мощности, автоматизированные трансформаторные подстанции с цифровым программным управлением, твердотельные регуляторы напряжения, устройства продольно-поперечной компенсации.

Технологии Micro Grid используют накопители электрической энергии, генерирующие установки на основе возобновляемых источников энергии, устройства сопряжения разнородных источников энергии, виртуальные электростанции, системы SCADE,EMS,DMS, WEB-технологии, биллинговая система.

На рис. 12 представлена структурная схема системы диспетчеризации НКУ "КАСКАД".

ПО "КАСКАД Soft" рассматривается как платформа цифровой подстанции. Применение единой среды для разработки системы автоматизации позволяет легко переносить программные модули между платформами программируемых контроллеров разных производителей – это ускоряет миграцию решений между ними, что позволяет разработать и внедрить систему, отвечающую всем требованиям клиента. Широкие коммуникационные возможности позволяют интегрировать АСУ в системы верхнего уровня по различным протоколам связи. Каскад Soft – универсальное, мультибрендовое, гибкое к будущим изменениям ПО.

Во-первых, при разработке можно реализовать требуемые алгоритмы системы АВР под различные схемы электроснабжения. Во-вторых, в любое время можно осуществить перенастройку или расширение системы автоматизации, дополнив необходимыми функциями.

Техническое состояние электрооборудования наглядно отображается на мнемосхеме (рис. 13).

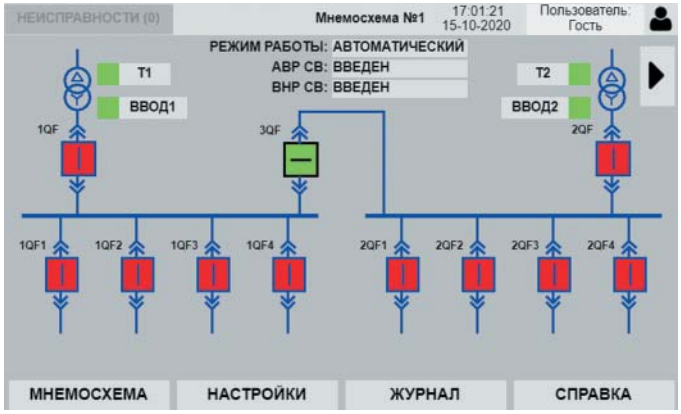


Рис. 13. Мнемосхема отображения технического состояния оборудования

Рис. 14. Переназначение входов и выходов контроллера

При этом можно отслеживать состояние и положение коммутационных аппаратов РУ, трансформаторов (температура и срабатывание защиты), наличие нормального напряжения на вводах и секциях. Визуализация доступна как с панели оператора и на самом РУ, так и удаленно на ПК с любым веб-браузером. Это позволяет оптимизировать процесс эксплуатации высококвалифицированным инженерным составом.

Система обеспечивает корректировку алгоритмов работы под конкретные нужды эксплуатационного персонала с минимальными временными затратами.

Проработаны и проверены на практике алгоритмы, которые учитывают самые различные ситуации и схемы как АВР так и автоматического возврата нормального режима.

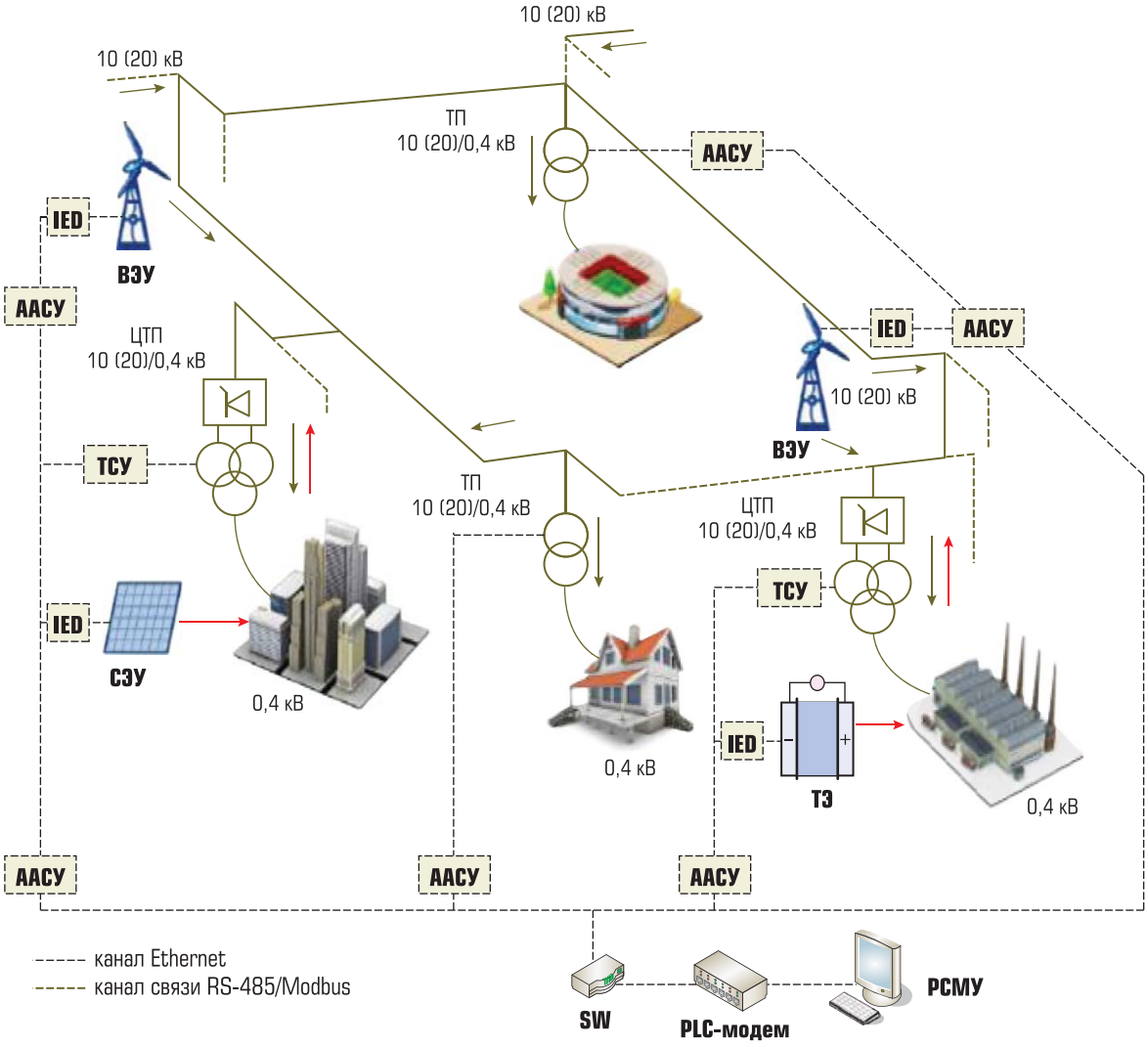
Гибкие настройки позволяют адаптировать ПО контроллера АВР посредством установки режимов подключения, отключения и переключения основных и резервных вводов, режимов пуска и останова АДЭС, приоритетов вводов, а также определения реакции блока АВР на выявление неисправностей.

Система диагностики КТП “Каскад” может комплектоваться датчиками температуры, которые устанавливаются в контактных соединениях коммутационных аппаратов, с целью диагностики их состояния. Датчики подключаются к контроллеру системы диагностики посредством аналоговых модулей ввода-вывода. Контроллер оценивает абсолютное значение и динамику изменения температуры, и в случае превышения критических параметров, рассчитывает время до отключения. По истечении данного времени происходит отключение автоматического выключателя, для его защиты от теплового повреждения, а также недопущения пожара в шкафу РУ.

Контроллер системы диагностики отслеживает и записывает во внутреннюю энергонезависимую память все события связанные с изменением состояния электрооборудования, настроек системы, сменой пользователя. Каждому событию присваивается метка времени с точностью, привязанной ко времени скана контроллера. В отличие от журналов, основанных на базе стандартных HMI подобная реализация позволяет с высокой точностью отследить последовательность событий, которые привели к аварийной ситуации. Кроме журнала ведется и список текущих неисправностей, которые отображаются в табличном виде, с моментом возникновения и квитирования.

В некоторых случаях может произойти ситуация при которой, контроллер АВР не выявил явных неисправностей оборудования, однако алгоритм отрабатывает некорректно или не полностью (как бы “зависает” на полпути). Это связано с тем, что на контроллер не приходит сигнал, который в нормальных условиях был.

С целью упростить поиск подобных неисправностей для оперативного персонала, реализована функция “умной” самодиагностики АВР – система подсказывает, каких условий недостаточно для перехода алгоритма на следующий шаг (рис. 14).



ААСУ – активно-адаптивная система управления
IED – интеллектуальное электронное устройство
SW – сетевой информационный коммутатор
ТСУ – технологическая система управления
РСМУ – распределенная система мониторинга и управления
ТЭ – установки на основе топливных элементов
ВЭУ – ветровые энергетические установки
СЭУ – солнечные энергетические установки

Рис. 15. Применение ЦТП в составе Интеллектуальной распределенной электрической сети 10(20)/0,4 кВ

Открыв данную таблицу персоналу прибывшему разобраться в ситуации гораздо легче понять, в чем проблема, что существенно сокращает время на ее поиск и устранение.

В заключение докладчик рассмотрел применение ЦТП в составе Интеллектуальной распределенной электрической сети 10(20)/0,4 кВ (рис. 15).

Оборудование, сконструированное на собственной системе решений “Каскад” отвечает всем современным требованиям и тенденциям, сертифицировано и апробировано в отраслях промышленности, мультибрендовое – комплектация под индивидуальные, особые требования клиента и имеет возможность для будущего расширения и ремонтопригодно.

Продолжение обзора X Международной научно-практической конференции “Автоматизация и информационные технологии в энергетике 2022” в следующем номере журнала.

***Егоров Александр Александрович** – канд. техн. наук, профессор АВН РФ, главный редактор журнала “Автоматизация и IT в энергетике”.*