ВЕСЬ ЦВЕТ
ЭЛЕКТРОНИКИ

ufi Approved Event

E·X·P·O ELECTRONICA

18-Я МЕЖДУНАРОДНАЯ ВЫСТАВКА
ЭЛЕКТРОННЫХ КОМПОНЕНТОВ
И КОМПЛЕКТУЮЩИХ

Совместно с выставкой
electrontech EXPO

24–26 марта 2015

МОСКВА
КРОКУС ЭКСПО

Получите электронный билет:
www.expoelectronica.ru

Организаторы: primexpo ITE GROUP PLC
+7 (812) 380 6003/07/00, electron@primexpo.ru

При содействии:
ЭЛИНТ СП Электроинторг СП
ITE CHINA
GiMA

0+

OpenSystems Publishing

МКА : ВКС

МИР КОМПЬЮТЕРНОЙ АВТОМАТИЗАЦИИ • ВСТРАИВАЕМЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ
COMPUTER AUTOMATION WORLD • EMBEDDED COMPUTER SYSTEMS

В НОМЕРЕ

CONTENTS

ВСТРАИВАЕМЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ

EMBEDDED COMPUTER TECHNOLOGIES

Стандарт VPX: путь к зрелости
Александр Ковалёв, Виктор Синенко, ЗАО «РТСофт»
4
VPX: on the road to maturity,
by Alexander Kovalev and Victor Sinenko, RTSoft

Инновационные технологии и решения «РТСофт» для транспортной отрасли
Фоторепортаж с выставки «ЭкспоСитиТранс-2014»
Пресс-служба ЗАО «РТСофт»
10
RTSoft's innovative technologies and solutions for transport sector at ExpoCityTrans'2014 Exhibition,
by RTSoft materials

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

SOFTWARE

Протоколы «Интернета вещей»: основные сведения
Стэн Шнайдер (Stan Schneider), технический эксперт
13
Understanding The Protocols Behind The Internet Of Things,
by Stan Schneider, Electronic Design

Тестирование встроенного программного обеспечения
Андрей Пронин, Вячеслав Ванюлин, Игорь Починок, Auriga, Inc., НИВЦ МГУ
19
Proven Practices for Testing Embedded Software,
by Andrey Pronin, Vyacheslav Vanyulin and Igor Pochinok, Auriga Inc, MSU RCC

ИУС ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ И ИНФРАСТРУКТУРНЫХ ОБЪЕКТОВ

INDUSTRIAL ENTERPRISE AND INFRASTRUCTURE IMSs

Отечественная инструментальная платформа для разработки информационно-управляющих систем PLATINUM-RT
Сергей Кирюхин, Алексей Ханыгин, Денис Алексеев, ЗАО «РТСофт»
25
PLATINUM-RT Russian Tool Platform for Information Management System Development. Part 1,
by Sergey Kiryukhin, Alexey Khanygin and Denis Alexeev, RTSoft

Автоматический подсчёт пассажиров общественного транспорта
Основные технические требования и подходы к реализации
Константин Утешев, ЗАО «РТСофт»
35
Automatic Public Transport Passengers Count: Basic Technical Requirements and Approaches to Implementation,
by Konstantin Uteshev, RTSoft

«РТСофт» на European Utility Week
Павел Литвинов, ЗАО «РТСофт»
40
RTSoft at the European Utility Week,
by Pavel Litvinov, RTSoft

ИУС ДЛЯ ЭЛЕКТРОЭНЕРГЕТИКИ

POWER INDUSTRY IMSs

Построение цифровых подстанций 35–110 кВ для распределительных сетей
Леонид Орлов, ЗАО «РТСофт»
43
Bulding 35–110 kV Digital Substations for Distribution Networks,
by Leonid Orlov, RTSoft

Распределительные сети и Микрогрид
А. А. Небера, Н. Г. Шубин. ЗАО «РТСофт»
45
Distribution Networks and Microgrid,
by Alexey A. Nebera and Nikolay G. Shubin, RTSoft

Исследование и применение методов ситуационного анализа кибербезопасности в интеллектуальных сетях
Гао Кунлун (GAO Kunlun), China Electric Power Research Institute,
Ванг (WANG Yufei), China Electric Power Research Institute,
Ксу Руши (XU Ruzhi), North China Electric Power University
51
Study and Practice of Cybersecurity Situation Evaluation Method for Smart Grid,
by Gao Kunlun and Wang Yufei, China Electric Power Research Institute, and Xu Ruzhi, North China Electric Power University

«РТСофт» на 45-й сессии СИГРЭ
А. Р. Вериго., А. А. Небера, Н. Г. Шубин , ЗАО «РТСофт»
61
RTSoft at SIGRE's 45th Session,
by Andrey R. Verigo, Alexey A. Nebera and Nikolay G. Shubin, RTSoft

НОВОСТИ РЫНКА **18, 24, 44, 64** EMBEDDED MARKET NEWS

Редакционный совет:

Синенко О.В. – председатель редакционного совета, директор НП «Вера+», д.т.н.

Егоров А.А. – начальник научно-учебного Центра МАИ «Интеллектуальные системы измерений, контроля и управления в промышленности», профессор АВН РФ, к.т.н.

Золотарёв С.В. – ведущий эксперт компании «Фиорд», к.т.н.

Итенберг И.И. – генеральный директор и главный конструктор ОАО «НКБ ВС», к.т.н.

Куцевич Н.А. – технический директор ЗАО «РТСофт», д.т.н.

Рыбаков А.Н. – технический директор ЗАО «РТСофт»

Сюзев В.В. – зав. кафедрой, профессор МГТУ им. Н.Э. Баумана, д.т.н., лауреат премии правительства в области образования

Шагурин И.И. – заместитель заведующего кафедрой, профессор МИФИ, д.т.н.

Редакция:

Татьяна Зеленова – *выпускающий редактор*

Илья Белов – *ответственный за вёрстку*

Учредитель:
ЗАО «СПА»

Адрес: 105077, Москва, а/я 158

Телефон: 8-499-271-32-32

Факс: 8-495-748-68-29

E-mail: mka@veraplus.msk.ru,

URL: www.mka.ru

Оформить подписку можно:

1. **На почте** по каталогам агентства «Роспечать» – «Газеты. Журналы. Книги. Учебные пособия» и Russian Newspapers & Magazines, индекс 72710.
2. **На почте** по Объединенному каталогу «Пресса России», индекс 45075.
3. **Через редакцию** по тел. 8-499-271-32-32.

Тираж 1000 экз., цена свободная.

Журнал для тех, кто принимает решения при создании открытых встраиваемых систем.
«Мир компьютерной автоматизации: встраиваемые компьютерные системы»
Computer Automation World: Embedded Computer Systems
№ 1 (1/28/46/105) 2015
Издаётся с 2007 (1995) года. Выходит 6 раз в год.
Зарегистрирован в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).
Свидетельство ПИ №ФС77-43074 от 15.12.2010

Александр Ковалёв, Виктор Синенко, ЗАО «РТСофт»

Стандарт VPX: путь к зрелости

Начав свой путь сравнительно недавно как преемница технологии VME для новых и перспективных проектов в оборонных приложениях, системная архитектура VPX вступила в пору зрелости. В своем современном виде VPX – это развитый стандарт, пользующийся серьёзной поддержкой на рынке и позволяющий создавать эффективные боевые решения экстра-класса, которые почти невозможно создать ни на какой другой технологической основе.

Строго говоря, под термином «VPX» следует понимать не конкретную спецификацию ассоциации VITA: «VITA 46». Это большая серия связанных стандартов, которые описывают вопросы архитектуры, системотехники, механики, альтернативных системных соединителей, методов охлаждения и обслуживания систем на уровне ТЭЗов для боевых встраиваемых систем. К рассмотрению такого сложного и масштабного явления, как VPX, можно подходить с разных сторон. В том числе с исторической. К началу 21-го столетия технология VME оказалась в эволюционном тупике, исчерпав все существенные возможности развития. Инициатива VME Renaissance ассоциации VITA имела своей основной целью повышение пропускной способности VME-совместимых систем, поскольку именно пропускная способность шины VMEbus являлась на тот момент (и остаётся по сей день) наиболее проблемным местом классической архитектуры VME. На первом этапе «ренессанса VME» был придуман протокол 2eSST (спецификация VITA 1.5), благодаря которому скорость параллельного интерфейса VME удалось поднять до 320 Мбайт/с. Затем была разработана спецификация VITA 31, описывающая реализацию в крейте VME некоего подобия высокопроизводительной системы CompactPCI PICMG 2.16 с подключением плат к быстрым внутрисистемным каналам GEthernet через стандартный разъём VME64x P0 (по два порта GEthernet на один разъём). В дальнейшем появилась возможность привлекать для организации взаимодействия между слотами не только GEthernet, но и другие передовые коммуникационные технологии, такие как InfiniBand, Serial RapidIO, 10 GEthernet и PCI Express. Соответствующий стандарт, получивший название VXS (спецификация VITA 41), определил разъём P0 новой конструкции, который позволил обеспечить поддержку до четырёх быстрых 10-гигабитных портов на одну плату, но привёл к частичной утрате механической совместимости с исходной системной архитектурой VME.

В середине «нулевых» стало окончательно ясно, что традиционная версия системной архитектуры VME со всеми её модификациями не имеет будущего в долгосрочной перспективе. На этом историческом фоне прозвучал заключительный аккорд программы VME Renaissance: ассоциация VITA (http://www.vita.com) одобрила спецификацию VPX (VITA 46), окончательно порвавшую с исходной архитектурой VME в плане механики системного разъёма, электрики и протоколов передачи данных.

Операция «Преемник»

Как уже говорилось выше, стандарт VPX должен был подвести логический итог программе VME Renaissance, акцент в которой делался на повышение внутрисистемной пропускной способности для VME-подобных систем. Однако разработчики новой магистрально-модульной архитектуры из числа компаний, входящих в консорциум VITA, желали использовать предоставившийся им шанс по максимуму. Наряду с простым увеличением скоростей обмена между платами, они собирались решить ряд других давно назревших проблем, которые не представлялось возможным решить в рамках классических магистрально-модульных стандартов вроде VME и CompactPCI.

По мысли создателей, архитектура VPX должна была поддерживать те же типоразмеры 3U и 6U (рис. 1, 2), что и её предшественницы, но базироваться на других системных разъёмах, поскольку унаследованные разъёмы VME и CompactPCI обладали рядом неустранимых недостатков. Основной из них – малая полоса пропускания для поддержки современных последовательных технологий обмена данными.

Кроме того, претендуя на статус ключевой технологии для клиентов из оборонной и аэрокосмической отраслей, VPX должна была быть готовой к применению в проектах с жизненным циклом, исчисляемым десятилетиями. Это обязывало её авторов создать задел на будущее и предусмотреть в новом стандарте поддержку высокоскоростных последовательных внутрисистемных соединений на основе как уже существующих (например, 10 GEthernet), так и перспективных высокопроизводительных коммуникационных технологий (40 GEthernet, 100 GEthernet). При этом системы на основе архитектуры VPX должны были стать комфортной средой обитания для мощных процессоров текущего и следующих поколений, что требовало предусмотреть эффективный отвод тепла от отдельных модулей. Было весьма желательно также, чтобы платформа, идущая на смену VME и CompactPCI, стала ответом на чаяния абсолютного большинства владельцев боевой компьютерной техники, давно мечтавших о возможности безопасной замены хорошо защищённых отдельных модулей в полевых условиях.

Не будет большим преувеличением сказать, что новый системный разъём является центральным структурным элементом всего здания VME и во многом определяет ключевые потребительские свойства этой системной архитектуры. Новый разъём ориентирован на использование высокопроизводительных коммуникационных технологий вроде 10 GEthernet, PCI Express, Serial RapidIO и InfiniBand. Для совместимости с унаследованными системами VME на разъёме «распинована» классическая шина VME. Поэтому поставщики оборудования иногда преподносят VPX как глубокий тюнинг VME-решений, что верно лишь отчасти.

Тем не менее сильная связь между VPX и VME очевидна. Эти системные архитектуры роднит ориентация на одни и те же приложения (преимущественно оборонные и аэрокосмические), а также поддержка со стороны одних и тех же производителей, которые, собственно, и продвигают стандарт VPX на рынок в качестве замены и «продолжателя дела VME». Подобно изделиям VME, изделия VPX могут существовать в защищённых версиях, рассчитанных на эксплуатацию в экстремальных условиях. В данном отношении VPX идёт много дальше VME, поскольку поддерживает такую степень защищённости на уровне плат, которая позволяет заменять отдельные модули «в поле» без принятия особых мер предосторожности и участия высококвалифицированного обслуживающего персонала (стандарт VPX REDI).

Кроме того, системная архитектура VPX близка к VME в том смысле, что она близка к пользователям VME. Существующим пользователям она предлагает наиболее естественный и эффективный путь в будущее на правах официально объявленной преемницы VME. Если же вести речь об освоении с нуля, то есть о новых пользователях, архитектура VPX может оказаться даже проще VME, поскольку технологически гораздо сильнее связана с миром общегражданских систем, наследуя из этого мира наиболее развитые технологии передачи данных.

Стандарт с человеческим лицом

Может показаться, что ввиду отсутствия совместимости между архитектурами VME и VPX на физическом, электрическом и программном уровнях освоение технологии VPX есть дело сложное и дорогое, однако это не так. VPX весьма дружественна к пользователю в силу одного важного обстоятельства: с точки зрения применяемых базовых технологий типичная VPX-система гораздо ближе к миру обычных настольных ПК, чем система

Рис. 1. Кондукционный модуль формата 6U VPX серверного уровня

Рис. 2. Кондукционный модуль формата 3U VPX с многоядерным процессором

VME. В типичной VPX-системе нет экзотической шины VMEbus, а все остальное по большей части заимствовано с рынка настольных компьютеров и серверов. Основная масса оборудования VPX строится на базе тех же x86-совместимых процессоров, модулей памяти и периферии и опирается на те же интерфейсные и коммуникационные технологии (PCI Express, GEthernet, USB, HDMI/DisplayPort), что и настольные системы. Даже мощные мультипроцессорные комплексы в стандарте VPX, при всей их новизне и уникальности, – это, в сущности, не что иное, как привычные вычислительные кластеры, где роль отдельных компьютеров играют VPX-модули, а межмашинное (межмодульное) взаимодействие, как и ранее, осуществляется по каналам GEthernet, выполненным не в виде кабелей, а в виде дорожек на объединительной магистрали. Как следствие, львиная доля труда по созданию типичной VPX-системы не требует каких-то сакральных знаний, которые приобретаются лишь за долгие годы работы в специальных областях над специальными проектами, и может осуществляться экспертами по вполне обычным системам настольно-офисного класса.

Стандарт VPX допускает использование различных коммуникационных технологий для организации взаимодействия между платами. Однако на практике внутрисистемный обмен чаще всего организуется при помощи привычных технологий GEthernet и PCI Express. Легко понять, почему это так: абсолютное большинство выпускающихся в настоящее время VPX-модулей строится на базе современных x86-совместимых процессоров, чьи чипсеты поддерживают технологию PCI Express по умолчанию.

При ближайшем рассмотрении дружественными оказываются даже те аспекты технологии VPX, которые не имеют никаких аналогов на рынке массовых компьютеров. Мы имеем в виду прежде всего стандарт VPX REDI, определяющий использование защищённых модулей в герметичных корпусах с кондуктивным или жидкостным охлаждением. В мире ПК нет ничего похожего на VPX REDI, однако этот стандарт разрабатывался специально для того, чтобы гарантировать предельную простоту и удобство взаимодействия с оборудованием для неискушённого пользователя.

Итак, ни отсутствие обратной совместимости с VME, ни принципиально новая функциональность не могут считаться факторами, осложняющими освоение системной архитектуры VPX. Тем не менее вплоть до недавнего времени сложности с освоением VPX возникали у многих клиентов. И обусловлены эти сложности были несовместимостью оборудования в рамках самой экосистемы VPX.

Свобода или вседозволенность?

Воздух свободы сыграл с авторами стандарта VPX злую шутку. Создатели VPX так сильно стремились вырваться за тесные рамки VME, что несколько переоценили потребности рынка в свободе самовыражения со стороны поставщиков оборудования. Желая обеспечить охват максимально широкого диапазона конечных приложений, авторы нового стандарта сделали его воистину всеобъемлющим – и, как ни странно, именно это стало серьёзным препятствием на пути VPX к широкому признанию. Несколько чрезмерная свобода манёвра, заложенная в спецификацию VITA 46, приводила к тому, что оборудование одного производителя оказывалось несовместимым с оборудованием другого производителя. В результате более-менее законченные проекты удавалось реализовывать лишь на базе изделий одного поставщика: Kontron, GE IP, Curtiss Wright или кого-то ещё.

Энтузиасты – и таких было немало – не видели в этом ничего страшного, однако подавляющее большинство «нормальных» пользователей такое положение дел не устраивало. Разработчики, привыкшие брать лучшие совместимые продукты из разных источников и быстро создавать мультивендорные конечные системы, оптимально «заточенные» под конкретные прикладные задачи, были де-факто лишены такой возможности. Несовместимость между VPX-изделиями разных производителей имела место главным образом на системном уровне, более конкретно – в таких важнейших аспектах, как назначение контактов в разъёме и организация тыльного ввода-вывода. Теоретически VPX, как и всякий приличный стандарт, должен был обеспечивать безоговорочную совместимость удовлетворяющих ему продуктов от разных поставщиков, на практике же такой совместимости не наблюдалось, ибо спецификация VITA 46 слишком многое оставляла на усмотрение производителей. Получалось, что свобода творчества поставщика оборудования шла в ущерб рыночной свободе действий клиента. С учётом ориентации технологии VPX на оборонные и аэрокосмические приложения этот момент служил серьёзным сдерживающим фактором на пути внедрения VPX.

Сложилась довольно странная ситуация, когда в целом идеология VPX устраивала всех участников рынка, но практика работы с VPX не устраивала почти никого. Отсутствие совместимости между изделиями разных производителей приводило к тому, что рынок VPX был малоконкурентным, а цены на нём – сравнительно высокими. В итоге в среде разработчиков довольно быстро утвердилась мысль,

что VPX – это сложно, неудобно и дорого. Самое грустное, что не все носители подобных представлений были людьми предвзятыми.

Дороговизна оборудования VPX была обусловлена не только слабой конкуренцией между производителями. Далеко не всегда из одного источника можно было получить все комплектующие, необходимые для построения системы с конкретными свойствами. Как правило, в продуктовом портфеле каждого отдельного производителя присутствовало *почти всё*, что нужно, а остальное он был готов разработать специально для заказчика за отдельную и немалую плату, и то, что должно было выглядеть, как закупка плат, превращалось в заказ проектного решения.

В результате страдали как клиенты, лишённые возможности свободно конфигурировать свои VPX-системы, так и поставщики, продающие оборудование стандарта VPX в меньших объёмах, чем им бы хотелось. Недовольство сложившейся ситуацией привело к тому, что компания Mercury Computer Systems и ряд других известных производителей оборудования для оборонных систем предприняли попытку напрямую договориться друг с другом о том, как обеспечить совместимость выпускаемых ими продуктов на уровне систем. Так по соседству с VITA возникла альтернативная организация OpenVPX, провозгласившая своей целью устранение проблемы несовместимости. В эту организацию вошли те производители, которых не устраивали текущие темпы роста рынка VPX и которые были готовы следовать совместно выработанным правилам, направленным на обеспечение совместимости аппаратных средств из разных источников. В результате на свет появилась спецификация OpenVPX, которая первоначально существовала вне рамок VITA, так как, по сути, была создана другим консорциумом. Впоследствии объединение производителей OpenVPX легализовалось в формате одного из комитетов VITA, а стандарт OpenVPX обрёл статус спецификации VITA 65.

Свобода через самоограничение

Стандарт OpenVPX был призван «модернизировать» технологию VPX таким образом, чтобы на её основе могла развиться конкурентная среда, которая бы способствовала снижению цен и обеспечивала совместимость оборудования из разных источников. Подобные экосистемы, возникающие вокруг открытых промышленных стандартов, позволяют пользователям оптимизировать конечные решения за счёт свободного, без оглядки на отсутствующую проблему совместимости, выбора тех изделий, которые наилучшим образом подходят для конкретных задач.

В настоящее время продукты, удовлетворяющие стандарту OpenVPX (VITA 65), предлагаются всеми ключевыми игроками сегмента VPX. Сегодня невыгодно разрабатывать и производить новые изделия только по базовому стандарту VPX, без учёта требований OpenVPX.

Границы свободы

Спецификация VITA 65 предлагает набор шаблонов (профилей), которым должны соответствовать части VPX-системы (процессорные модули, платы ввода-вывода, объединительные магистрали), чтобы корректно функционировать в её составе. Фактически, в многомерном пространстве возможностей, предоставляемых базовым стандартом VPX, выделяются и конкретизируются некоторые области с достаточно чётко очерченными границами, соответствующие наиболее распространённым типам продуктов и сценариям их применения. И идея свободы, загнанная в эти рамки, стала наконец конструктивной рыночной силой. Теперь производитель, желающий разработать модуль с некоторой функциональностью, находит в стандарте OpenVPX нужный профиль, создаёт продукт с удовлетворяющей этому профилю разводкой выводов и отражает данный факт в описании изделия в виде буквенно-цифрового кода. На основании этого кода пользователь может определить, с какими продуктами других производителей должно быть совместимо данное конкретное изделие, и принять взвешенное решение относительно его покупки.

Руками трогать!

Ещё одно преимущество технологии VPX, позволяющее расходовать бюджет более эффективно, – это стандарт VPX REDI (VITA 48), определяющий модули в герметичных защитных кожухах (рис. 3). Авторы спецификации VITA 48 стандартизовали различные виды охлаждения: воздушное, кондуктивное, потоком жидкости,

Рис. 3. Универсальная система VPX 3U с защищёнными коннекторами

разбрызгиванием. В заказных кастомизированных системах всё это использовалось и раньше, но стоило немалых денег. Спецификация VPX REDI впервые позволила реализовывать продвинутые схемы охлаждения на основе стандартных серийных аппаратных средств от разных производителей за гораздо меньшие деньги.

Не секрет, что для боевой компьютерной техники, сроки эксплуатации которой исчисляются десятилетиями, общая стоимость владения может многократно превысить начальные затраты на разработку, закупку оборудования, интеграцию и написание программного обеспечения (ПО). Стандарт VPX REDI отражает концепцию двухуровневой поддержки (2-level maintenance), призванной уменьшать стоимость владения за счёт исключения из процесса обслуживания одного этапа. Традиционно пользователи оборонных компьютерных решений заменяли вышедший из строя крейт целиком со всем содержимым. Неисправная система демонтировалась, после чего либо отправлялась к производителю, либо просто выбрасывалась, а на её место устанавливалась исправная. При использовании оборудования, удовлетворяющего стандарту VPX REDI, конечные пользователи могут иметь дело с содержимым крейта и заменять отдельные неисправные модули в его составе, что гораздо удобнее, быстрее и дешевле. Кроме того, благодаря герметичному исполнению модулей VPX REDI с ними можно работать без специальной электростатической защиты в условиях, далёких от лабораторных. Закрытые кожухи, предусмотренные стандартом VPX REDI, надёжно изолируют печатные платы от электрических, механических и климатических внешних воздействий и позволяют осуществлять замену модулей без участия высококвалифицированного технического персонала. Замена может производиться людьми, не имеющими вообще никаких навыков обращения с компьютерной техникой. По сути, стандарт VPX REDI позволяет свести весь комплекс операций по обслуживанию развёрнутых систем к простейшей последовательности действий: извлечению неисправного модуля и установки на его место исправного.

В стандарте VPX REDI нашли свое воплощение давние чаяния военных по поводу того, чтобы типовым элементом замены являлся бы не крейт, а защищённый модуль, для вставки/извлечения которого не требовался бы квалифицированный обслуживающий персонал.

Альтернативы

Технология VPX способна обеспечить преимущество в практически любых приложениях, относящихся к сегментам высокопроизводительных оборонных, аэрокосмических и ответственных систем. Особенно большую пользу VPX приносит в тех задачах, которые хорошо распадаются на отдельные части и могут быть решены путём построения мультипроцессорных конфигураций с широкополосной связью между отдельными центральными процессорами (ЦП). Если обработки очень много и при этом она не обязана быть локализована в одном процессоре, VPX будет прекрасным выбором, поскольку эта технология позволяет создавать хорошо масштабируемые сильносвязанные системы с огромным числом вычислительных узлов.

Хотя во всей красе преимущества VPX проявляются именно в кондуктивных решениях (рис. 4), это не умаляет значения VPX как технологии для построения высоконадёжных высокопроизводительных систем с воздушным охлаждением (рис. 5). Для задач высшей производительности, различных DSP-подобных и кластерных приложений очень важны многочисленные скоростные линии связи между

Рис. 4. Универсальная кондукционная система VPX 3U

Рис. 5. Типовые конвекционные платформы VPX 6U

частями системы. Такие системы нельзя построить на оборудовании CompactPCI или VME, которое в принципе не способно обеспечить достаточный уровень внутрикрейтовой пропускной способности. Многопроцессорные комплексы в стандартах CompactPCI или VME всегда будут слабее VPX-систем просто в силу ограниченности соответствующих системных архитектур. При этом системы CompactPCI и VME ещё и будут менее надёжны, что немаловажно с учётом особенностей тех прикладных областей, которые входят в сферу интересов всех трёх стандартов.

На технологической платформе VPX можно решать едва ли не все мыслимые задачи, требующие высокоскоростной связи между компонентами системы и гибкости при организации внутрисистемных соединений (поддержки разнообразных интерфейсов). Стандарт CompactPCI Serial не позволяет создавать мультипроцессорные конфигурации, поскольку технология PCI Express унаследовала от шины PCI архитектурный принцип выделенного хоста. В архитектурном отношении система CompactPCI Serial представляет собой, по сути, обычный компьютер с одним ЦП и периферийными платами. И, разумеется, стандарт CompactPCI Serial допускает использование лишь одного метода организации внутрисистемных соединений, тогда как VPX поддерживает минимум четыре таких метода. Стандарт VPX позволяет строить любые конфигурации: мультимашинные (рис. 6), мультипроцессорные, мультипроцессорные с периферией и даже сегментированные, в которых определённые периферийные платы могут работать через VPX-коммутаторы только с определёнными хостами, а хосты при этом могут взаимодействовать друг с другом по каналам PCI Express или Gigabit Ethernet. Подобного не позволяет делать ни одна другая системная архитектура, включая MicroTCA. Мультипроцессорные системы на основе MicroTCA создавать можно, но коммутаторы MCH не могут обеспечивать сегментацию. Кроме того, стандарт MicroTCA начисто лишён какой-либо преемственности по отношению к VPX, CompactPCI и другим системным архитектурам. В частности, процессорные и периферийные модули в стандарте MicroTCA (AdvancedMC) имеют совершенно иные размеры, не предусматриваемые привычной механикой 3U/6U. Наконец, системы MicroTCA даже в версиях Rugged/Hardened (спецификации MTCA.1, MTCA.2 и MTCA.3 консорциума PICMG (www.picmg.com) не могут обеспечить тех уровней защищённости и удобства в использовании, которые даёт стандарт VPX REDI. Можно долго спорить о том, где здесь заканчиваются объективные технические преимущества и начинается косность мышления, однако правда в том, что самая консервативная часть целевой аудитории VPX воспринимает шумиху вокруг инициатив наподобие Rugged/Hardened MicroTCA в лучшем случае как шутку.

Рис. 6. Двухмашинный компьютерный кластер с многоядерными процессорами, в формате VPX 6U для систем класса РЭБ

Две причины для жизни VPX

Сегодня VPX – это зрелый промышленный стандарт для использования в самых ответственных проектах. Системная архитектура VPX в её нынешнем состоянии – хорошая основа для решения сложных задач в реальном мире, а не в мире высоких идей. Хотя, как показывает практика, на поле VPX реальный мир и высокие идеи неплохо сосуществуют...

Стандарт OpenVPX принят на вооружение как ведущими мировыми и отечественными производителями изделий уровня плат и систем, так и их многочисленными клиентами. Причём термин «на вооружение» во многих случаях можно понимать буквально. Проблемы VPX, оттягивавшие начало масштабного внедрения этого перспективного стандарта, решены.

Если года три-четыре тому назад ещё могли быть какие-то сомнения относительно того, «взлетит» ли технология VPX, то сегодня ответ на этот вопрос очевиден. За будущее VPX можно быть совершенно спокойным по двум очень простым причинам:

1. Ни одно развитое государство мира не отказывается от планов создания, покупки или продажи современных средств вооружений, развитие которых требует использования совершенных встраиваемых компьютерных технологий. Бюджеты большинства военных ведомств говорят сами за себя.

2. Ни одна магистрально-модульная компьютерная технология на мировом рынке не обладает сегодня аналогичным совокупным набором свойств и преимуществ, делающих её достойным конкурентом VPX при создании огромного разнообразия перспективных ответственных оборонных систем самого различного назначения: от торпеды до бортовой РЛС истребителя или ЗРК.

Пресс-служба ЗАО «РТСофт»

Инновационные технологии и решения «РТСофт» для транспортной отрасли

Фоторепортаж с выставки «ЭкспоСитиТранс-2014»

Компания «РТСофт» продемонстрировала инновационные технологии и решения для транспортной отрасли на III международной выставке «ЭкспоСитиТранс-2014». Мероприятие проходило в конце прошлого, 2014 года в Москве. Посетители стенда «РТСофт» могли получить представление о диапазоне услуг и решений, предлагаемых компанией «РТСофт» как непосредственно предприятиям железнодорожного и общественного транспорта, так и производителям оборудования и системным интеграторам, обслуживающим заказчиков из транспортной отрасли.

Положение компании «РТСофт» на рынке продуктов, услуг и решений для транспорта во многом уникально. Это обусловлено, прежде всего, наличием в портфеле компании широкого спектра базовых аппаратных и программных средств, удовлетворяющих требованиям EN50155 и других международных отраслевых стандартов. Сюда относятся «компьютеры-на-модуле», платы-носители и одноплатные компьютеры, а также встраиваемые операционные системы, ОС реального времени, средства разработки графических интерфейсов и приложений. На стенде «РТСофт» были представлены, в частности, сверхкомпактные одноплатные компьютеры формата Pico-ITX (рис. 1, слева), «компьютеры-на-модуле» типоразмера COM Express basic (рис. 1, справа), платы-носители «компьютеров-на-модуле» и высокопроизводительные процессорные модули для систем CompactPCI.

Наряду с базовыми строительными блоками компания «РТСофт» предлагает своим клиентам из транспортного сектора универсальные модульные аппаратно-программные платформы (рис. 2), легко адаптирующиеся под требования конкретных проектов и значительно ускоряющие создание различного рода информационных систем. Интеграторы, которые работают в транспортной отрасли,

Рис. 1. Одноплатный компьютер формата Pico-ITX (слева) и «компьютер-на-модуле» типоразмера COM Express basic на базе новейших процессоров Intel (справа)

Рис. 2. Конфигурируемая платформа формата CompactPCI 6U

Рис. 3. Бортовой вычислитель «Кена 2.0»

могут использовать платформенные решения для развёртывания беспроводных сетей, организации видеонаблюдения, передачи мультимедийного контента пассажирам и других приложений. В рамках выставки компания «РТСофт» продемонстрировала некоторые собственные оценочные платформы: бортовой вычислитель KenaBoxPC (рис. 3) и защищённый панельный компьютер «РТКон» (рис. 4), а также передовые транспортные компьютеры серии Kontron TRACE и малошумные серверы Kontron KISS с расширенным температурным диапазоном. Основанные на открытых стандартах, данные аппаратные и программные средства обеспечивают значительную экономию времени и средств на разработку и производство информационных систем транспортной ориентации.

Ещё одну группу решений компании «РТСофт» для индустрии общественного транспорта составляют комплексные информационно-управляющие системы, позволяющие полностью автоматизировать процесс управления пригородными пассажирскими перевозками, начиная с продажи билетов, контроля прохода пассажиров через турникеты, подсчёта входящих и выходящих пассажиров на остановочных пунктах, а также сбора и предоставления информации о текущем состоянии каждой единицы подвижного состава (местонахождение, данные о работе и состоянии основных агрегатов, температура воздуха в салоне) и заканчивая представлением комплексных аналитических отчётов. Подобные решения строятся на основе продуктов «РТСофт» из первых двух групп – базовых аппаратных и программных средств и интегрированных платформ – и применяются на объектах транспортной инфраструктуры вне зависимости от специфики и сферы деятельности предприятия (городской, пригородный общественный и ЖД-транспорт, объекты спортивного и культурно-развлекательного назначения и др.). Гости выставки смогли узнать о таких новейших разработках компании, как комплексная система продажи и контроля билетов (рис. 5) и комплексная система управления доступом на объекты транспортной инфраструктуры.

Внимание посетителей стенда привлекла автоматизированная система подсчёта пассажиров, выполненная силами подразделения «УралРТСофт» (г. Екатеринбург). Обеспечивая высокую достоверность результатов подсчёта, данная разработка мо-

Рис. 4. Защищённый панельный компьютер «РТКон» в составе передовой системы мониторинга транспорта

Рис. 5. Автоматизированная билетная система «АСУ–билет»

жет служить хорошим подспорьем при решении весьма широкого круга задач, от оптимизации сборов транспортными компаниями до автоматизации процессов управления технической эксплуатацией устройств электроснабжения и электрификации объектов на основе анализа рисков. Большой интерес вызвала также не имеющая мировых аналогов система транспортного мониторинга (рис. 6), созданная в сотрудничестве с партнеёами компании «РТСофт» и отлично приспособленная к условиям обширных территорий нашей страны (Крайний Север, Сибирь, Дальний Восток), лишённых сотовой связи. Там, где доступны сети 3G, 4G или Wi-Fi, она функционирует подобно большинству других мониторинговых решений. Там же, где обычные каналы передачи данных отсутствуют, система использует спутниковую связь, но за счёт уникального алгоритма и особой схемы организации работы делает это крайне дозированно и эффективно, в результате чего её эксплуатация в среднем обходится не дороже эксплуатации большинства менее продвинутых альтернатив.

Рис. 6. Не имеющая мировых аналогов система онлайн–мониторинга транспорта

Также гостям выставки была представлена информация по такому традиционно сильному направлению бизнеса «РТСофт», как автоматизация управления электроснабжением. Решения компании по защите, автоматизации и диспетчеризации энергохозяйства объектов транспортной инфраструктуры включают автоматизированные системы управления тяговыми подстанциями и комплексные системы мониторинга и сетевого анализа качества электроэнергии. Кроме того, «РТСофт» предлагает программные комплексы планирования и анализа электрических режимов сетей внешнего и тягового электроснабжения с поддержкой функций вероятностных расчётов надёжности электроснабжения и системы технологического управления релейной защитой (РЗА) с поддержкой функций мониторинга и моделирования РЗА. Внедрение подобных решений повышает надёжность функционирования устройств электроснабжения, безопасность и эффективность их эксплуатации.

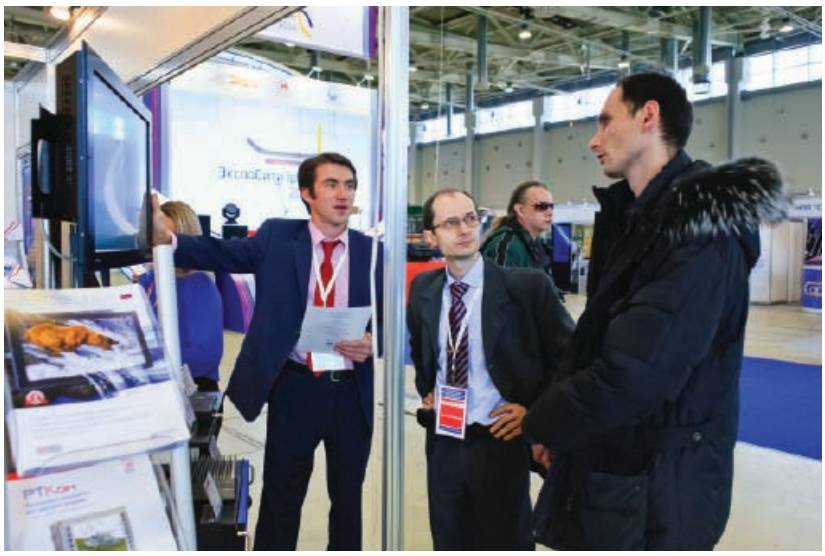


Рис. 7. Специалисты компании «РТСофт» общаются с посетителями выставки

Важное конкурентное преимущество «РТСофт» – ориентация на требования клиента: компания предлагает услуги по разработке и производству аппаратных и программных средств и внедрения информационно-управляющих систем под заказ с тщательным учётом специфики конечных задач. Посетители стенда компании смогли получить квалифицированные консультации по технологиям, решениям и услугам, предлагаемым компанией «РТСофт» транспортному сектору (рис. 7).

Стэн Шнайдер (Stan Schneider), технический эксперт

Протоколы «Интернета вещей»: основные сведения

Интернет полностью изменил способы коммуникаций и совместной работы людей. Он ознаменовал собой начало новой эры свободной информации для каждого, трансформируя жизнь до такой степени, которую трудно было вообразить раньше. Однако следующий этап развития Интернета связан не с людьми. Он касается интеллектуальных устройств с возможностью установления между ними связи.

Чтобы успешно взаимодействовать с реальным миром, эти устройства должны совместно работать на таких скоростях и обладать такими возможностями, которые значительно превосходят те, которые нужны людям или используются людьми. «Интернет вещей» (Internet of Things – IoT) изменит мир, возможно, более основательно, чем современный Интернет, ориентированный на людей.

Введение

Сегодня Интернет обеспечивает соединение веб-сайтов и рабочих станций. В настоящее время в нём насчитывается гигантское количество сайтов – почти миллиард, что оказывает сильное влияние на все стороны нашей жизни (рис. 1).

С пугающей скоростью – всего за несколько лет – мобильная революция обеспечила сотовыми телефонами бóльшую часть населения мира. Имея в своем распоряжении более 5 миллиардов смартфонов, большинство людей уже имеет или вскоре получит мобильный доступ к сети.

Кроме того, в мире насчитывается 50 млрд интеллектуальных устройств. «Интернет вещей» позволит им устанавливать между собой связь и обеспечит создание в полном смысле слова распределённых приложений с межмашинной (machine-to-machine – M2M) связью. «Интернет вещей» в 50 раз превысит по объёму традиционный Интернет. Он обеспечит соединение в 10 раз большего числа устройств, чем это позволила в своё время сделать мобильная революция, и станет стимулом дальнейших преобразований нашей жизни.

Где же все эти устройства? Да среди нас. Они часть нашей повседневной жизни. В реальности вы владеете многими из них! В новейших автомобилях применяется более 100 процессоров. Интеллектуальные устройства проникают в промышленные комплексы, больницы, дома, транспортные системы и другие сферы жизни. Сегодня эти системы связаны пока не сильно, но такое положение вещей быстро меняется.

Соединение устройств в таком масштабе позволяет создавать приложения, возможности которых поражают воображение. «Интернет вещей» обеспечит фундаментальные вещи, которые не были реализованы прежде. Некоторые представление об этих новых возможностях уже можно достаточно ясно себе представить.

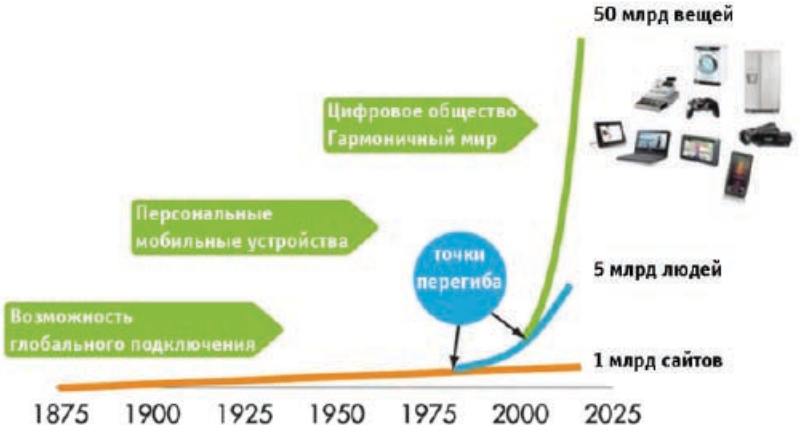


Рис. 1. В последнее время отмечается резкое увеличение числа устройств с выходом в сеть

Что такое «Интернет вещей»?

В начале 1990-х годов суть каждой новой технологии представлялась, как ворота в информационную супермагистраль. На самом деле такие виды аналогий не помогали дать точное определение Интернета. В действительности Интернет оказался новым способом разделения Вашей жизни с другими людьми, новой бизнес-моделью совершения покупок, а также новым способом дать образование Вашим детям. Интернет определяется в большей степени тем, что можете делать Вы, а не тем, что́ делает он. От подобного недоразумения страдает и «Интернет вещей».

Крупные компании – игроки на поле информационных технологий – определяют понятие «Интернета вещей» по-разному. Cisco называет его «Интернетом всего» (или «Всеобъемлющим Интернетом» – Internet of Everything) и говорит, что это будет «последняя волна Интернета – соединение физических объектов для достижения более высокого уровня безопасности, комфорта и эффективности». IBM описывает «Интернет вещей» как «совершенно новую всемирную паутину, состоящую из сообщений, которые могут передавать между собой устройства в цифровой форме. Этот тот же самый Интернет, но другая сеть».

«Промышленный Интернет» (Industrial Internet) компании General Electric (GE) – пожалуй, наиболее захватывающая концепция, поскольку даёт возможность непосредственно представить себе новые приложения. С точки зрения GE, промышленный Интернет представляет собой «объединение агрегатов и интеллектуальных данных с целью создания гениальных машин».

Девиз компании RTI – Your Systems. Working as One, то есть «Ваши системы. Работая как один». В компании настаивают на том, что «Интернет вещей» будет представлять собой совершенно новый сервис. Он будет таким же основательным, как сотовая сеть, GPS или сам Интернет.

Каждый описывает будущее по-своему, но все сходятся во мнении, что «Интернет вещей» и интеллектуальные системы, которые он позволит создать, принципиально изменят наш мир.

Обзор протоколов

Устройства (D) должны устанавливать друг с другом связь (D2D). Затем нужно собрать и передать данные с этих устройств в серверную (S) инфраструктуру (D2S). Эта серверная инфраструктура должна совместно использовать данные (S2S), имея возможность передавать данные обратно устройствам, программам анализа или людям. Если посмотреть «с высоты птичьего полёта», то можно выделить следующие протоколы для решения задач в этой инфраструктуре:

- MQTT: протокол для сбора данных устройств и передачи их серверам (D2S);
- XMPP: протокол для соединения устройств с людьми, частный случай D2S-схемы, когда люди соединяются с серверами;
- DDS: быстрая шина для интегрирования интеллектуальных устройств (D2D);
- AMQP: система организация очередей для соединения серверов между собой (S2S).

Каждый из этих протоколов широко распространён. Есть по крайней мере 10 вариантов реализации каждого из них. Понятно, что в них легко запутаться, так как на верхнем уровне они схожи. По сути, все четыре вышеперечисленных протокола представляют собой протоколы «Интернета вещей» реального времени с публикацией/подпиской, которые способны соединять тысячи устройств. Справедливость этого представления зависит от того, как Вы определяете термины «реальное время», «вещи» и «устройства».

На самом деле эти протоколы очень разные. Современный Интернет поддерживает сотни протоколов. «Интернет вещей» будет поддерживать ещё на сотни протоколов больше. Важно уяснить сферу применения каждого из них.

Простая схема, приведённая на рис. 2, отражает основные сценарии использования этих протоколов. Конечно, в действительности это не так просто. Например, «подсистема управления» (control plane), которая обеспечивает контроль за

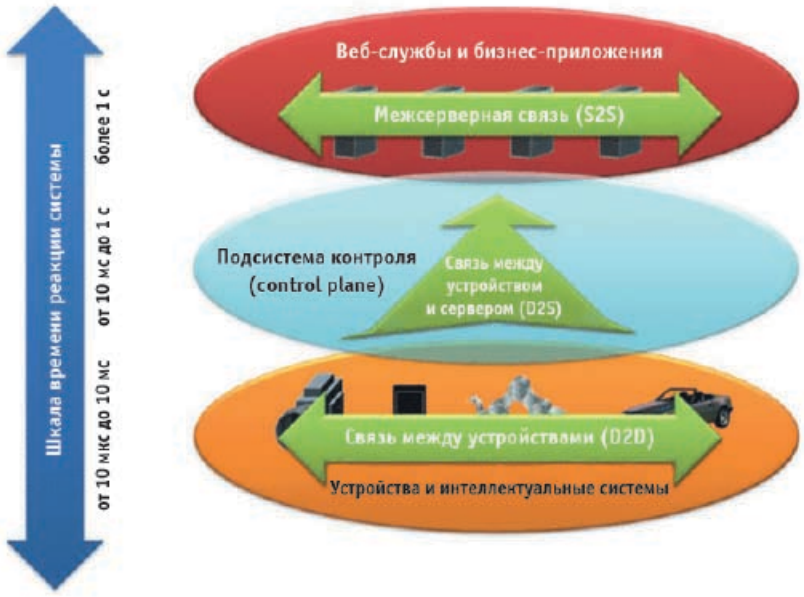


Рис. 2. Протоколы «Интернета вещей» и время реакции системы

всеми соединениями и управление ими, достаточно сложна. Многие протоколы взаимодействуют именно в её рамках.

MQTT

Протокол MQTT (Message Queue Telemetry Transport) обслуживает сбор данных с устройств (рис. 3). Как следует из названия этого протокола, основное его назначение – телеметрия, или дистанционный мониторинг. Его задача состоит в сборе данных от множества устройств и передача этих данных в IT-инфраструктуру. Он предназначен для крупных сетей небольших устройств, которыми нужно управлять из облачной сети.

Протокол MQTT обеспечивает лишь возможность передачи между устройствами, но не распределяет данные по многим получателям. Поскольку протокол MQTT имеет вполне определённое применение, он несложен и обеспечивает всего несколько опций управления. Кроме того, ему не нужно быть очень быстрым. В связи с этим режим «реального времени» обычно измеряется в секундах.

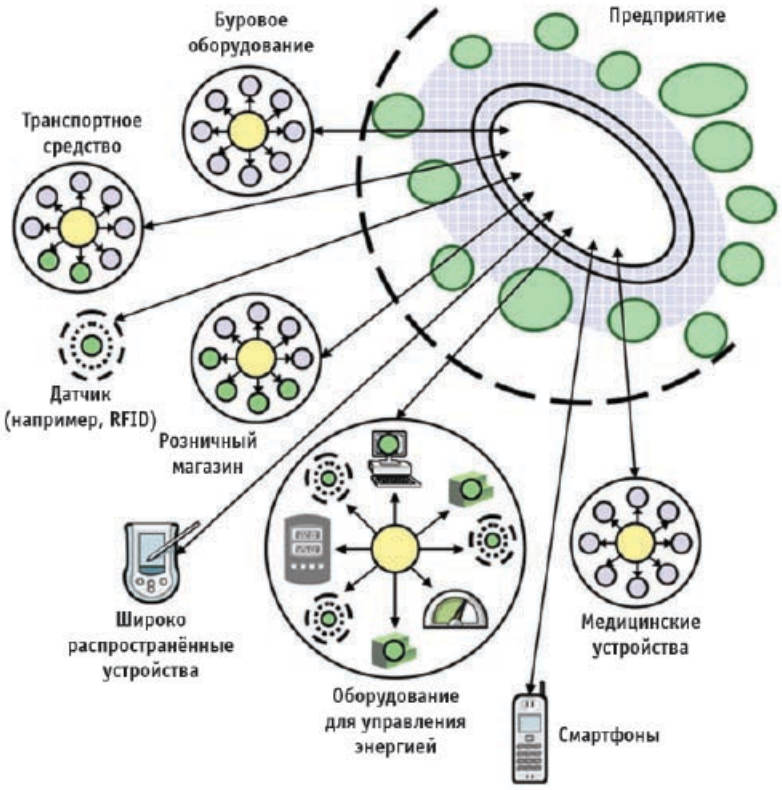


Рис. 3. Протокол MQTT реализует систему на основе звездообразной сети

Для MQTT обычно используется архитектура звездообразной сети. Все устройства подключены к серверу концентратора данных, подобно новому решению MessageSight от IBM. Поскольку терять данные совсем не желательно, этот протокол работает поверх TCP, что обеспечивает простой и надёжный поток данных. В связи с тем, что эти данные использует IT-инфраструктура, вся система предназначена для простой передачи данных в системы предприятий и компаний, например такие, как ActiveMQ и сервисные шины предприятий (enterprise service buses – ESB).

Протокол MQTT обеспечивает такие приложения, как мониторинг утечек и контроль за возможной умышленной порчей нефтепроводной сети. Тысячи датчиков такой системы должны быть сосредоточены в одном месте для анализа. Когда в такой системе возникает какая-либо проблема, имеется возможность предпринять действия для коррекции этой проблемы. Другими приложениями для MQTT могут быть контроль потребления энергии, управление светом и даже интеллектуальное садоводство.

Этот протокол участвует в сборе данных от множества источников и делает их доступными для IT-инфраструктуры.

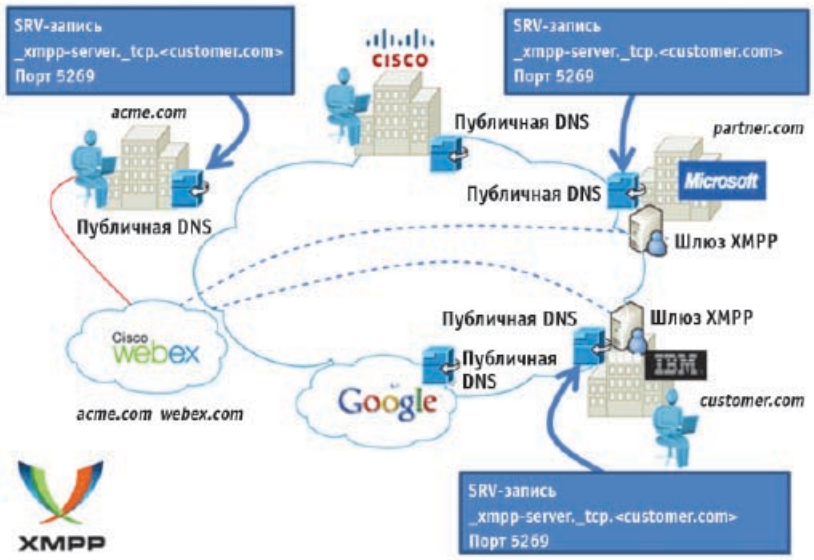


Рис. 4. Протокол XMPP обеспечивает обмен текстовыми сообщениями между точками доступа

XMPP

Протокол XMPP поначалу назывался Jabber. Он был разработан для системы мгновенного обмена

сообщениями для связи между людьми с помощью текстовых сообщений (рис. 4). XMPP означает Extensible Messaging and Presence Protocol, или расширяемый протокол обмена сообщениями и информацией о присутствии. И вновь название даёт неверное представление о целевом использовании, ведь присутствие означает непосредственное участие людей.

В протоколе XMPP используется текстовый формат XML в качестве встроенного типа, обеспечивая естественную связь между людьми. Подобно MQTT он работает по TCP или, возможно, по HTTP поверх TCP. Его преимуществом является метод адресации вида name@domain.com, который помогает соединять пользователей в огромном пространстве Интернета.

Применительно к «Интернету вещей» XMPP обеспечивает простой способ адресации устройств. Это особенно удобно, когда данные передаются между отдалёнными, чаще всего независимыми точками, как в случае связи между двумя абонентами. Этот протокол не обладает высокой скоростью. Фактически, в большинстве реализаций этого протокола используется метод опроса или проверки дополнений только по требованию. Протокол, называемый BOSH (Bidirectional streams over Synchronous HTTP) позволяет серверам принимать сообщения. Но масштаб «реального времени» для XMPP близок к человеческому масштабу и измеряется в секундах.

XMPP реализует существенное преимущество, например, при подключении Вашего домашнего термостата к веб-серверу, чтобы Вы могли получить к нему доступ с Вашего телефона. Сильными сторонами этого протокола является адресация, безопасность и масштабируемость, что делает его идеальным для приложений «Интернета вещей» с ориентацией на потребителя.

DDS

В отличие от MQTT и XMPP протокол DDS (Data Distribution Service – сервис распределения данных) обслуживает устройства, которые непосредственно используют данные устройств. Этот протокол распределяет данные по другим устройствам (рис. 5). Хотя этот протокол поддерживает интерфейс с IT-инфраструктурой, основная задача DDS заключается в соединении устройств с другими устройствами. Это ориентированный на данные стандарт промежуточного ПО, используемый в высокопроизводительных военных, промышленных и встраиваемых приложениях. Протокол DDS способен эффективно и синхронно доставлять множеству получателей миллионы сообщений в секунду.

Устройства запрашивают данные иначе, чем IT-инфраструктура. Во-первых, устройства работают быстро. Масштаб «реального времени» часто измеряется в микросекундах. Устройствам нужно осуществлять связь с другими устройствами, используя сложные пути, поэтому простые и надёжные двухточечные TCP-потоки данных ограничивают возможности такой передачи. Взамен этого DDS обеспечивает детализированный контроль качества сервиса (QoS), многоадресную передачу, перестраиваемую надёжность и всеобъемлющую избыточность. Кроме того, сильной стороной DDS является разветвление данных. Протокол DDS обеспечивает мощные способы фильтрации и отбора данных по адресам назначения, причём число синхронных получателей данных может исчисляться тысячами. Некоторые устройства довольно компактны, поэтому существуют облегчённые версии DDS, которые работают в условиях ограниченного объёма.

Для использования данных от устройств звездообразная сеть совершенно не годится. Вместо этого DDS реализует прямую шинную связь между устройствами на базе реляционной модели данных. В компании RTI её называют шиной данных (DataBus), поскольку это сетевой аналог базы данных (database).

Подобно тому, как база данных управляет доступом к хранимым данным, шина данных управляет доступом к данным и обновлениями одновременно многими пользователями. Это именно то, что нужно высокопроизводительным устройствам, чтобы они работали вместе как единая система.

Рис. 5. Протокол DDS реализует архитектуру публикации и подписки

Высокопроизводительные системы интегрированных устройств используют протокол DDS. Это единственная технология, которая обеспечивает гибкость, надёжность и скорость, необходимые для построения сложных приложений реального времени. Эти приложения включают в себя военные системы, ветроэлектростанции, интегрированные системы больниц, системы диагностической визуализации,

системы сопровождения ресурсов и автомобильные системы испытаний и обеспечения безопасности. Протокол DDS с высокой скоростью соединяет устройства внутри работающей распределённой системы.

AMQP

И наконец протокол AMQP (Advanced Message Queuing Protocol, или усовершенствованный протокол организации очереди сообщений), который иногда рассматривают как протокол «Интернета вещей» (протокол IOT). Как следует из названия, AMQP обслуживает исключительно очереди (рис. 6). Он пересылает транзакционные сообщения между серверами. Этот протокол, в качестве ориентированного на сообщения промежуточного ПО, был создан для банковской отрасли и способен обрабатывать тысячи организованных в очередь транзакций.

В протоколе AMQP большое внимание уделено борьбе с потерей сообщений. Различные коммуникационные линии – от поставщиков контента до коммутаторов каналов и от списков очередности до пользователей – используют протокол TCP, который обеспечивает высоконадёжное двухточечное соединение. Кроме того, конечные точки должны подтверждать принятие каждого сообщения. Данный стандарт описывает также опциональный режим транзакций с формальной многофазной последовательностью обновления транзакций. Оставаясь верным своему происхождению (банковская отрасль), промежуточное программное обеспечение AMQP сфокусировано на слежении за всеми сообщениями и обеспечении их доставки по назначению, независимо от наличия сбоев и перезагрузки системы.

AMQP используется главным образом в обмене деловыми сообщениями. Обычно под «устройствами» понимают мобильные телефоны, поддерживающие связь с центрами обработки данных в операционных офисах. В случае «Интернета вещей» AMQP наилучшим образом подходит для реализации функций «подсистемы управления» (control plane) или аналитических функций на базе серверов.

Заключение

Для «Интернета вещей» требуется множество протоколов. Четыре типа протоколов, которые были рассмотрены в данной статье, заметно различаются между собой. Вероятно, проще всего классифицировать их по нескольким ключевым параметрам: качеству сервиса, адресации и приложению.

Контроль качества сервиса (QoS) значительно лучше характеризует протокол, чем тяжеловесное понятие «режима реального времени». Контроль качества сервиса связан с гибкостью доставки данных. Систему со сложным контролем качества сервиса труднее программировать, но на её основе можно построить приложение с более высокими требованиями.

Рассмотрим, например, такой показатель, как надёжность. Большинство протоколов работает поверх TCP, что обеспечивает простой уровень надёжности. Каждый байт, попадающий в коммуникационный канал, должен быть доставлен получателю, даже если понадобится выполнить множество попыток. Это реализуется просто и чаще всего без проблем, но не позволяет управлять синхронизацией. В случае медленного абонента одноканальный TCP-трафик дублируется.

По контролю качества сервиса заметно отличается от других протоколов протокол DDS, поскольку ориентирован на коммуникации между устройствами. Кроме надёжности, DDS обеспечивает также контроль так называемой «жизнеспособности» (при исследовании проблем), обнаружения и использования ресурсов, а также синхронизации.

Помимо этого, фундаментальной проблемой является поиск данных в огромной базе данных «Интернета вещей». Здесь с лучшей стороны проявляет себя протокол XMPP. Его схема адресации типа user@domain полностью использует правила, установившиеся в Интернете. Одна-

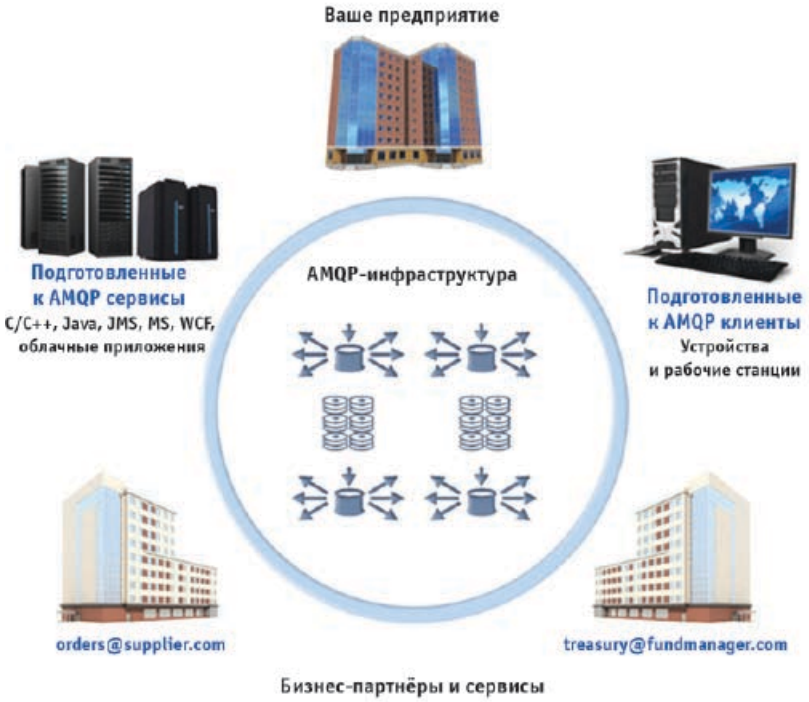


Рис. 6. Протокол AMQP – ориентированное на сообщения промежуточное ПО, созданное для банковской отрасли

ко XMPP не способен запросто обрабатывать большие массивы данных, относящихся к одному серверу. Протокол MQTT, благодаря своей связи с сервером, справляется с подобной задачей лучше. Если Вы можете подключиться к такому серверу, то Вы соединяетесь с сетью. Очереди AMQP действуют подобно серверам, но для S2S-систем. И в этом случае DDS сильно отличается от других протоколов. Вместо сервера он использует специальный фоновый протокол, который автоматически отыскивает данные. DDS-системы обычно более ограниченны. Особого внимания требует поиск по распределённой сети (WAN) или обширным группам устройств.

Пожалуй, ключевые особенности протоколов зависят от их предполагаемого применения. Использование данных между устройствами в корне отличается от сбора данных на устройстве. Например, включение освещения (в этом случае оптимальным вариантом является XMPP) совершенно отличается от генерирования энергии (DDS), мониторинга линий передачи (MQTT) или анализа потребления энергии в центре обработки данных (AMQP).

Конечно, есть перекрывающиеся области применения протоколов. Например, DDS может обслуживать и принимать данные из облачных сред, а MQTT – передавать информацию обратно в устройства. Тем не менее основные задачи всех четырёх протоколов различны, различны архитектуры и возможности. Все эти протоколы критичны к (быстрой) эволюции «Интернета вещей». «Интернет вещей» – большое пространство, в котором существует множество протоколов. Поэтому к выбору оптимального протокола для своего приложения нужно подходить основательно, и объективно взвешивать все положительные и отрицательные свойства каждого из них.

Источник: http://electronicdesign.com/print/embedded/understanding-protocols-behind-internet-things

Новости рынка

Операционная система для «Интернета вещей» от ARM

Компания ARM, известный разработчик полупроводниковых чипов, выступая в непривычной для публики роли, готовит к выпуску новую операционную систему, призванную сыграть большую роль в создании «Интернета вещей».

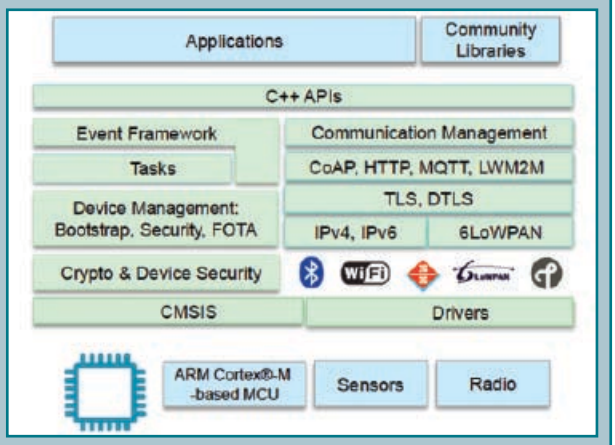
По замыслу создателей, ОС mbed реализует общий программный уровень для обеспечения защиты и соединения множества устройств (от светильников уличного освещения и газовых счётчиков до бытовых приборов), которые, как ожидается, будут в ближайшие годы связываться в сети.

Вместе с этой операционной системой ARM планирует продавать mbed Device Server – серверное ПО для сбора данных от устройств «Интернета вещей» и предоставления их другим сервисам, например аналитическим программам.

В настоящее время в устройствах «Интернета вещей» используется смесь различных ОС, и, по мнению специалистов ARM, нужна доминирующая компания, с которой могли бы сотрудничать разработчики и сервис-провайдеры. ОС mbed поможет компаниям лучше использовать данные, полученные от связанных друг с другом интеллектуальных устройств.

Устанавливаться ОС mbed может, например, в городских светильниках уличного освещения, собирая данные о количестве пешеходов и определяя потребность во включении и выключении света, что позволяет экономить электричество.

ОС mbed будет доступна в 2015 году для бесплатного использования в микросхемах на базе продуктов ARM.



Компания ARM больше всего известна своим процессором Cortex-A, который используется в смартфонах, планшетных компьютерах и носимых устройствах. Но в них уже есть операционные системы, такие как Android и iOS.

Кроме того, ARM выпускает семейство микроконтроллеров Cortex-M. Эти менее мощные микросхемы можно найти во встроенном оборудовании типа счётчиков платы за парковку и антиблокировочных тормозных систем (ABS). Именно на эти чипы нацелена ОС mbed.

Разработка mbed началась в 2006 году. Серверное ПО mbed device server разработано компанией Sensinode, которую ARM купила в 2013 году.

Идеология ОС mbed поддерживается множеством партнёров, включая таких поставщиков ПО, как IBM и Salseforce.com (что гарантирует подключение их приложений к mbed-серверам для сбора данных) и производителей чипов типа Freedcale и Broadcom.

(окончание на стр. 24)

Андрей Пронин, Вячеслав Ванюлин, Игорь Починок, Auriga, Inc., НИВЦ МГУ

Тестирование встроенного программного обеспечения

В статье описывается опыт создания эффективной тестовой платформы, включая инфраструктуру, виртуальную лабораторию и процесс тестирования.

Особенности тестирования встроенного программного обеспечения

Специфика встроенного программного обеспечения (ПО) задаёт определённые требования к организации процесса тестирования. С одной стороны, специалист по тестированию заметит много общего с процессом тестирования прикладного ПО, но, с другой стороны, выявит и немало отличий.

M2M вместо UI

Первое, что бросается в глаза, – функциональность пользовательских интерфейсов (UI – User Interface) обычно ограниченна: консольное текстовое меню, интерфейс командной строки, набор цифровых входов и выходов и, пожалуй, всё. С другой стороны, интерфейсы для M2M и межкомпонентного взаимодействия могут обладать обширными функциональными возможностями и быть очень сложными, например API для высокоуровневого ПО, различные сетевые протоколы для обмена данными и управления. Поэтому основной фокус при тестировании встроенного программного обеспечения смещается с тестирования пользовательских интерфейсов на тестирование компонентов, неочевидных для конечных пользователей.

Зависимость от оборудования

Второе существенное отличие – высокий уровень зависимости от аппаратного обеспечения. Даже в том случае, когда встроенное ПО построено на базе более-менее стандартного программного фреймворка, оно должно учитывать особенности конкретной аппаратной платформы. По определению, встроенное программное обеспечение разрабатывается для конкретного аппаратного модуля (или, что встречается чаще, комплекса аппаратных средств).

Зачастую подобные аппаратные модули разрабатываются одновременно с соответствующим встроенным ПО. Именно оно первым запускается на данном оборудовании. В отличие от сферы разработки приложений, в случае встроенного ПО у разработчика нет возможности быть уверенным в том, что операционная система была протестирована для конкретной аппаратной платформы или что возможности самой аппаратной платформы по исполнению различных программ были тщательным образом проверены. В результате разработанное программное обеспечение может содержать куски кода, специфичные для конкретных версий аппаратной платформы.

Работа встроенного ПО может зависеть от таких вещей, на которые инженеры, как правило, не обращают внимания при разработке прикладного ПО, например от длины кабеля, частоты последовательного порта или типа устройств, подключённых к шине обмена данными. Всё это делает успешную работу встроенного программного обеспечения в большей степени зависимой от конкретного аппаратного модуля или поведения других модулей в той же шине или сети.

По сравнению со стандартной разработкой, такие вещи, как «состояние гонки» (далее используется оригинальное название – «race conditions»), чаще всего вызываются не взаимодействием внутренних компонентов самого программного обеспечения, а взаимодействием программного обеспечения со средой. Таким образом, количество факторов и параметров, влияющих на работу встроенного ПО намного выше. Воспроизведение дефектов поэтому также гораздо сложнее.

Сложности обновления встроенного ПО

Процедуры поддержки, такие как развёртывание и обновление программного обеспечения, получение отладочной информации, также отличаются от того, что используется для традиционного прикладного программного обеспечения, где можно полагаться на plug-and-play, автоматическую конфигурацию, мастера установки, наличие удобного отладчика в IDE, или, по меньшей мере, можно сбросить лог-файл на диск.

В мире встроенного ПО обновления требуют перевода программного обеспечения в специальный режим, удаления EEPROM-защиты от записи, подключения к серверу раздачи файлов (например, TFTP), нескольких перезагрузок и тому подобных вещей. Таким образом, весь этот процесс весьма длителен и неудобен. Кроме того, может оказаться, что устройство хранения файлов поддерживает только ограниченное количество циклов перезаписи.

Поэтому на этапе активной разработки, версии, как правило, обновляются реже, чем это происходит для других видов ПО. Новые ревизии, как правило, развёртываются после того, как было исправлено значительное количество дефектов. Соответственно, главная задача тестирования на этом этапе – выявление как можно большего числа дефектов, не останавливая процесс после обнаружения первого, даже если он вызывает сбой продукта.

Необходимость промежуточных инструментов тестирования

Тестировать M2M-интерфейсы вручную невозможно. Поэтому перед началом тестирования встроенного ПО нам необходимо разработать специальные приложения – агенты тестирования, которые позволяют создавать входной сигнал и получать ответ системы через доступные интерфейсы. Часто также требуется эмулировать специфические паттерны электрических сигналов на различных линиях передачи данных, чтобы протестировать поведение встроенного ПО в различных ситуациях. Для этого может использоваться специальный аппаратно-программный комплекс.

Ограниченная доступность оборудования

Учитывая высокий уровень зависимости от аппаратной платформы и тот факт, что встроенное программное обеспечение часто разрабатывается одновременно с самой платформой, стоит отметить некоторые важные последствия этого.

Во-первых, на момент активной разработки может быть готово к использованию лишь малое число образцов новейшего оборудования. Во-вторых, диапазон типов аппаратных модулей, для которых требуется выполнить тестирование ПО, может быть достаточно широким. Соответственно, команда тестировщиков вынуждена распределять это ограниченное количество аппаратных модулей между собой и/или организовывать удалённый доступ к ним. Во втором случае инженеры не имеют физического доступа к аппаратному обеспечению.

Проблемы с определением источника дефектов

При тестировании новой, только что разработанной аппаратной платформы обычно выявляется большое количество дефектов самого аппаратного обеспечения. При этом любой обнаруженный дефект может быть вызван как ПО, так и самой аппаратной платформой. Об этом важно постоянно помнить. Хуже всего то, что программное обеспечение может прекрасно работать с одной версией аппаратного модуля и иметь проблемы при работе с другой версией.

Высокая ценность каждого выявленного дефекта

Мы уже писали выше о том, что в случае с встроенным ПО дефекты воспроизвести сложнее. Именно поэтому каждый такой дефект ценен сам по себе, и обязанность тестировщика – собрать максимум информации о нём в момент выявления, так как второй раз воспроизвести его, возможно, удастся не скоро. В сочетании с очень ограниченными возможностями по отладке встроенного программного обеспечения это ставит перед инженерами дополнительные непростые задачи.

Ограничения, связанные с обновлениями программного обеспечения, требуют настойчивости и упорства в процессе тестирования, выявления максимального количества дефектов для каждой версии программного обеспечения, придают особую важность процессам сборки и развёртывания.

Высокие требования к автономности системы

Необходимость устойчивости системы к вводу некорректных данных и её автономности требует очень тщательного стрессового тестирования. Как следствие – требуется эмулировать последовательность быстро сменяющихся событий, чтобы проверить код на все возможные race conditions.

Основы подхода и платформы тестирования

Автоматизированное тестирование

Очевидно, что использование ручного тестирования в качестве основного метода для встроенного ПО практически нереализуемо. Необходимость проведения рутинного, длительного, повторяющегося стрессового тестирования; работа с M2M-интерфейсами;

высокая потребность в выявлении race conditions для часто сменяющихся событий,, а также ряд других факторов подводят нас к выводу, что поле боя остаётся за автоматизированным тестированием.

Конечно, всегда остаётся небольшой процент тестов, которые более выгодно проводить вручную, чем автоматизировать. Но этот процент ниже обычного, что объясняется более высокой относительной эффективностью автоматизации в среде с удалённым доступом и специальными средствами поддержки, которые будут описаны дальше. В любом случае автоматизация обычно успешно реализуется для более чем 95 % тестовых сценариев. При этом важно понимать, что автоматизация и использование агентов тестирования не просто изменяет способ выполнения тестовых сценариев и демонстрации результатов, но оказывает влияние на все аспекты процесса тестирования.

Проектирование тестов и отслеживание требований

Поскольку большинство тестовых сценариев в случае тестирования встроенного ПО не может быть выполнено вручную, стандартный подход к проектированию тестов (сбор требований, разработка тестовых сценариев, ручное тестирование, оптимизация, исправление, детализация, создание сценария на базе кейсов ручного тестирования) здесь не сработает.

Вместо этого на основании требований к встроенному ПО создаются два артефакта: набор тестовых сценариев и требования к тестовой среде, которая состоит из фреймворка автоматизации и агентов тестирования. Формально, требования к встроенному программному обеспечению преобразуются в тестовые сценарии, которые, в свою очередь, формируют требования к тестовой среде и агентам. Но на практике тестовые сценарии и требования к вспомогательному программному обеспечению не разделяются.

Валидация инфраструктуры для поддержки тестирования

Ещё один фактор, влияющий на процесс тестирования ПО, – это требование валидации самого вспомогательного ПО. Фактически, это означает, что вначале необходимо протестировать саму среду тестирования и агенты, то есть инженеры должны выполнить весь стандартный комплекс действий, включая проектирование тестов, их выполнение, анализ покрытия и др. Агенты тестирования, как правило, представляют собой достаточно простые программные решения с ограниченным набором требований, поэтому их тестирование намного проще, чем тестирование оригинального программного продукта. Тем не менее зачастую для них требуется внедрять сложные протоколы обмена данными (включая шифрование, аутентификацию, компрессию, установление соединения и др.), поэтому на деле их тестирование не такая уж простая задача.

Полноценное тестирование агентов часто невозможно при отсутствии более-менее рабочей версии целевого процесса. Таким образом, успешное прохождение теста агентом также означает успешное прохождение базовых функциональных тестов в определённой области для конечного ПО.

Во время этого тестирования широко используются верифицированные ранее агенты тестирования и инструменты отладки аппаратного обеспечения, такие как анализаторы шины, сетевые анализаторы пакетов, зонды JTAG и осциллоскопы. Средства отладки особенно эффективны на данном этапе, цель которого – получение приложения с базовым функционалом. Это ещё одно естественное следствие процесса разработки встроенного программного обеспечения. Разработка инструментов поддержки тестирования выполняется параллельно с проектированием проектного встроенного программного обеспечения, а планы разработки как целевого ПО, так и агентов тестирования в значительной степени зависят друг от друга.

Вторая составляющая процесса тестирования – среда автоматизированного тестирования – также требует валидации. Тем не менее в отличие от агентов тестирования, которые выполняют функции, имеющие отношение к конкретному встроенному продукту, она может и должна проектироваться и реализовываться независимо от реального проекта, в рамках более широкого технологического или организационного сегмента. Такая реализация поможет существенно сократить трудовые издержки, а также отменит необходимость создания такой среды для каждого нового проекта.

Отслеживание и анализ дефектов

Кроме собственно самих процессов верификации и валидации, сильное влияние на жизненный цикл дефектов и настройку репозитария отслеживания дефектов оказывает необходимость валидации инфраструктуры. Для встроенного программного обеспечения необходимо учитывать несколько возможных вариантов происхождения дефектов: конечное ПО, аппаратное обеспечение или инфраструктура поддержки тестирования. На практике это требует указания для каждого обнаруженного дефекта идентификаторов целевого ПО, аппаратного обеспечения и инструмента тестирования. Кроме того, рекомендуется включить представителя команды разработки вспомогательной инфраструктуры тестирования в рабочую группу по приоритизации задач при устранении дефектов (да-

лее используется в оригинальном значении – triage committee).

Для поиска дефектов, вызванных аппаратным обеспечением, команда тестирования должна включать в себя специалиста с хорошими познаниями в области аппаратного обеспечения и опытом работы с различными инструментми по отладке аппаратного обеспечения, упомянутых выше. Этот специалист также должен входить в triage committee. В его задачи входит анализ каждого дефекта на предмет его возникновения вследствие проблем с аппаратным обеспечением, сбор и анализ дополнительных данных при возникновении предположений в аппаратном происхождении дефекта, а также консультирование команды тестирования в случае любого сомнительного поведения аппаратного обеспечения.

Матрица покрытия аппаратного обеспечения

Высокая вероятность выявления ошибок аппаратного обеспечения не означает, что всё исчерпывается только необходимостью указания идентификаторов оборудования в описании дефекта или включения инженера по аппаратному обеспечению в команду тестирования. Конечное ПО также необходимо протестировать на всех целевых типах и ревизиях аппаратного обеспечения. Это вовсе не означает, что каждый тестовый сценарий должен быть запущен на всех возможных модулях/типах/версиях аппаратного обеспечения. Необходимо сделать осознанный выбор между полнотой покрытия аппаратного обеспечения и трудозатратами. Зачастую возможно объединить модули аппаратного обеспечения в группы для тестирования каждой функциональной области или, по меньшей мере, произвести случайную выборку для регрессионного тестирования. При этом стратегии тестирования в разных проектах могут отличаться друг от друга в зависимости от требований и ограничений конкретного проекта.

В любом случае матрица покрытия аппаратного обеспечения необходима. В ней должны содержаться все комбинации «тестовый сценарий – модуль аппаратного обеспечения», которые запланированы к верификации. По вполне очевидным причинам, среда автоматизированного тестирования обязана позволять дальнейшие спецификацию и изменение матрицы, которые не должны сказываться при этом на тестовых сценариев.

Отслеживание сборок программного обеспечения

Правильно построенный процесс сборки и развёртывания программного обеспечения – существенный элемент успеха тестирования встроенного ПО. Крайне важно правильно идентифицировать сборку целевого ПО, для которой был обнаружен дефект. Для решения проблем, связанных с идентификацией сборки ПО, существует несколько методов.

Один из полезных методов – получение номера сборки с запущенного программного обеспечения в начале выполнения набора тестов. Обычно, если у встроенного ПО есть какой-либо пользовательский интерфейс, он позволяет получить такую информацию. Использование этого метода предотвращает неверную идентификацию версии ПО в описании дефекта, если набор тестов был по ошибке запущен на неверной сборке.

Другой метод используется для smoke-тестов для стабильных версий ПО. На практике инфраструктура поддержки тестирования содержит в себе все необходимые инструменты для создания сборки, назначения ей уникального номера, маркировки её в дереве исходного кода, архивации бинарных файлов, передачи их на сервер развёртывания (TFTP-сервер) и затем на целевую плату, а также обновления ПО на плате. Все эти операции могут быть выполнены перед началом ночного smoke-теста для стабильной сборки ПО. Для проектов, не имеющих ограничений по количеству обновлений ПО для целевого аппаратного модуля, эти операции могут быть выполнены полностью (сборка и развёртывание на плате) или частично (только развёртывание) перед каждой сборкой, гарантируя тестирование правильной версии ПО.

Поддержка отладки

Помимо обнаружения максимального количества ошибок, качественно выстроенный процесс тестирования ставит своей целью также помощь разработчикам в исправлении дефектов. Согласитесь, дефект, найденный командой тестирования, имеет мало ценности, если он не может быть воспроизведён и, соответственно, исправлен командой разработчиков из-за отсутствия достаточной информации.

Как уже было сказано выше, при работе с встроенным ПО воспроизведение дефектов вызывает много сложностей, поэтому при первом появлении дефекта необходимо собрать о нём как можно больше информации. В связи с тем, что отладка встроенного ПО также намного сложнее, чем отладка прикладного ПО, команда разработки зачастую использует специальные отладочные сборки или специальные режимы отладки целевого ПО с усовершенствованными возможностями протоколирования.

Эта ситуация приводит к двум важным следствиям. Во-первых, расписание и другие характеристики отладочных и стабильных сборок целевого ПО могут отличаться, и дефект, который зафиксирован в одной

версии, может отсутствовать в другой. Поэтому так важно при тестировании отслеживать версии сборки программного обеспечения, в которых обнаружен дефект.

Во-вторых, тестовые сценарии должны быть разработаны таким образом, чтобы при необходимости позволить использование расширенных возможностей отладочной версии или режима. Когда дефект обнаружен, тестовый кейс должен сохранить результат отладки ПО в протоколе соответствующего тестирования, чтобы разработчик, перед которым стоит задача по исправлению дефекта, мог использовать эти данные во время анализа. Тестовый кейс должен также включать возможность определения типа версии целевого ПО – отладочная или релизная или переключения между режимами. Эти детали в большей степени зависят от специфики конкретного проекта и, как правило, реализуются через параметры тестового сценария или при помощи специальных агентов тестирования.

Прогоны тестов

В силу противоречивых характеристик встроенного программного обеспечения обычно предусматривается два вида прогонов тестов.

Идеальным методом является пакетный запуск прогона тестов. Все выбранные тестовые кейсы запускаются в соответствии с матрицей покрытия аппаратного обеспечения, а результаты сохраняются в протоколе тестирования. В случае обнаружения ошибки прогон теста не останавливается, но вместо этого собирается вся возможная информация о состоянии системы в момент обнаружения дефекта (и все способы поддержки отладки в этом случае обретают важность), а тестирование продолжается по следующему тестовому кейсу. Безусловно, фреймворк поддержки тестирования должен выполнять полную очистку системы после каждого тестового сценария, чтобы избежать влияния одного сценария на другой в общем и серии неудавшихся тестов после первого сбоя в частности. Этот процесс включает в себя перезагрузку системы, обычно – перезагрузку ПО после успешно выполненного кейса тестового сценария и перезагрузку аппаратного обеспечения после сбоя.

Такие прогоны занимают длительное время, которое увеличивается за счёт очистки системы между тестами. Из-за продолжительности этих прогонов они обычно запускаются в автоматическом режиме на ночь. Такие пакетные прогоны особенно полезны при проведении smoke-тестов, а также регрессионных тестов для новых сборок.

В отдельных случаях тесты прогоняются до первого сбоя. После ошибки прогон теста останавливается, а состояние системы консервируется. Разработчик получает уведомление и возможность детально изучить состояние системы, чтобы выявить причину, вызвавшую сбой. Кроме того, можно создать автоматизированную среду тестирования, которая позволит останавливать прогон теста только при сбое в опреде-

10 главных проблем автоматизации, которые необходимо решить при тестировании встраиваемого ПО

1. Физический доступ к встроенной системе для проведения тестирования или получения результатов. Для датчиков и некоторых других аппаратных интерфейсов, возможно, потребуются особые условия доступа.

2. Возможности поддержки автоматизации тестирования в самом продукте. Перехватчики, ловушки для подключения тестовых средств или вызываемые API-интерфейсы должны быть добавлены в код продукта изначально.

3. Верификация поведения. Рекомпиляция встроенного кода на ПК часто влияет на время прогона.

4. Доступность оборудования. Проводите верификационные тесты на оригинальном оборудовании. Автоматизация на симуляторе не заменяет тестирования непосредственно на устройстве.

5. Безопасность. Любой код тестирования (или агент) во встроенной системе, в частности в выпускаемой версии, не должен оставлять возможностей для её взлома.

6. Вопросы временных характеристик. В некоторые устройства встроено ПО, зависимое от контроллеров времени.

7. Эксперты в команде. Команде нужны люди, подкованные как в технологии, так и в тестировании.

8. Автоматизация мультимедийных компонентов. Неважно, что это – воспроизведение звуков или мигание светодиодов, – всё должно быть протестировано.

9. Ограничения памяти. Бывают ситуации, когда оперативной памяти слишком мало, что вызывает сбой системы.

10 Недетерминизм тестируемой системы. Благодаря целому ряду причин (race conditions, генераторы случайных чисел, состояние системы) тестируемая система может вести себя по-разному в разные прогоны тестов, что существенно затрудняет тестовое покрытие и прохождение критериев Pass/Fail.

Источник: LogiGear

лённом тестовом кейсе (или наборе кейсов). Такие прогоны тестов полезны, когда необходимо исследовать дефекты, для которых информация, собранная в пакетном режиме, недостаточна, так что разработчику требуется доступ к системе в момент проявления дефекта для её изучения.

Виртуальная лаборатория

Методологические подходы, описанные в предыдущих разделах, позволяют построить эффективный процесс тестирования встроенного программного обеспечения. Тем не менее есть и ещё одна важная часть этого процесса – программно-аппаратный комплекс «Виртуальная лаборатория» (Virtual Laboratory или VL). Данный комплекс предоставляет средства для решения некоторых технически сложных задач, с которыми можно столкнуться во время тестирования.

Во-первых, он включает в себя базу данных существующих аппаратных модулей, каждому из которых присвоен простой строковый идентификатор. Для каждого модуля можно указать несколько признаков, таких как версия аппаратного обеспечения, идентификаторы канала связи: IP-адрес, MAC-адрес, логин и пароль к системе и т.д. Для тестового сценария это означает, что, зная идентификатор модуля, он может восстановить все остальные признаки, необходимые для коммуникации с данной платой и предоставить полноценный отчёт о дефектах.

Во-вторых, VL поддерживает работу с последовательными консолями, стойками питания (устройства, позволяющие включать и выключать питание на целевых аппаратных модулях), реле с сухими контактами. Соответствующие консоли/реле/стойки указаны для конкретных модулей в базе данных, что позволяет тестовым сценариям исполнять любые операции с конкретным модулем, зная только его имя.

В-третьих, VL обеспечивает возможности для получения исключительного доступа к совместно используемому аппаратному оборудованию. Перед подключением к консоли конкретного модуля тестовый сценарий должен сначала «заблокировать» данный модуль при помощи специальной команды. Когда модуль заблокирован, ни одна другая сущность не может «заблокировать» его. После окончания процесса тестирования тестовый сценарий «разблокирует» модуль, предоставляя возможность контроля другим участникам тестирования. Подобный механизм блокировки взаимоисключающего доступа предотвращает случайные попытки прогона тестов в одно и то же время на одной и той же плате разными сценариями или операторами.

VL предоставляет удобный для пользователя интерфейс командной строки через защищённое подключение и может использоваться как тестовыми сценариями, так и специалистами-операторами. VL – это база для выполнения всех автоматизированных и ручных тестов для целевого программного обеспечения.

Краткие выводы

Тестирование встраиваемого программного обеспечения может быть достаточно трудоёмким и сложным процессом, а дефекты – воспроизводиться с трудом. Выделив время на создание правильной тестовой среды и выстраивание надлежащего процесса тестирования, вы добьётесь наилучших результатов.

Новости рынка

Операционная система для «Интернета вещей» от ARM

(Окончание. Начало на стр. 18)

ОС mbed управляется по событиям и для передачи данных в облако поддерживает несколько коммуникационных стандартов, включая Wi-Fi, Bluetooth Smart, Thread, и версию суб-6 ГГц стандарта 6LoWPAN для работы на больших расстояниях. Поддерживается также LTE и несколько других стандартов сотовой связи.

ОС mbed занимает всего 256 Кбайт памяти (и даже менее), поэтому может устанавливаться в таких миниатюрных устройствах, как датчики. Она включает интерфейсы программирования на C++, каркас обработки событий, менеджер коммуникаций, поддержку шифрования и другие возможности.

По словам представителей ARM, бóльшая, но не вся часть кодов ОС mbed будет открытой. В принципе, портировать ОС mbed на свои чипы могли бы, при желании, такие компании, как Imagination или Intel. Однако ARM считает важным подчеркнуть, что хотя для использования в микросхемах ARM коды mbed открыты, реализация в устройствах других фирм будет платной.

Источник: http://www.pcworld.com/article/2690575/arm-builds-an-os-for-the-internet-of-things.html

Сергей Кирюхин, Алексей Ханыгин, Денис Алексеев, ЗАО «РТСофт»

Отечественная инструментальная платформа для разработки информационно-управляющих систем PLATINUM-RT

Данная статья посвящена уникальной отечественной программной инструментальной платформе PLATINUM-RT разработки ЗАО «РТСофт», предназначенной для создания автоматизированных информационно-управляющих систем на предприятиях различных отраслей.

Инструментальная платформа PLATINUM-RT представляет собой единую интегрированную программную среду, которая объединяет большое количество разнообразных служб и приложений и позволяет создавать автоматизированные системы различного назначения. Например системы сбора, хранения и предоставления данных, системы автоматизированного управления технологическими и функциональными процессами, а также информационно-аналитические системы поддержки принятия решений.

Инструментальная платформа «PLATINUM-RT» обладает следующими основными характеристиками:

- широкими возможностями масштабирования системы сбора данных – от нескольких до сотен источников данных;
- возможностями построения разнообразной высоконадёжной отказоустойчивой архитектуры для создания клиент-серверных и мультисерверных систем с использованием механизмов буферизации данных, резервирования серверов и сетевой инфраструктуры;
- простотой конфигурирования и централизованным управлением создаваемыми системами;
- единой моделью объекта автоматизированного управления и единым пространством имён элементов информационно-управляющей системы;
- совместной разработкой, удалённым развёртыванием и сопровождением программных продуктов и компонентов;
- применением шаблонных и объектно-ориентированных структур;
- высокой степенью безопасности, основанной на ролевом подходе;
- поддержкой приложений MES и SCADA, широкими возможностями коммуникации;
- современными методами анализа трендов и сбором исторических данных;
- возможностями анализа информации и генерации отчётов на базе WEB.

Функциональные компоненты инструментальной платформы PLATINUM-RT

Интегрированная среда разработки (рис.1) – комплексный набор инструментов для разработки, тестирования и развёртывания клиентских приложений в системе. В среде разработки создаются и конфигурируются объекты, которые будут интегрированы в создаваемые приложения и инфраструктуру, поддерживающую функционированию данных приложений. Среда разработки позволяет проводить импортирование новых типов объектов, проводить их конфигурирование и развёртывание на компьютерах в сетевой структуре. Организация среды разработки позволяет реализовывать корпоративный принцип проектирования приложений, то есть одновременную работу нескольких разработчиков над одним или несколькими приложениями.

Базовым системным понятием данной платформы является объект. Объекты позволяют объединять все параметры конфигурации каждого элемента системы, такие как определение каналов ввода-вывода, логика обработки (скрипты), конфигурация архивирования и алармов/событий, а также политика безопасности (контроль доступа и права на действия) и графические элементы.

Разработка шаблонов производится на базе объектов. Основное назначение шаблонов заключается в

интеграции общих конфигурационных параметров объекта определённого типа для последующего многократного использования в проекте. Введение механизма шаблонов облегчает и сокращает сроки разработки приложений. Шаблоны используются для создания других шаблонов и экземпляров.

Аналитический инструментарий (рис. 2) – набор инструментов для расчётов, контекстуализации (взаимосвязи), хранения и наглядного отображения предопределённых данных на информационных панелях в виде ключевых показателей производительности (KPI) в режиме реального времени с требуемой степенью агрегирования и детализации.

Аналитический инструментарий представляет собой промышленное решение класса EMI (Enterprise Manufacturing Intelligence), которое позволяет эффективно использовать набор программных средств для анализа данных и генерации отчётов. Данное программное обеспечение (ПО) системной платформы PLATINUM_RT обеспечивает средства по доступу к информации из многочисленных источников, как системной платформы, так и сторонних источников данных (например, MES, LIMS, ERP), форматированию, хранению и наглядному отображению данных на информационных панелях. Данный ресурс системной платформы позволяет производить, в соответствии с предопределёнными правилами, обновления данных, что даёт возможность получать информацию об основных показателях производственной деятельности предприятия – о текущем состоянии основных средств предприятия, качества продукции и объём её выпуска, наличия трудовых ресурсов, материальных запасов и энергопотребления.

Результаты анализа могут быть представлены (опубликованы) на информационных панелях, а также на web-портале.

Генератор отчётов (рис. 3) – инструмент по разработке форм отчётности, использующий данные как платформы PLATINUM-RT, так и других источников, используя, например, OPC, ODBC, CSV, MS Excel, Modbus, BACnet, SNMP, OLEDB. Отчёты могут содержать текст, таблицы данных, круговые диаграммы, линейчатые диаграммы, секторные диаграммы, гистограммы, графики и другие виды представления информации.

Данный компонент/сервер включает такие средства проектирования, как «мастер быстрой генерации проектов», примеры виртуальных отчётов, встроенные и готовые к использованию шаблоны отчётов. Сервер предоставляет возможность формирования/разработки интерактивных web-отчётов с использованием встроенных фильтров, ручного ввода данных и управления данными.

Генератор отчётов представляет возможность распространения отчётов через Интернет/интранет посредством web-портала.

Сервер приложений (рис. 4) – один из базовых компонентов системы, исполняющий одно или несколько приложений в соответствии с заданной конфигурацией системы. Сервер приложения – основа

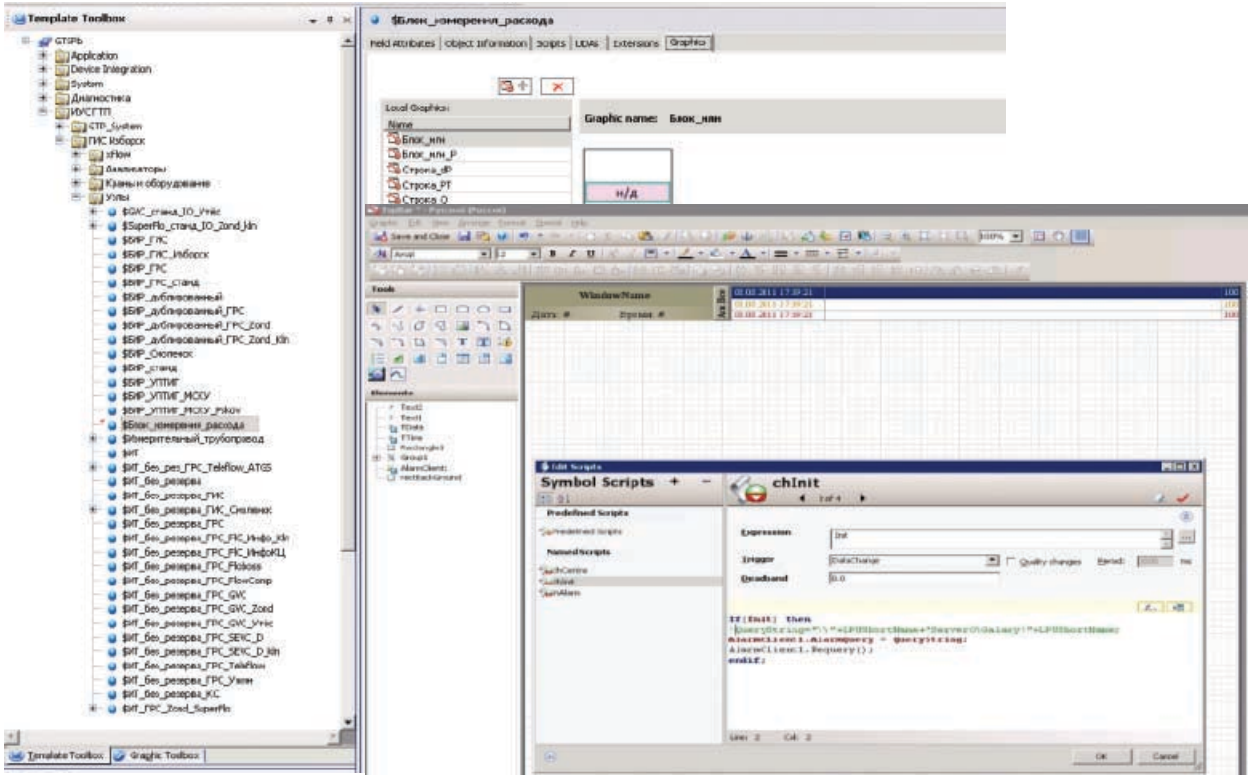


Рис. 1. Интегрированная среда разработки

любой распределённой системы, разработанной на основе платформы PLATINUM-RT. Сервер приложений обеспечивает инфраструктуру для работы приложений систем уровня DCS и решения задач уровня MES. Он обеспечивает взаимодействие и совместную работу различных подсистем, интегрирует, обрабатывает и предоставляет данные для различных пользователей.

Сервер приложений может использоваться при разработки больших, территориально распределённых систем. Сервер приложений обеспечивает возможность работы в неустойчивых сетях и в сетях с ограниченной пропускной способностью за счёт механизмов буферизации и сжатия данных.

Сервер приложений может решать следующие задачи:

- обеспечение единой инфраструктуры для работы приложений;
- обеспечение протоколов обмена данными между узлами в системе;
- поддержание иерархической модели предприятия;
- генерация алармов;
- регистрация событий, действий операторов и других пользователей;
- конфигурирование и запись архивных данных в сервер событий;
- исполнение сценариев .NET.

Рис. 2. Аналитический инструментарий

Сервер приложений предоставляет развитой инструментарий для разработчиков сложных систем. К данным инструментам можно отнести:

– объектный подход к разработке приложения;
– централизованное управление проектом, ведение журнала внесённых изменений, управление правами доступа разработчиков;
– обеспечение одновременной совместной работы нескольких разработчиков над проектом;
– единая расширяемая библиотека графических элементов и мнемосхем;
– единая библиотека шаблонов объектов;
– доступ к библиотекам, разработанным на .NET;
– разработка и развёртывание приложений с использованием библиотеки графических символов, а также отслеживание изменений и обновление установленных приложений «на лету».

Сервер событий (архив данных) (рис. 5) – это высокопроизводительная реляционная база данных реального времени для регистрации и хранения информации о функционировании объектов.

Основные функции данного сервера:

– сбор производственной информации от серверов ввода-вывода, операторских приложений, серверов приложений и других устройств;
– сжатие и сохранение данных;
– предоставление производственной информации в соответствии с запросами.

Сервер событий содержит информацию о системных событиях, сводках, конфигурациях, системе безопасности, резервном копировании и системном мониторинге. Данные записываются в сжатом виде и хранятся в хронологическом порядке. Сервер событий получает и записывает данные как с полной, так

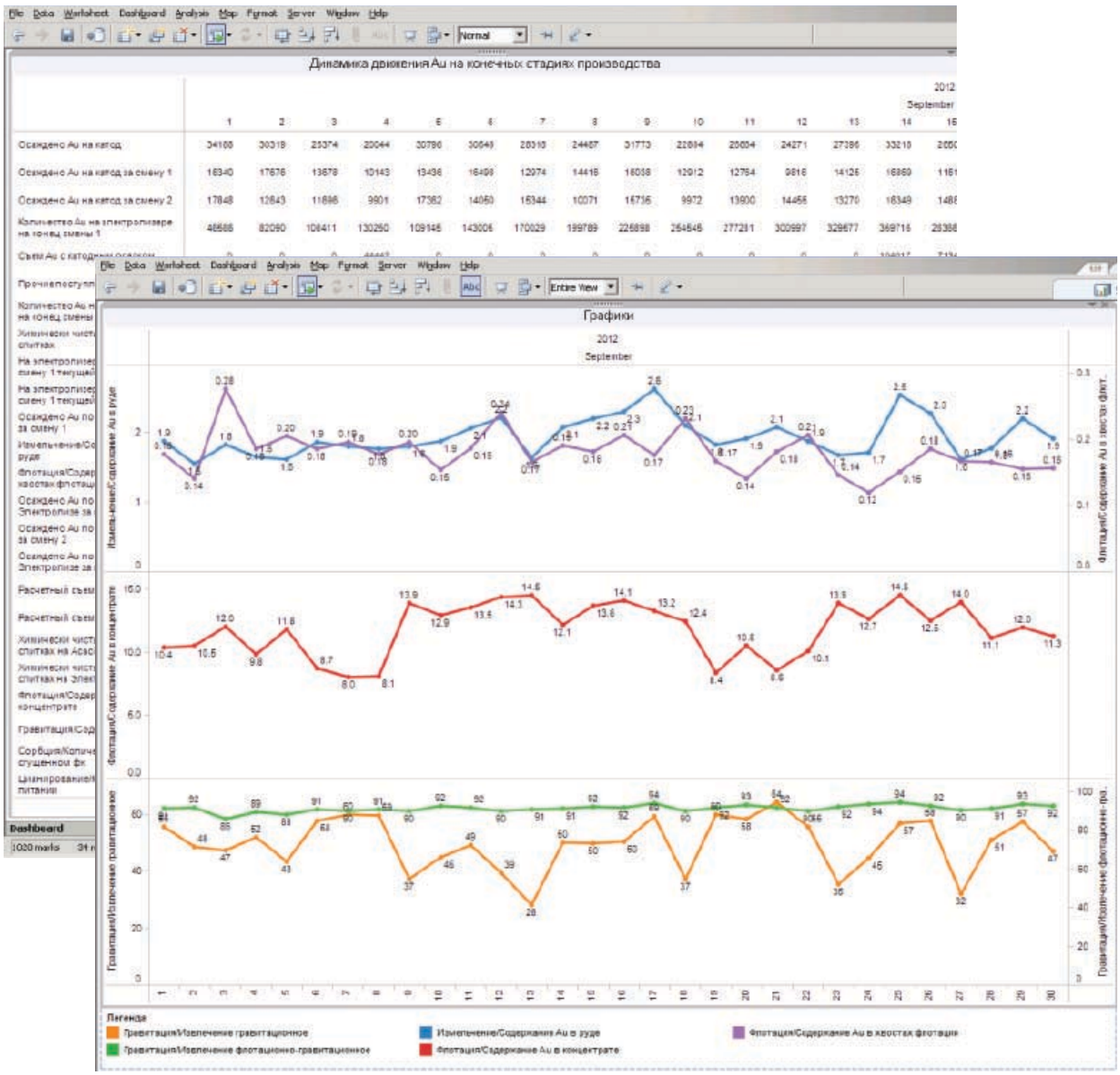


Рис. 3. Генератор отчётов

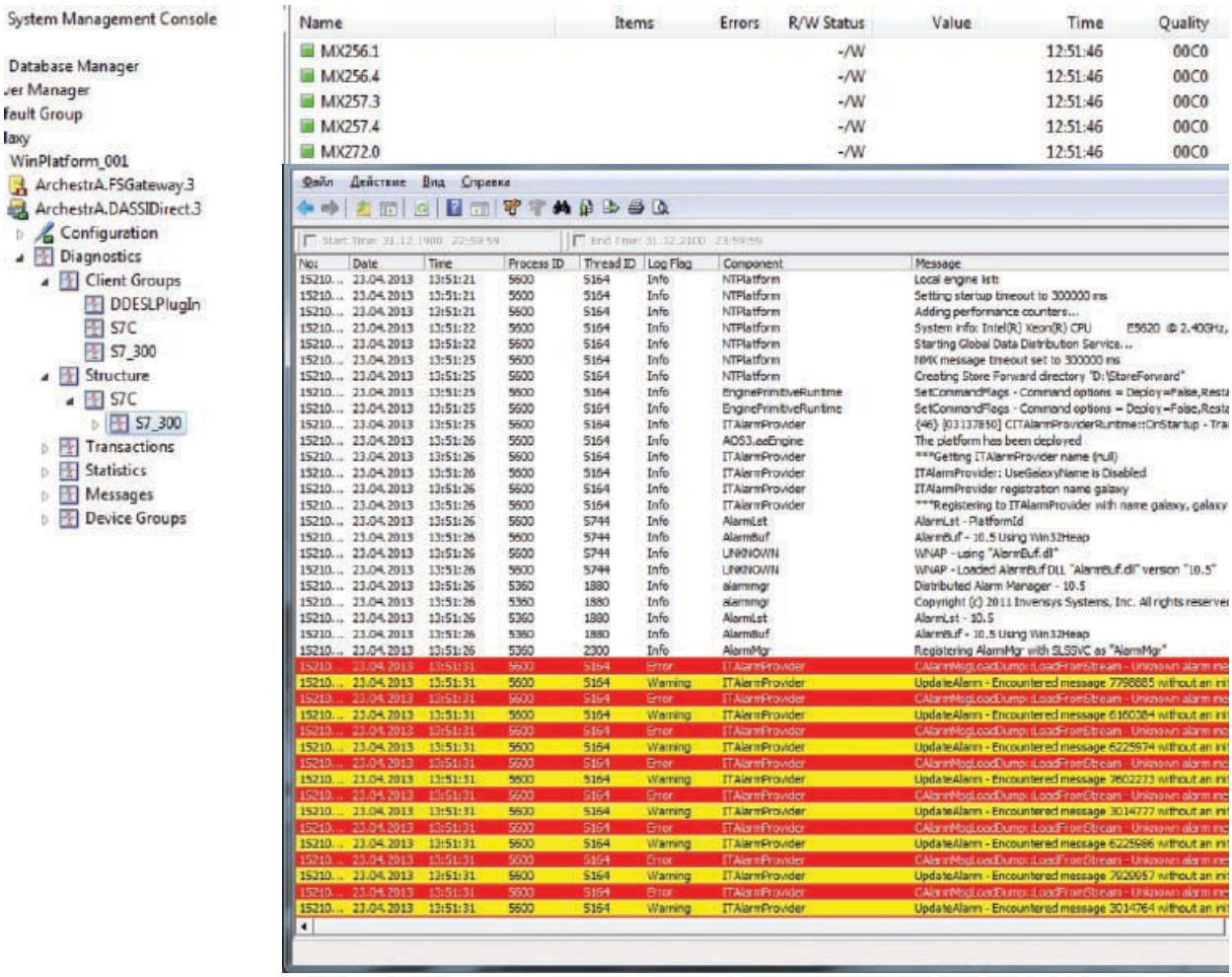


Рис. 4. Сервер приложений

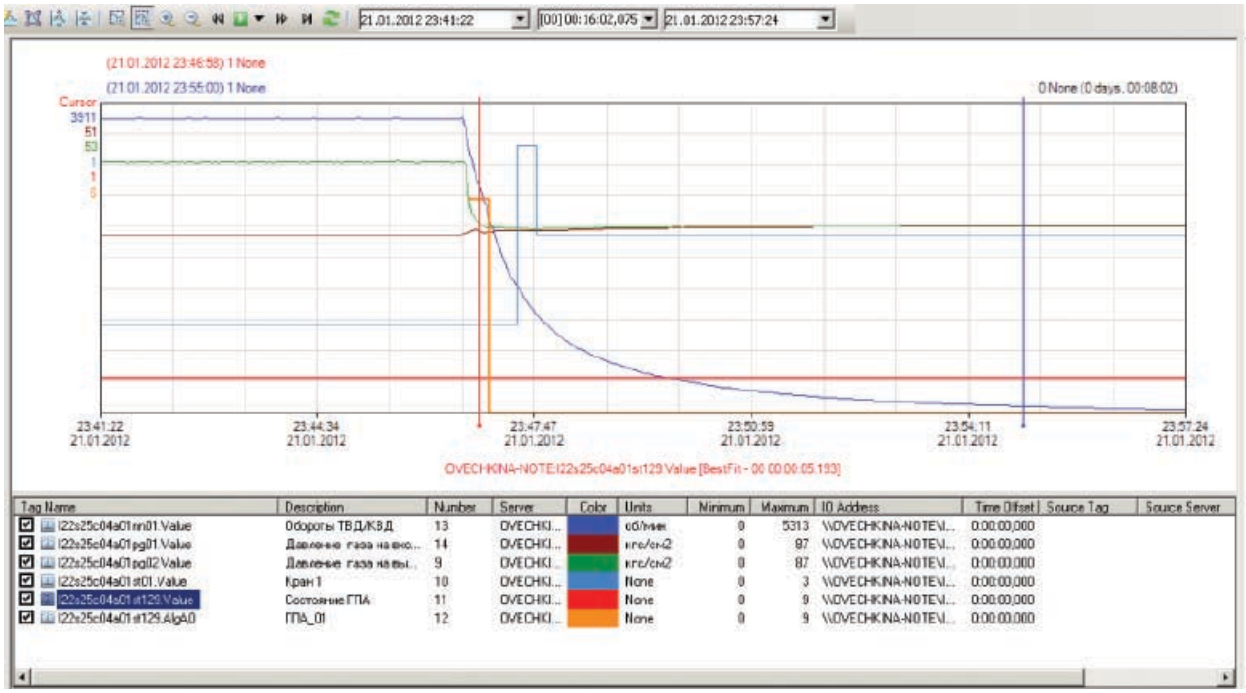


Рис. 5. Сервер событий (архив данных)

и с заданной разрешающей способностью и предоставляет клиентским приложениям оперативную и архивную информацию вместе с информацией о конфигурации, событиях и другими производственными данными.

Конфигурационный сервер (рис. 6) – реализует функции по формированию единой объектной модели, общего пространства имён, функции по объектному управлению, диспетчеризации приложений, распределению вычислительных мощностей, управлению разработкой и модификацией приложений.

Конфигурационный сервер предоставляет следующие возможности:

- формирование единой платформы описания структуры объектов управления;
- формирование свойств объектов в контекстах различных систем (проектная документация, система сбора данных, SCADA-системы);
- создание алгоритмов автоматического формирования иерархического имени тега по структуре родительских объектов;
- возможность задания горизонтальных связей между иерархиями объектов;
- генерация любых конфигурационных файлов.

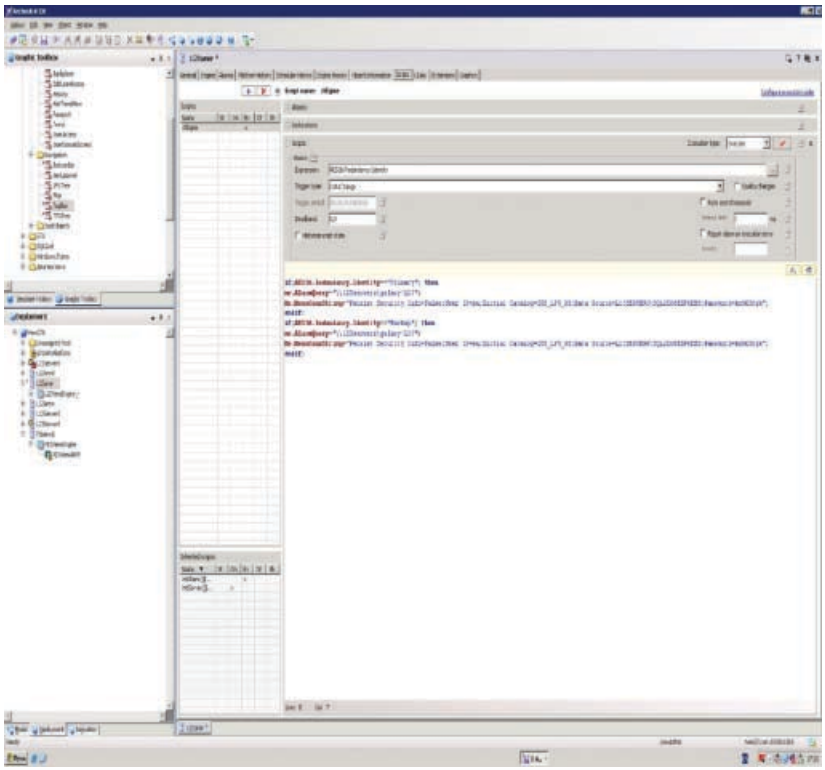


Рис. 6. Конфигурационный сервер

Информационный сервер (рис. 7) – реализует функции представления информации (графики, тренды и отчётность) на основании данных как платформы PLATINUM-RT, так и внешних источников данных. Базовая функциональность доступна посредством web-страницы.

Информационный сервер обеспечивает просмотр всей информации предприятия через Интернет или внутреннюю сеть предприятия. С помощью Internet Explorer

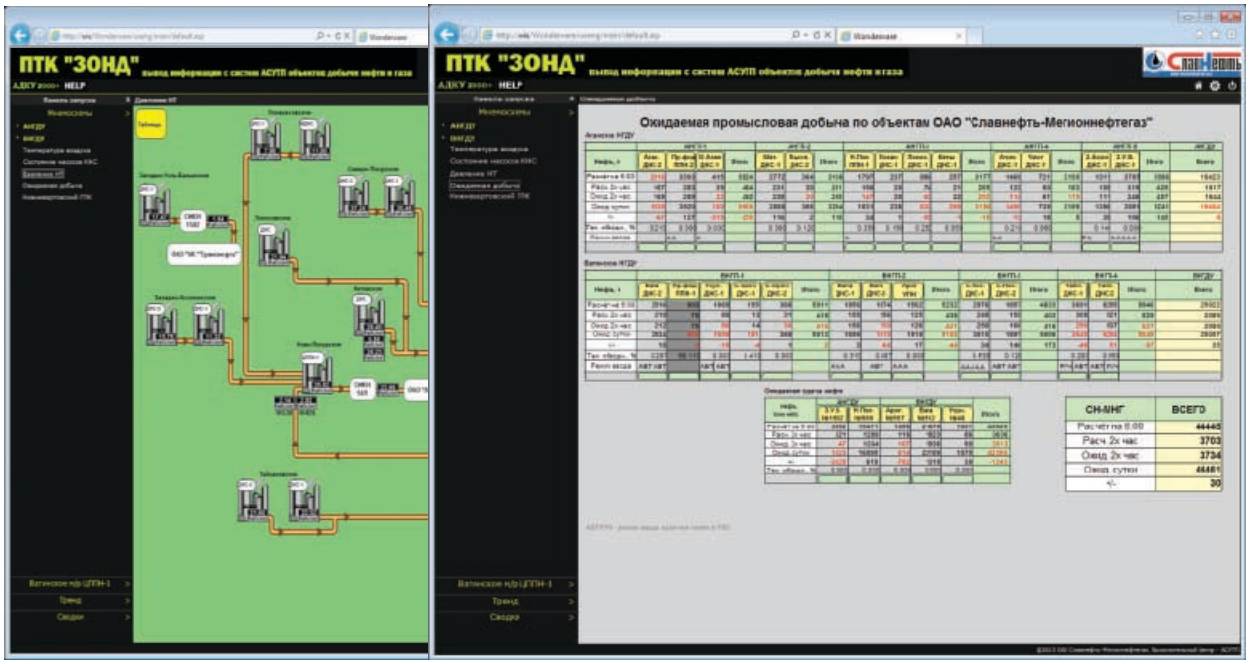


Рис. 7. Информационный сервер

информационный сервер может предоставлять различные сведения от множества источников данных, в частности отчёты, документы, данные аварийных сигналов, хронологические данные и данные в реальном времени.

Информационный сервер предоставляет следующие возможности/средства:

– web-изображения, содержащие web-контент, например страницы HTML или код расширяемого языка разметки (XML – Extensible Markup Language). Этот контент хранится в легкодоступных, многократно используемых компонентах;
– панели доступа, представляющие собой логическую группу узлов (папок) навигации и ссылок, доступную только конкретным пользователям, назначенным этой группе;
– инструментарий, обеспечивающий широкие возможности формирования отчётов на основании данных сервера событий. Отчёты формируются на основе Microsoft SQL Server Reporting Services (SSRS). Эта функция позволяет создавать, развёртывать и генерировать отчёты SSRS в информационном сервере.

Интеграционный сервер (рис. 8) – реализует функции по интеграции приложений платформы PLATINUM-RT с программным обеспечением сторонних поставщиков (ERP, PLM и т. д.).

Интеграционный сервер позволяет устанавливать связь с любой бизнес-системой или дополнительным приложением от стороннего поставщика. Благодаря этому реализуется единый согласованный подход к интеграции различных производственных площадок с центром планирования и управления производственной деятельности предприятия, позволяющий отказаться от разрозненных массивов информации и требующей большого объёма обслуживания двухточечной интеграции, а также сократить затраты на обслуживание IT-систем.

Интеграционный сервер обеспечивает поддержку основных отраслевых стандартов доставки сообщений, включая web-службы, File Drop, FTP, MSMQ, XML, HTTP и SOAP, поддержку определений сообщений B2MML на основе стандартов ISA-S95 и репозиторий сообщений на базе Microsoft SQL Server.

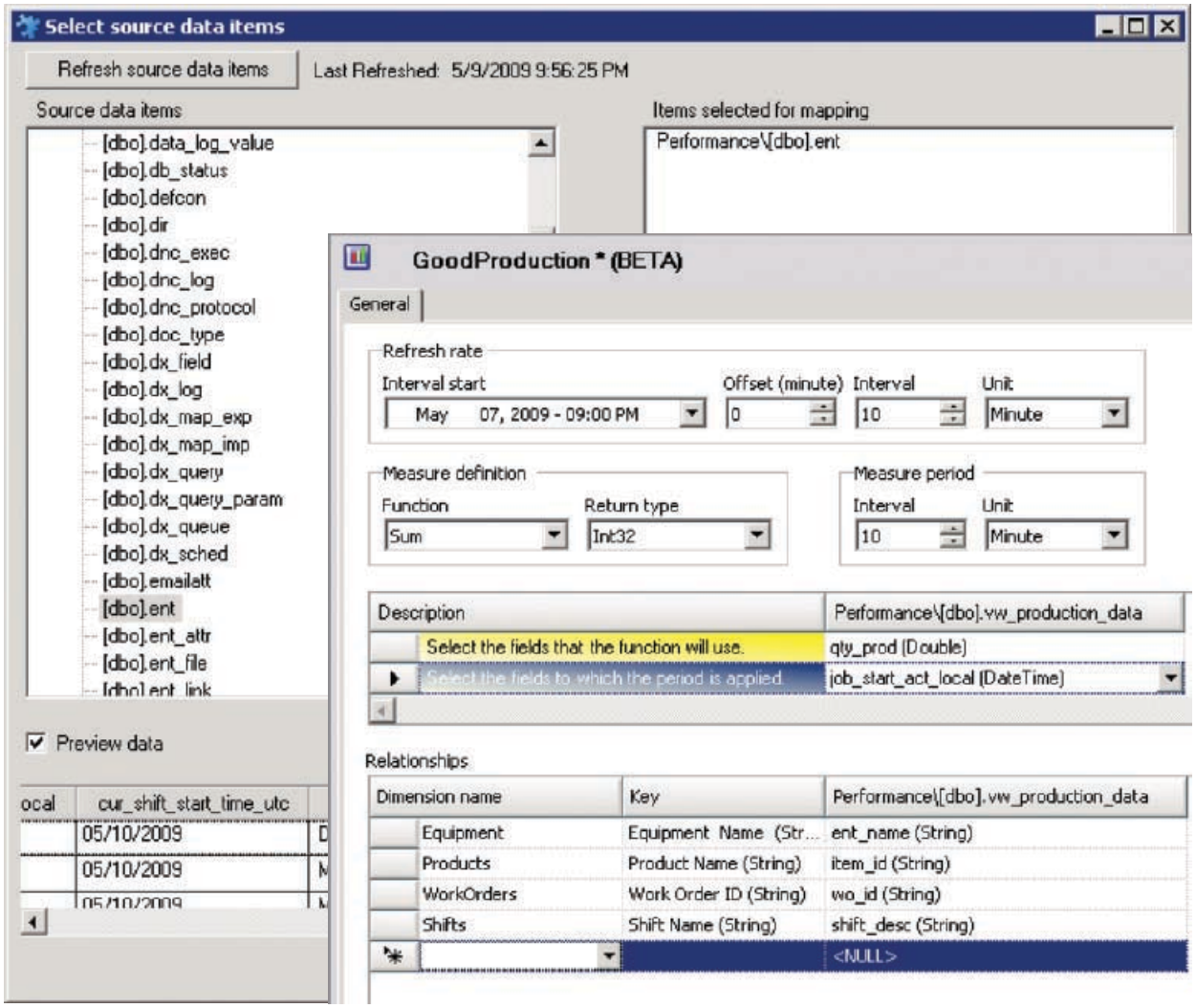


Рис. 8. Интеграционный сервер

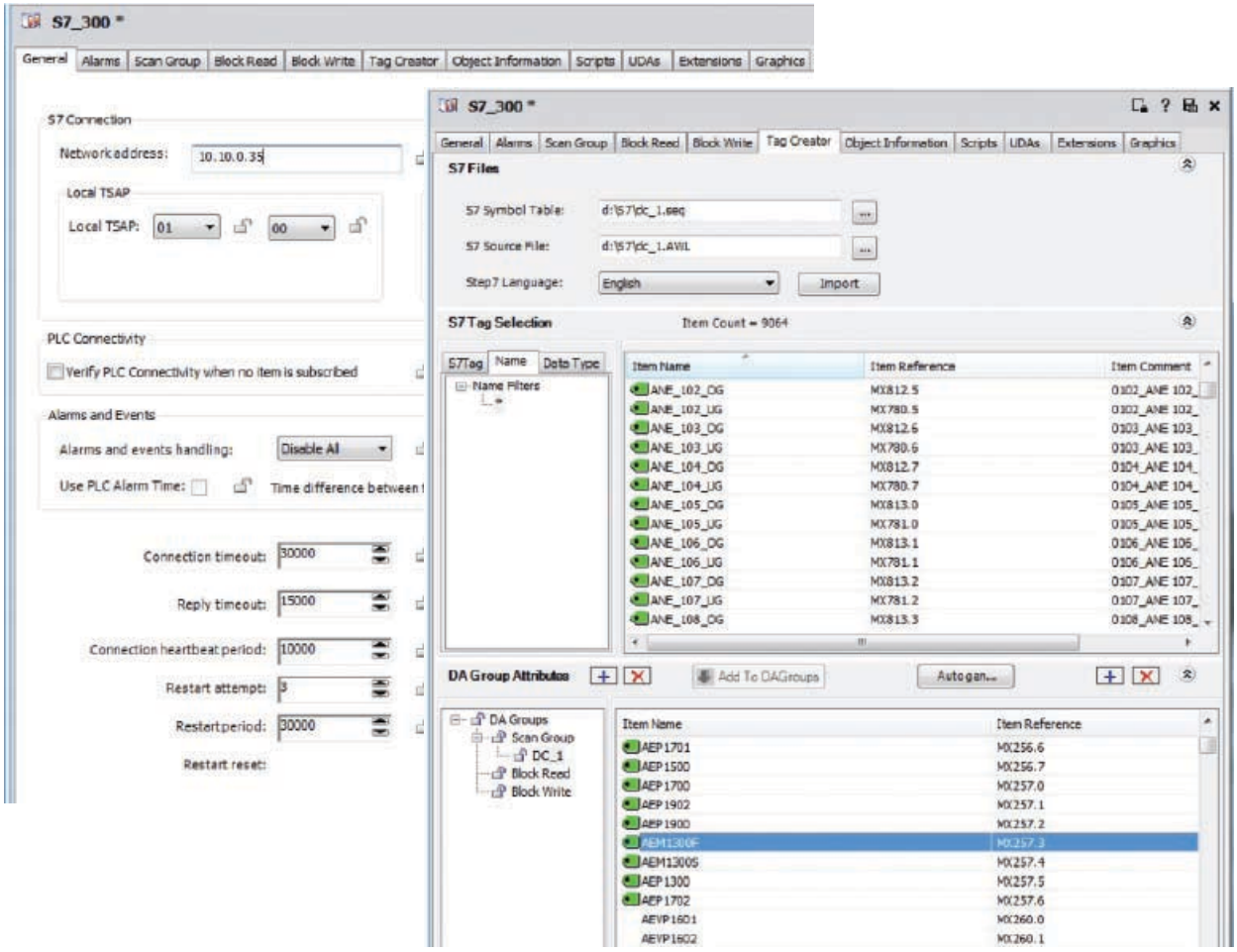


Рис. 9. Коммуникационный сервер

Интеграционный сервер позволяет осуществлять ввод данных формата Excel/XML и экспорт данных в форматах Excel, HTML, PDF для последующего построения отчётов на основании технологических данных.

Коммуникационный сервер (рис. 9) – реализует функции обмена данными с внешними источниками данных в соответствии с требованиями стандартных промышленных протоколов или посредством разработанных специализированных драйверов для поддержки внешних устройств.

Коммуникационный сервер обеспечивает сбор данных с источников по следующим протоколам:

– обмен данными по стандартным протоколам: OPC, SuiteLink, IEC 60870-5-10X, modbus, profibus, HART, DF1, SNMP и др.;
– обмен данными по специальным протоколам: СЭТ 4ТМ, СЭБ, Меркурий, CE 301, CE 303; МКТС, СПТ961, Ирга-2, Ирга-2.3, Взлёт ТСРВ, Взлёт ТСР-М, Взлёт МР УРСВ, СПГ-763, Гиперфлоу, Суперфлоу, ВКТ 7.

В качестве физической среды передачи данных могут использоваться следующие интерфейсы: RS 232/485, PLC, Ethernet, GSM, GPRS, радиомодем 433МГц.

Коммуникационный сервер поддерживают спецификации OPC Data Access 2.0/3.0, OPC UA и предлагают ряд дополнительных преимуществ помимо стандартных, включая возможности удалённого конфигурирования и управления сервером, а также эффективную диагностику при поиске неисправностей.

Сервер диагностики (рис. 10) – набор инструментов, позволяющих проводить диагностику компонентов платформы, состояния активных приложений, каналов подключения источников данных и информационного обмена с внешними устройствами (источниками данных), протоколирование исключительных ситуаций и событий, агрегирование данных, анализ причин возникновения нештатных ситуаций, визуализацию текущего состояния компонентов систем автоматизации, предоставление информации об отказах и результатов аналитических расчётов по наработкам этих компонентов.

Сервер диагностики поддерживает реализацию диагностических моделей как локальных, так и функционально и территориально распределённых интегрированных автоматизированных систем.

В качестве объекта контроля могут быть программно-аппаратные компоненты систем автоматизации, включая серверы, устройства преобразования протоколов передачи данных, источники бесперебойного

питания, рабочие станции и коммуникационное оборудование.

Сервер безопасности (рис. 11) – набор инструментов, позволяющих реализовывать политику безопасности, основанную на формировании групп безопасности для объектов приложений, создании ролей для пользователей с присвоением им соответствующих прав.

В платформе PLATINUM-RT каждое приложение осуществляет управление своей собственной моделью безопасности. Схема безопасности представляет собой трёхуровневую модель конфигурации для создания и поддержания:

– пользователей, связанных с конкретными ролями;
– пользовательских ролей, связанных с конкретными системными полномочиями администрирования, конфигурирования и оперативного управления, которые предоставляются группам безопасности;
– групп безопасности, связанных с определёнными объектами.

В системе безопасности сервера предусмотрены три режима аутентификации.

– **Уровень приложения:** для аутентификации пользователей используется конфигурация локального приложения.
– **Уровень пользователя операционной системы (ОС)** – все параметры безопасности приложения устанавливаются и содержатся в ОС на уровне пользователя.
– **Уровень группы пользователей ОС** – используется система аутентификации пользователя операционной системы на основе группы. Все параметры безопасности приложения устанавливаются и содержатся на созданной в ОС карте соответствия пользователей и ролей для назначения безопасности.

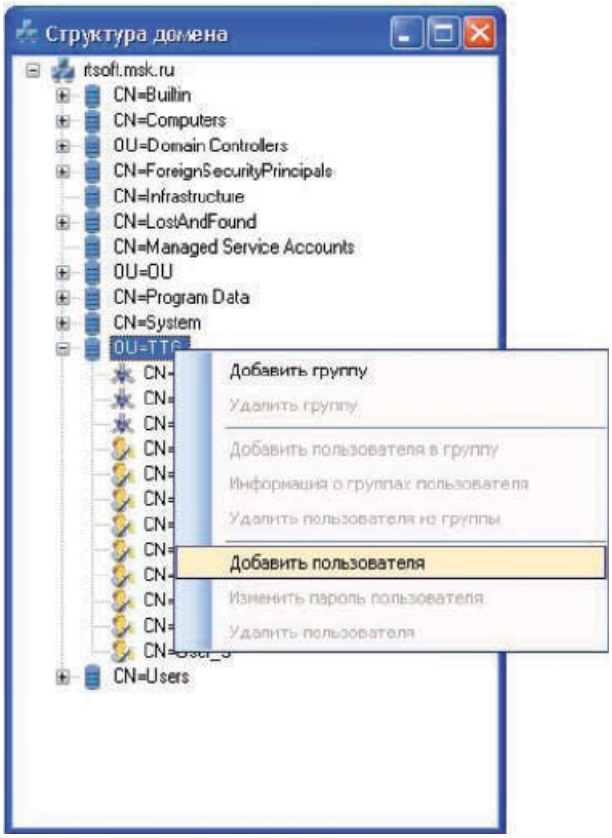


Рис. 11. Сервер безопасности

Доступ к информационному серверу обеспечивается посредством тесной интеграции со средствами безопасности Microsoft Windows (Kerberos), представляемый операционной системой Microsoft Windows Server, и механизмами защиты, используемыми Internet Information Services (IIS).

Для дополнительной защиты программное обеспечение сервера безопасности поддерживает также протокол защищённых сокетов (SSL – Secure Sockets Layer), аутентификацию по паролю, цифровые сертификаты и диалоговые окна входа в систему Windows. Для использования цифровых сертификатов необходимо установить цифровой сертификат сервера, выданный сторонней компанией.

В сервере безопасности имеется компонент фильтрации списка пользователей Active Directory по групповой принадлежности. Данный компонент реализован в виде DLL с поддержкой графического интерфейса.

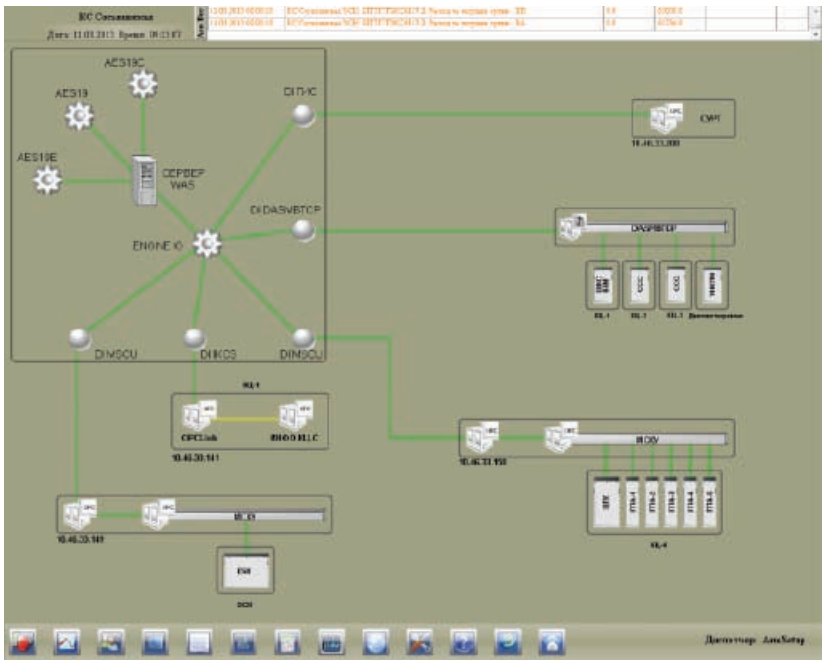


Рис. 10. Сервер диагностики

Специализированные приложения и компоненты – набор дополнительных программных модулей, расширяющих возможности платформы при реализации систем автоматизации, имеющих специфические особенности применения.

К специализированным программным компонентам относятся:

1. Модуль интеграции с геоинформационной системой (ГИС) (рис. 12).

Данный модуль реализован в виде .Net Control с конфигурационной базой данных и обеспечивает визуализацию состояния объектов контроля на картографической топооснове. Модуль даёт возможность проводить масштабирование, выделение и просмотр свойств объектов, индикацию с учётом текущего состояния. Отображение осуществляется средствами ГИС, в качестве которых могут использоваться следующие системы: ArcGis, MapInfo, GRASS.

2. Модуль параметрической диагностики (рис. 13) на основе статистических методов обработки данных.

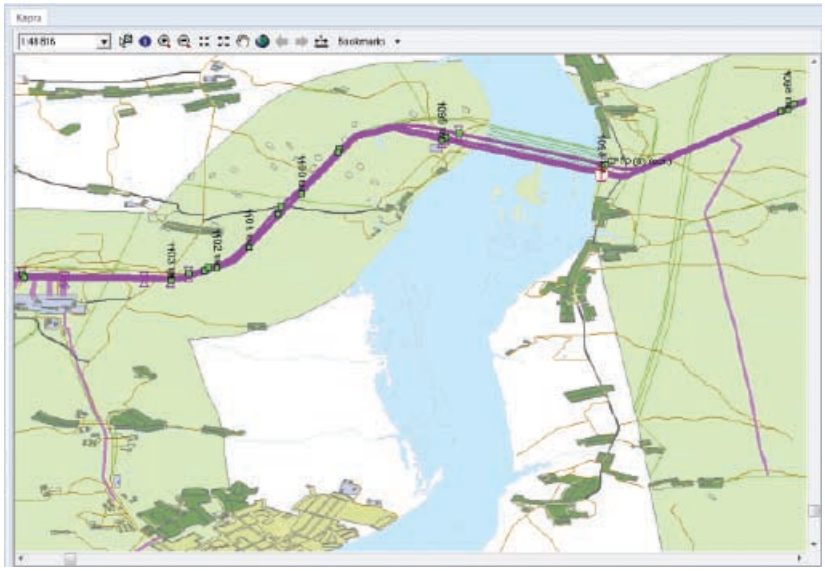


Рис. 12. Модуль интеграции с ГИС

Рис. 13. Модуль параметрической диагностики

Данный модуль реализован в виде сервиса с локальной базой данных и предназначен для мониторинга параметров функционирования оборудования с целью выявления отклонений, которые могут привести к отказу. Контроль осуществляется на основе обработки оперативных технологических параметров с использованием методов имитационного моделирования по пространственному контексту. Алгоритм обработки строится на сравнении реальных значений с данными, характерными для предопределённой модели.

3. Модуль представления иерархического дерева объектов производственной модели. Данный модуль реализован в виде DLL с поддержкой графического интерфейса, который обеспечивает более удобный/расширенный инструментарий работы с объектами, например создание специализированного интерфейса навигации по объектам контроля, созданного на базе дерева объектов в соответствии со сконфигурированной производственной моделью с преопределёнными уровнями детализации.

4. Модуль оповещения об алармах с рассылкой SMS-сообщений. Данный модуль реализован в виде программы, которая обеспечивает сканирование текущего состояния алармов и рассылку сообщений для заданного списка пользователей.

5. Модуль конвертации схем Autocad. Данный модуль реализован в виде DLL и обеспечивает конвертацию схем Autocad в формат XAML для возможности встраивания в приложения, реализуемые на WPF для визуализации мнемосхем.

К специализированным компонентам относятся графические библиотеки, представляющие набор графических символов и шаблонов для типовых элементов управления технологическими процессами в следующих отраслях промышленности:

– инженерные системы зданий и сооружений;
– транспортировка газа;
– технические средства общеобъектных систем и энергетических установок;
– комплексы переработки жидких и твёрдых радиоактивных отходов.

(окончание в следующем номере журнала)

Константин Утешев, ЗАО «РТСофт»

Автоматический подсчёт пассажиров общественного транспорта

Основные технические требования и подходы к реализации

Приводятся основные технические требования к системам подсчёта пассажиров общественного транспорта, обсуждаются имеющиеся на рынке технические решения и варианты реализации, их достоинства и недостатки.

Назначение систем подсчёта пассажиров и решаемые ими задачи

Системы подсчёта пассажиров предназначены для получения информации о реальном количестве перевезённых пассажиров, востребованности маршрутов общественного транспорта, загруженности подвижного состава в интересующие интервалы времени и последующего анализа пассажиропотоков.

На современном этапе развития техники трудоёмкий ручной подсчёт пассажиров может быть заменён специализированными Автоматическими Системами Подсчёта Пассажиров (АСПП), обеспечивающими требуемую точность и объективность получаемых данных.

Принятые подходы к реализации АСПП позволяют практически без дополнительных финансовых затрат реализовать также и контроль текущего состояния каждой единицы подвижного состава (местонахождение, факты отклонения от расписания и маршрута движения, данные о работе и состоянии основных агрегатов, температура воздуха в салоне и т. п.).

Таким образом, современные АСПП позволят специалистам транспортных предприятий:

- планировать/оптимизировать маршрутную сеть и график движения подвижного состава для каждого маршрута с учётом дней недели, сезонности и других факторов;
- выявлять безбилетников и «скрытых безбилетников» (пассажиры, следующие дальше зон, оплаченных при покупке билетов);
- планировать режимы работы и нагрузку касс, разъездных кассиров и контролёров;
- получать информацию о соблюдении расписания движения каждой единицы подвижного состава;
- контролировать текущее местоположение всех единиц подвижного состава и факты отклонения от маршрута;
- объективно и оперативно реагировать на жалобы пассажиров касательно соответствия температуры воздуха в салоне требованиям санитарных норм;
- получать объективную информацию о пробеге и о работе основных подсистем подвижного состава (для планирования ремонтов и технического обслуживания).

Типовая структура и принцип работы АСПП

Несмотря на различные физические принципы реализации подсчёта пассажиров и конструктивные особенности систем от разных производителей, структура АСПП достаточно типовая (рис. 1).

В состав АСПП входят следующие компоненты:

– **устанавливаемые на подвижном составе:**

–– датчики и первичные средства измерения:

––– датчики подсчёта пассажиров;

––– датчики контроля положения дверей вагона;

––– датчики контроля состояния подвижного состава (при необходимости); например датчики температуры воздуха в салоне;

–– контроллер сбора и передачи данных, оснащённый:

––– модулем контроля текущего положения подвижного состава (GPS/ГЛОНАСС);

––– модулем передачи данных (GSM/GPRS) на сервер АСПП;
––– дискретным и/или аналоговым вводом-выводом (при необходимости);
––– промышленными сетями для сбора данных с интеллектуальных датчиков и интеграции с бортовыми системами подвижного состава (при необходимости);
–– антенна GSM/GPRS + GPS/ГЛОНАСС;

– **устанавливаемые в офисе транспортного предприятия:**
–– сервер;
–– автоматизированные рабочие места (АРМ) специалистов и руководителей транспортного предприятия.

Как правило, система работает следующим образом. У каждой двери подвижного состава размещаются датчики, фиксирующие факт прохода пассажира. Совокупность аппаратных и алгоритмических решений, применённых в АСПП, позволяет различать отдельных пассажиров в потоке людей, а также отличать реальный проход пассажира от скопления людей в тамбуре при плотном заполнении вагона пассажирами. Необходимое количество датчиков определяется с учётом ширины дверного проёма (для обеспечения гарантированного перекрытия дверного проёма зонами покрытия датчиков).

Подсчёт пассажиров начинается с момента остановки подвижного состава (фиксируется GPS/ГЛОНАСС-приёмником) и открытия дверей (контролируется по срабатыванию конечного выключателя соответствующей двери). После закрытия дверей подсчёт пассажиров на данной остановке прекращается. Контроллер АСПП обрабатывает данные со всех датчиков и отправляет собранную информацию на сервер АСПП по каналу GSM/GPRS.

На сервере Системы производится сопоставление GPS-координат собранных данных с координатами остановок на маршруте, привязка данных к конкретной остановке и их архивное хранение. Визуализация накопленной информации и предоставление требуемой отчётности обеспечивается на экранах АРМ специалистов и руководителей транспортного предприятия.

Основные требования к АСПП

С учётом особенностей эксплуатации электронных компонентов на подвижном составе к современным системам АСПП предъявляются следующие требования:

– **к функциональным характеристикам:**
–– точность подсчёта пассажиров – не менее 95 %;
–– буферизация накапливаемой информации при пропадании связи GSM/GPRS (например, в случае выхода транспортного средства за пределы зоны покрытия GSM/GPRS);
–– автоматическое возобновление передачи данных при восстановлении связи;
–– наличие аппаратного сторожевого таймера;

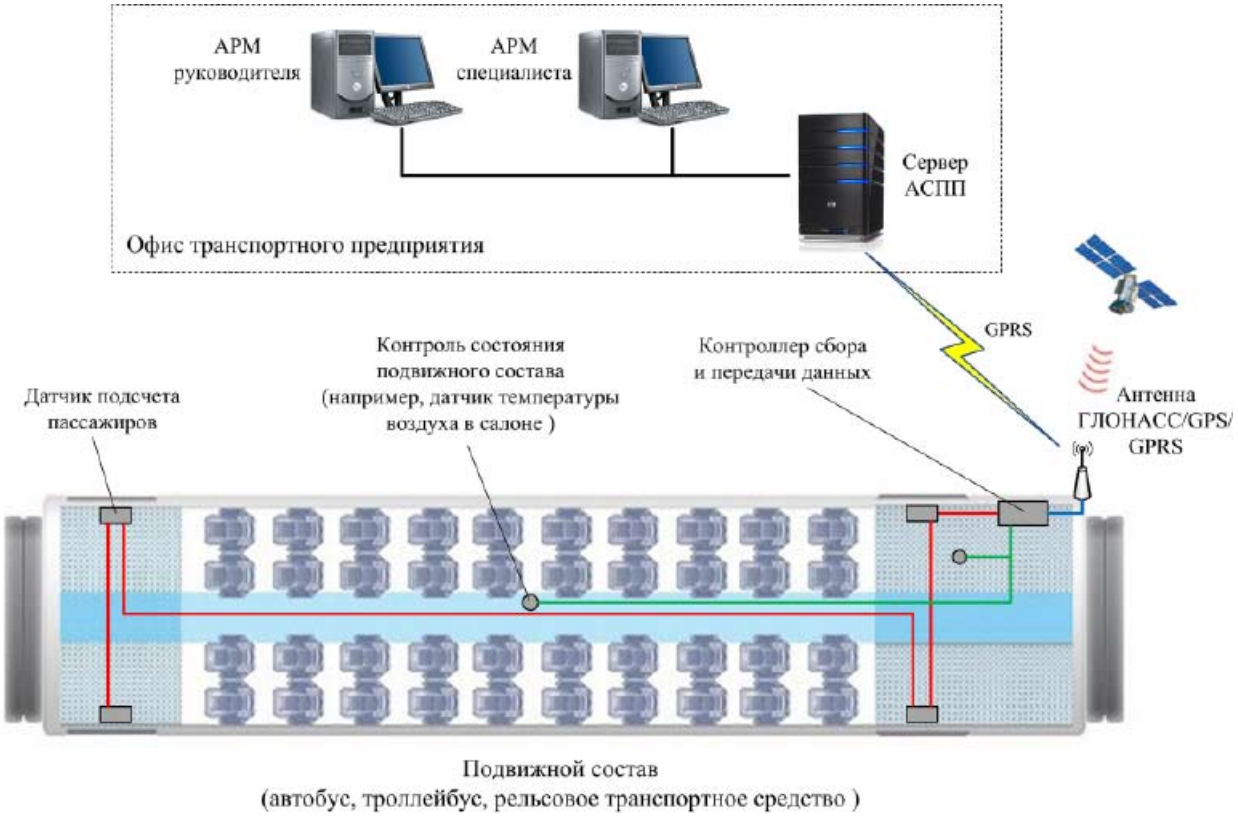


Рис. 1. Типовая структура АСПП

–– автоматический рестарт при пропадании и последующем восстановлении электропитания;
–– сохранность собранных данных и конфигурационной информации при пропадании электропитания;
–– возможность удалённой диагностики и контроля работоспособности оборудования;
–– срок службы – не менее 10 лет;

– к условиям эксплуатации:

–– температура окружающей среды от –40 до + 70°С;
–– работа в условиях высокой влажности, вибраций, наличия электромагнитных помех;

– к электропитанию:

–– электропитание должно осуществляться от штатной электросети подвижного состава;
–– небольшое энергопотребление;

– к конструктивному исполнению:

–– промышленное антивандальное исполнение;
–– компактность;
–– эстетичность/незаметность;
–– пассивное охлаждение;
–– соблюдение жёстких требований по электро- и пожаробезопасности;
–– смонтированные компоненты АСПП не должны преграждать доступ к штатному оборудованию подвижного состава (для выполнения ремонтов и технического обслуживания).

Варианты реализации и имеющиеся технические решения

Функциональность, эксплуатационные характеристики и стоимость систем АСПП определяются двумя основными компонентами:

– датчиками, обеспечивающими непосредственный подсчёт пассажиров;
– контроллером, выполняющим обработку и передачу данных на сервер системы АСПП.

Датчики подсчёта пассажиров

С точки зрения физических принципов работы можно выделить следующие типы датчиков подсчёта пассажиров.

а) Датчики подсчёта пассажиров типа «чувствительная ступенька» (рис. 2).

Датчик выполнен в виде ступеньки и устанавливается около двери транспортного средства под резиновое покрытие пола. Датчик срабатывает по каждому факту нажатия. Специальный алгоритм обработки сигналов от данных датчиков, основанный на анализе временной задержки, позволяет отслеживать ситуации, когда один и тот же пассажир встал на ступеньку двумя ногами или топтался на ней.

Достоинства:

– относительно невысокая стоимость.

Недостатки:

– относительно небольшой срок службы в связи с особенностями установки и контактным принципом работы;
– необходимость установки нескольких датчиков для широких дверных проёмов, что удорожает решение;
– невозможность определения направления движения пассажира (на вход или на выход);
– ориентированы на подсчёт общего количества перевезённых пассажиров за большой интервал времени (без возможности подсчёта вошедших/вышедших пассажиров на каждой остановке).

б) Инфракрасные датчики, работающие по принципу прерывания или отражения луча (рис. 3).

Простейшие версии датчиков данного типа формируют луч, пересекающий пространство дверного проёма в горизонтальной плоскости. Датчик срабатывает по каждому факту прерывания луча. Более развитые модели имеют два луча, контроль очерёдности прерывания которых позволяет отслеживать не только факт прохода, но и направление движение пассажира (на вход или на выход).

Наиболее совершенные датчики данного типа устанавливаются над дверным проёмом вагона, излучают и фиксируют отражённые пассажирами сигналы. Анализ полученной всеми датчиками одной двери информации производится в специализированном внешнем вычислителе (контроллере) по достаточно сложным и закрытым для пользователя алгоритмам. В частности, определяется направление

Рис. 2. Датчики подсчёта пассажиров типа «чувствительная ступенька»

Рис. 3. Инфракрасные датчики, работающие по принципу прерывания или отражения луча

движения пассажира, исключаются ситуации двойного подсчёта одного и того же пассажира, попавшего в зону покрытия двух смежных датчиков одной двери, обрабатываются ситуации повторного пересечения пассажиром луча датчика при подъёме или спуске по ступенькам транспортного средства.

Встречаются также комбинированные устройства, состоящие из согласованных между собой активных и пассивных инфракрасных датчиков.

Достоинства:
- потенциально, самое доступное по цене решение;
- компактность, простота установки;
- получение информации о числе как вошедших, так и вышедших пассажиров на каждой остановке.

Недостатки:
- необходимость установки нескольких датчиков для широких дверных проёмов, что удорожает решение;
- в сложных ситуациях (при проходе пассажиров по диагонали дверного проёма, вдоль ступенек, при высовывании пассажира из двери, при движении пассажиров с габаритным багажом и т. д.) точность подсчёта падает;
- возможность блокировки луча датчика статичным объектом (например, стоящим в проходе пассажиром);
- для обработки информации требуется внешний специализированный вычислитель с, как правило, закрытым для пользователя программно-алгоритмическим обеспечением.

а) Единые массивы (матрицы) инфракрасных датчиков (рис. 4).

в) Несмотря на схожий базовый принцип работы (излучение и контроль отражённого инфракрасного сигнала) датчики данного типа принципиально отличаются от описанных выше. Ключевым элементом датчика является матрица из нескольких сотен чувствительных элементов, на основе обработки сигналов от которых непосредственно в датчике (без необходимости применения внешнего вычислителя) формируется 3D-профиль объектов (пассажиров) в контролируемой области.

Высота отдельных точек объекта вычисляется на основе измерения промежутка времени, в течение которого инфракрасное излучение от передатчика, отразившись от объекта, было зафиксировано каждым из чувствительных элементов приёмника.

Дальнейшее отслеживание объектов позволяет зафиксировать факт и направление пересечения ими линии дверей, то есть считать входящих и выходящих из вагона пассажиров.

Достоинства:
- получение информации о числе как вошедших, так и вышедших пассажиров на каждой остановке;
- компактность, простота установки;
- обработка сигналов производится непосредственно в датчике и не требует внешнего вычислителя;
- угол обзора позволяет использовать один датчик и для широких дверей подвижного состава.

Недостатки:
- высокая стоимость (по крайней мере, на данный момент);
- из-за переотражения сигналов возможно появление «шумов» в формируемом датчиком 3D-профиле объекта, что может привести к ошибкам подсчёта пассажиров.

г) датчики на основе интеллектуальной обработки изображений с обычных или стереоскопических видеокамер (рис. 5).

Датчики данного типа представляют собой компактные компьютеры, оснащённые встроенными видеокамерами. Наиболее интересен вариант с двумя камерами (стереокамеры). На основе синхронной обработки изображений с двух камер программно-алгоритмическое обеспечение датчика строит 3D-профиль контролируемой области, выделяет объекты (пассажиров), отслеживает факт и направление пересечения объектами линии дверного проёма вагона и, таким образом, вычисляет количество пассажиров, входящих и выходящих из вагона.

Достоинства:
- потенциально, самая высокая точность подсчёта на основе обнаружения и отслеживания движения

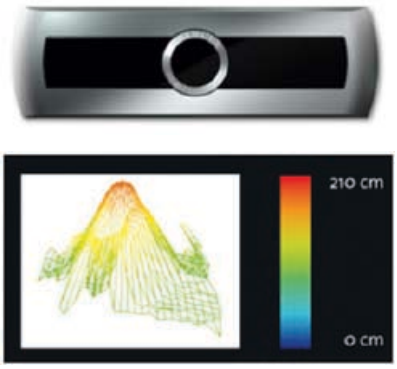


Рис. 4. Матрицы инфракрасных датчиков

Рис. 5. Стереоскопические датчики

объекта в контролируемой области (область дверного проёма);
– получение информации о числе как вошедших, так и вышедших пассажиров на каждой остановке;
– угол обзора позволяет использовать один датчик и для широких дверей подвижного состава;
– обработка сигналов производится непосредственно в датчике и не требует внешнего вычислителя;
– возможность применения алгоритмов подсчёта для нетипового поведения пассажиров и сложных ситуаций (в частности, повторное пересечение границы двери одни и тем же пассажиром, учёт высоты и формы лестниц в подвижном составе, обработка ситуации открытия дверей в контролируемой зоне и т. д.);
– удобство настройки; настройка контролируемой области и параметров работы датчика производится через web-интерфейс непосредственно на изображении, формируемом камерой датчика (имеется возможность задавать контролируемые зоны в районе двери, смещать линии подсчёта входящих/выходящих пассажиров, игнорировать статические объекты в зоне видимости датчика и т. д.);
– возможность записи и передачи по сети обычного видеоизображения с датчика для последующего анализа качества подсчёта пассажиров;
– имеются модели со встроенной инфракрасной подсветкой, позволяющей датчику работать в любых условиях освещённости.

Недостатки:
– относительно большие габаритные размеры и сложность скрытой установки;
– невозможность работы в полной темноте (нужен хотя бы минимальный источник света).

Примечание. В сети Интернет имеется также информация о датчиках, основанных на обработке сигналов от тепловизоров. В качестве недостатков данного принципа подсчёта отмечается высокая стоимость, относительно небольшой угол обзора, жёсткие ограничения на минимальную высоту установки датчика, которые не выполняются в отечественных поездах. Однако конкретные модели датчиков-тепловизоров для подсчёта пассажиров в общественном транспорте авторам данной статьи неизвестны.

Контроллер сбора и передачи данных

Можно выделить два класса контроллеров сбора и передачи данных, применяемых в системах подсчёта пассажиров:

а) Полнофункциональные компьютеры/контроллеры в промышленном исполнении (рис. 6).

Достоинства:
– возможность проводить любые требуемые вычисления (обработка сигналов от датчиков, защита/шифрование информации и т. д.);
– большая номенклатура поддерживаемых интерфейсов и протоколов обмена данными;
– возможность реализации собственных протоколов обмена данными;
– широкие возможности по архивированию/буферизации больших объёмов данных.

Недостатки:
– высокая стоимость с учётом желаемых технических характеристик для эксплуатации на транспорте;
– относительно большие габариты.

б) Терминалы для сбора данных от датчиков и передачи информации на удалённый сервер по каналу GSM/GPRS (рис. 7).

Достоинства:
– потенциально, самое доступное по цене решение;
– компактность, простота установки.

Недостатки:
– нет возможности реализовать сложные алгоритмы обработки данных (например, совместную обработку сигналов от нескольких датчиков подсчёта пассажиров);
– ограниченный состав реализованных/доступных интерфейсов и протоколов обмена данными.

Тип контроллера сбора и передачи данных определяется в первую очередь применяемыми датчиками подсчёта пассажиров и необходимостью во внешнем вычислителе для корректной обработки сигналов от них.

Заключение

В настоящий момент уровень развития средств автоматизации позволяет создавать системы подсчёта пассажиров общественного транспорта с требуемыми эксплуатационными характеристиками. Наиболее интересным и перспективным вариантом (с учётом итоговой стоимости решения) видится применение датчиков подсчёта пассажиров на базе стереоскопических видеокамер и ГЛОНАСС-терминалов с подходящим набором интерфейсов и сигналов ввода-вывода для сбора и передачи данных на сервер АСПП.

Рис. 6. Полнофункциональный промышленный компьютер

Рис. 7. ГЛОНАСС–терминал

Павел Литвинов, ЗАО «РТСофт»

«РТСофт» на European Utility Week

С 4 по 6 ноября в Амстердаме прошла крупнейшая в Европе выставка, посвящённая современным технологиям и решениям для коммунального хозяйства, European Utility Week. Своими впечатлениями об этом мероприятии и мыслями о перспективах внедрения интеллектуальных технологий на российский рынок делится в интервью с Редакцией журнала «МКА: ВКС» начальник аналитического отдела компании «РТСофт» Павел Васильевич Литвинов.

Редакция: *Чем вызван интерес к выставке? Ведь столь поэтично звучащее Utility на русский язык переводится просто ЖКХ?*

Павел Литвинов: Сегодняшний уровень использования современных технологий в этой области в России более чем скромный, но именно это и внушает оптимизм. Очевидно, что многолетнее ежегодное повышения тарифов – путь, который ведёт в тупик. Можно посчитать сложный процент от повышений только за последние 10 лет, можно сравнить наши тарифы с европейскими – а разговоры об убытках и необходимости новых повышений не стихают. Объективно сейчас рождается новый рынок, размер которого определяется масштабами страны и глубиной накопившихся проблем. За новыми трендами на ближайшие 5 лет и решениями, которые будут востребованы уже завтра, и имело смысл лететь в Амстердам.

Р.: *Как это выглядело, чтобы просто представить?*

П.Л.: Масштабное зрелище. На территории четырёх футбольных полей представители 450 компаний демонстрировали настоящее и будущее отрасли. Параллельно проводилась конференция, посвящённая различным аспектам сбережения и рационального использования ресурсов (энергия, газ, вода). Напряжённое расписание презентаций с примерами прикладного использования представляемых решений на все три рабочих дня. Среди самых ярких были впечатления, оставленные от посещения мероприятий Innovation Hub – где были представлены тренды, которые определят и изменят нашу жизнь в ближайшие годы. Многие вендоры, казалось бы, далёкие от Utility работают над решениями, которые могут быть полезны этому рынку.

С ними можно было познакомиться на стендах таких гигантов, как ABB, Ericsson, Cisco, NEC, IBM, Siemens, Panasonic и даже Google!

Р.: *Состав посетителей?*

П.Л.: Со всего мира. Виден растущий интерес со стороны развивающихся стран. Если вам нужно в непринуждённой обстановке пересечься, например, с

Выставочный зал

Конференция

министром энергетики Пакистана или Монголии – отличные шансы. По утверждению организаторов, более 30 тыс. посетителей. По собственным впечатлениям, ближе 5 км от Amsterdam RAI невозможно было найти место в гостинице.

Р.: *Как же возможна экономия и сбережение при таких расходах на рекламу и продвижение?*

П.Л.: Хотелось бы точнее расставить акценты. С точки зрения потребителя, речь идёт скорее не об экономии (в самом слове есть оттенок того, что вы чего-то приятного себя лишаете), а о рациональном использовании и потреблении. С точки зрения поставщиков ресурсов – они получают предсказуемую отдачу от инвестиций, бóльшую эффективность и управляемость своей операционной деятельности. Поставщики – выручку от продажи изделий, системные интеграторы – долгосрочные многоэтапные проекты. А в масштабах государства получается значительная экономия ресурсов при, что не менее важно, одновременном увеличении удовлетворённости потребителей.

Р.: *Звучит многообещающе для всех сторон! С чего посоветуете начать?*

П.Л.: Приходите в «РТСофт» со своими вопросами, задачами и проблемами. Подберём оптимальное решение! Простой пример: автомат управления уличным освещением, который может дистанционно управляться или работать автономно, – имеет встроенный астрономический календарь. Круглый год без всяких забот у вас будет оптимальный режим освещения от коттеджа до городских районов. Когда речь идёт о городе, полезной будет уникальная для такого вида устройств функция АЧР: если частота снижается – автомат отключает нагрузку.

Р.: *А что-нибудь более масштабное?*

П.Л.: Известно, что одним из краеугольных камней Smart Grid являются технологии умного учёта. Мы готовы предложить счётчики, концентраторы данных и специализированное ПО с большим потенциалом к построению различных решений с низкой совокупной стоимостью владения на их основе. Вот некоторые технические возможности умных счётчиков:

- возможность длительной автономной работы с накоплением данных;
- функции контроля качества электроэнергии;
- лёгкая масштабируемость от десятков до десятков тысяч устройств;
- надёжное шифрование соединения и передаваемых данных;
- сервис поддержки событий, позволяющий дистанционно отслеживать состояние счётчика и все аспекты его эксплуатации;
- удалённое обновление ПО; поддержка двух прошивок (если новая не применилась или работает неправильно, можно вернуться к более ранней версии и восстановить функциональность);
- возможность передачи сообщений с верхнего уровня на объектовый (это может быть текстовое сообщение или даже картинка; энергосбытовая компания может уведомить об отключениях, необходимости оплаты и т. п.);
- дистанционное отключение нагрузки при определённых условиях.

Р.: *Где ещё, кроме сферы ЖКХ, могут использоваться эти решения?*

П.Л.: Коммунальная сфера далеко не единственный рынок для подобных решений, просто он самый массовый. Максимально быстрая отдача может быть достигнута в промышленности. Предлагаемые

Общий вид стенда партнёров «РТСофт» компании NES

нами решения далеко выходят за рамки технического и (или) коммерческого учёта электроэнергии. Смежные задачи помогает решать техническое совершенство приборов учёта и используемой архитектуры:

– наличие порта расширения, позволяющего собирать информацию с внешних устройств и передавать её по протоколу PLC (Power Line Communication) вместе с данными счётчика. Другими словами, мы получаем интерфейс, который позволяет параллельно с учётом решать и другие задачи в части сбора и передачи информации на верхний уровень. Главное, не требуется проектировать и прокладывать линии связи, приобретать телекоммуникационное оборудование. При этом мы не используем беспроводные соединения, применение которых на многих объектах ограниченно или прямо запрещено по соображениям информационной безопасности;
– наличие дополнительной шины, позволяющей полноценно включить в работу другие устройства учёта – вода, тепло, газ и т. п.;
– гибкая система настройки режимов обмена данными с концентратором. Есть возможность послать срочный запрос и не разрывать канал до получения ответа;
– возможность передавать кодированную информацию через сообщения и использовать её для телеуправления смежными системами.

Разумеется, это не жёсткое «реальное время», но в любой работающей технологической системе оно уже реализовано средствами АСУ ТП и SCADA. А вот дополнительные потребности в части сбора и передачи информации на верхний уровень для вспомогательных, вторичных и новых систем – пожалуйста. Без вмешательства в существующие!

Р.: *Как вам видится портрет потребителя перечисленных технологий и его мотивация?*

П.Л.: Такие решения будут приниматься руководителями со стратегическим типом мышления, амбициями, устремлёнными в будущее, сделать город, завод или просто ДЭЗ образцовым и эффективным. Хорошая экономическая и финансовая подготовка – ускорят принятие мудрого решения ☺. Что касается мотивации, она в достаточной мере осуществляется на государственном уровне. Ежегодное повышение тарифов, которое позволяло не думать о модернизации, всё чаще замораживается или существенно ограничивается. Можно упомянуть «Государственную программу Российской Федерации «Энергоэффективность и развитие энергетики», принятую в апреле 2014 года. Программа не только ставит задачи, но и определяет объёмы и порядок финансирования.

Р.: *Большое спасибо за интересное и вдохновляющее интервью!*

Автомат управления уличным освещением

Счётчики разных модификаций и концентратор данных (слева) производства компании NES

Леонид Орлов, ЗАО «РТСофт»

Построение цифровых подстанций 35–110 кВ для распределительных сетей

Технологии цифровой подстанции (ЦПС) активно развиваются, и сегодня рассматривается их применение как в магистральных, так и в распределительных сетях РФ. Однако для применения технологий ЦПС в распределительно-сетевой компании (РСК) необходимо учесть ряд технических и организационных факторов.

Традиционно к элементам ЦПС относят следующие технологии:

- полевое УСО или контроллер для «цифровизации» коммутационных аппаратов:
  - базовый вариант – УСО для разъединителей и ЗН, используемое только для нужд АСУТП;
  - расширенный вариант – УСО для всех КА, используемое также для нужд РЗА, ПА и других вторичных систем ПС;
- цифровизация измерительных ТТ/ТН:
  - базовый вариант – аналоговые мультиплексоры (AMU), подключаемые к традиционным ТТ/ТН, с оцифровкой измерений в формат МЭК 61850-9-2;
  - расширенный вариант – цифровые ТТ/ТН с непосредственной выдачей информации в формате МЭК 61850-9-2;
- централизованные решения (укрупнение функциональных устройств или программная реализация всех функций в едином сервере).

Базовый принцип ЦПС – однократный ввод информации с последующим многократным её использованием для нужд различных систем.

В ходе совместной работы со специалистами различных РСК мы пришли к выводу, что применение технологий ЦПС в РСК затруднительно, поскольку в них ещё не получила широкого распространения комплексная автоматизация ПС.

Эффективность различных технологий автоматизации и ЦПС для различных типов ПС РСК

Технология	ОРУ-110	ОРУ-35	КРУЭ-110	КРУ-35
Распределённая структура	+	+	+	+
Комплексная АСУТП	+	+	+	+
МЭК 61850-8-1 для АСУТП и ОБР	+	+	+	+
МФУ (ТМ+ОБ)	+	+	+	+
МФУ (ТИ+ТС+ТУ)	+	+	+	+
МФУ (РЗА+АУВ+КП)		+		+
МЭК 61850-8-1 GOOSE для РЗА		+		+
Полевое УСО	+	+	+	
Полевой контроллер			+	
AMU с выходом 61850-9-2				
ЦИТ с выходом 61850-9-2				

Был сформирован перечень базовых технологий автоматизации, освоение которых должно предшествовать применению элементов ЦПС:

– распределённая структура систем автоматизации;
– реализация систем автоматизации в виде отдельных функциональных ПТК (телемеханика, оперативная блокировка, система мониторинга РЗА);
– комплексная автоматизация ПС с использованием единого ПТК АСУТП;
– комплексный подход ко вторичным системам;
– использование многофункциональных устройств РЗА/АСУТП/ТМ для нужд различных подсистем.

Техническая целесообразность применения данных технологий несомненна, но основным препятствием для их внедрения является существующая организационная структура РСК. Общепринятый подход к автоматизации в РСК – это создание нескольких автономных ПТК, ориентированных на независимое использование различными службами.

Комплексная автоматизация ПС потребует пересмотра зон ответственности различных служб при эксплуатации единого ПТК АСУТП, а в будущем – единого ПАК ЦПС.

Ещё одна особенность РСК – объекты автоматизации (в основном ПС 35–110кВ и ниже). Не все технологии ЦПС эффективны для таких объектов. Целесообразность их использования также зависит от типоисполнения ПС.

По результатам исследований компании «РТСофт» разработана таблица эффективности различных технологий автоматизации и ЦПС для различных типов ПС РСК (см. предыдущую страницу).

Выводы по результатам анализа:

1) ЦПС для РСК – это в первую очередь комплексный подход к автоматизации и вторичным системам;

2) Наиболее эффективны простые решения:

а. Многофункциональные устройства РЗА/АСУТП/ТМ;

б. Полевые УСО и контроллеры с поддержкой МЭК 61850-8-1.

Компания «РТСофт» готова предложить и реализовать оптимальные и эффективные решения по построению цифровых ПС всех классов напряжения.

Новости рынка

«РТСофт» автоматизировал первую инновационную цифровую подстанцию Санкт–Петербурга «Монетная»

Компания «РТСофт» автоматизировала цифровую комплектную трансформаторную подстанцию Санкт-Петербурга – КТПМ 35 кВ № 830 «Монетная». Это первая подстанция нового поколения, часть грандиозного проекта по реконструкции энергосетей Петроградского района города.

Специалисты «РТСофт» создали на подстанции автоматизированную систему управления технологическим процессом (АСУТП) на базе собственного программно-технического комплекса SMART-SPRECON и провели первый этап пусконаладочных работ. Стоит отметить, что работы по внедрению оборудования и программного обеспечения «РТСофт» был и сделаны в кратчайшие сроки – менее чем за 2 недели. На КТПМ 35 кВ «Монетная» установлена АСУТП последнего поколения, выполненная с учётом самых высоких требований к надёжности. Система удобна в эксплуатации и позволяет персоналу полностью управлять объектом с диспетчерского центра.

Мероприятие по случаю торжественного запуска этого энергообъекта состоялось 11 сентября 2014 года. В нём приняли участие генеральный директор ОАО «Россети» Олег Бударгин, врио губернатора Санкт-Петербурга Георгий Полтавченко, генеральный директор ОАО «Ленэнерго» Андрей Сорочинский. Присутствующие отметили уникальность и важность выполненного проекта. Ведь сегодня для Санкт-Петербурга реконструкция сильно изношенных подстанций – острая необходимость.

«Монетная» – инновационный проект, который выводит на новый уровень развитие энергосистем Санкт-Петербурга. Подстанция создана с применением самых современных технологий, экологична и занимает в три раза меньшую площадь, чем прежние трансформаторные подстанции.

Во время церемонии официальные лица протестировали оборудование и проверили возможности АСУТП. Все системы с успехом выдержали испытания, а реализация проекта получила самую высокую оценку.

Первая инновационная подстанция позволит Петроградскому району избавиться от перебоев с электричеством, значительно снизить потери и повысить надёжность электроснабжения.

Источник: Пресс-служба ЗАО «РТСофт»

А. А. Небера, Н. Г. Шубин. ЗАО «РТСофт»

Распределительные сети и Микрогрид

SmartGrid, MicroGrid, возобновляемые источники энергии, синхронизированные векторные измерения – самые обсуждаемые темы в электроэнергетическом мире. На стыке этих новейших энергетических технологий и зарекомендовавших себя современных энергосистем при непосредственном участии потребителей на наших глазах рождается электроэнергетика будущего. Пока не до конца понятно – чем закончится эта встреча хорошего и нового. Приведёт ли она к очередной научно-технической революции и радикальным изменениям привычного энергетического уклада или новейшие технологии будут незаметно поглощены эволюцией развития? Предлагаемая статья не даёт ответа на этот вопрос, в ней обсуждаются конкретные проблемы и возможности трансформации фрагментов современных распределительных сетей в малые распределённые энергосистемы – в MicroGrid (Микрогрид).

Введение

Тенденции развития электрических распределительных сетей (РС) определяются изменяющимися потребностями общества и находятся в зависимости от прогресса электроэнергетического оборудования, технологий потребления электроэнергии, коммуникационных технологий и разнообразных условий территории (климатические, экологические, стеснённость и др.).

Характерные для современного общества потребности и объективные условия, такие как:

- желание людей жить за пределами перегруженных и экологически загрязнённых мегаполисов;
- стремление администраций к выносу промышленности и её инфраструктуры из центра городов и вообще за пределы городской черты;
- рост электровооружённости домашних хозяйств и культурно-спортивно-развлекательных предприятий;
- повышение требований к сокращению времени на технологическое присоединение новых потребительских электроустановок к сети (принцип «время не ждёт»);
- дороговизна и объективно медленные (относительно динамичных потребностей бизнеса) темпы строительства электрических сетей, –

в совокупности с такими факторами, как:

- постоянное повышение КПД и встречное снижение себестоимости малой электро-, ко- и тригенерации;
- расширяющееся рыночное предложение оборудования для возобновляемых источников энергии (ВИЭ) и малой генерации при одновременном росте интереса к этой теме потребителей электроэнергии (потенциальный спрос);
- наличие в ряде регионов источников относительно дешёвого топлива, –

являются движущими силами (драйверами) трансформации существующих РС в относительно независимые *распределённые энергосистемы (РЭ)*, допускающие возможность свободного синхронного присоединения к ним разнообразной малой генерации.

Открытый, постоянно пополняемый список возможных видов малой генерации включает в себя топливные элементы, ветровые турбины, фотоэлектрические и нагревательные солнечные системы, гидравлические, геотермальные и газопоршневые установки, микротурбины, работающие на газе, в том числе на биотопливе, и другие. В отличие от огромной ЕЭС России и других больших энергосистем, относительно небольшие по мощности РЭ не могут нормально функционировать без двух дополнительных компонентов:

- *накопителей энергии*, способных быстро и точно нейтрализовать небалансы активной и реактивной мощности;
- *системы автоматического управления (САУ)*, обеспечивающей живучесть распределённой энергосистемы на всём множестве схемно-режимных ситуаций, включающем нормальные, ремонтные, аварийные и послеаварийные режимы.

Небольшие автоматически управляемые РЭ, обладающие чёткими территориальными границами, получили название *микрогридов* (МГ). В одной из первых публикаций, посвящённой обсуждаемой теме, – «White Paper on Integration of Distributed Energy Resources. The CERTS MicroGrid Concept» [1], МГ определяется как агрегированное множество нагрузок и микроисточников, управляемых как единая система, производящая электро- и теплоэнергию, обеспечивающая надёжность и безопасность локального потребления. Таким образом, первоначально термин МГ обозначал полностью изолированную локальную систему электроснабжения. В современной трактовке МГ – это **группа распределённых нагрузок потребления и различных энергетических ресурсов – источников и накопителей энергии (электро-, тепло-), объединённых электрической сетью переменного и/или постоянного тока в рамках определённых границ, действующая и воспринимаемая операторами больших энергосистем и центров управления сетями как единый управляемый объект, который можно свободно подключать/отключать к/от электрической сети общего назначения.** При отключении от энергосистемы МГ должен продолжать надёжное и безопасное энергоснабжение своих внутренних потребителей в автономном (островном) режиме с соблюдением нормативных требований к качеству электроэнергии.

Пример МГ приведён на рис. 1.

Особенности функционирования и Требования к микрогриду

Наиболее близкими предшественниками МГ являются широко применяемые схемы электроснабжения предприятий с системами гарантированного питания (СГП). Современные СГП работают по логике *или*, при которой электрическое питание либо полностью обеспечивается от сети энергосистемы, либо – частично или полностью – от внутреннего независимого источника энергии. Таким образом, СГП предназначены для кратковременного частичного замещения основного источника питания на резервный. МГ же, согласно замыслу, разрабатываются для длительной синхронной работы с большой энергосистемой в целях достижения более экономичного и надёжного энергообеспечения внутренних потребителей. Обозначенное су-

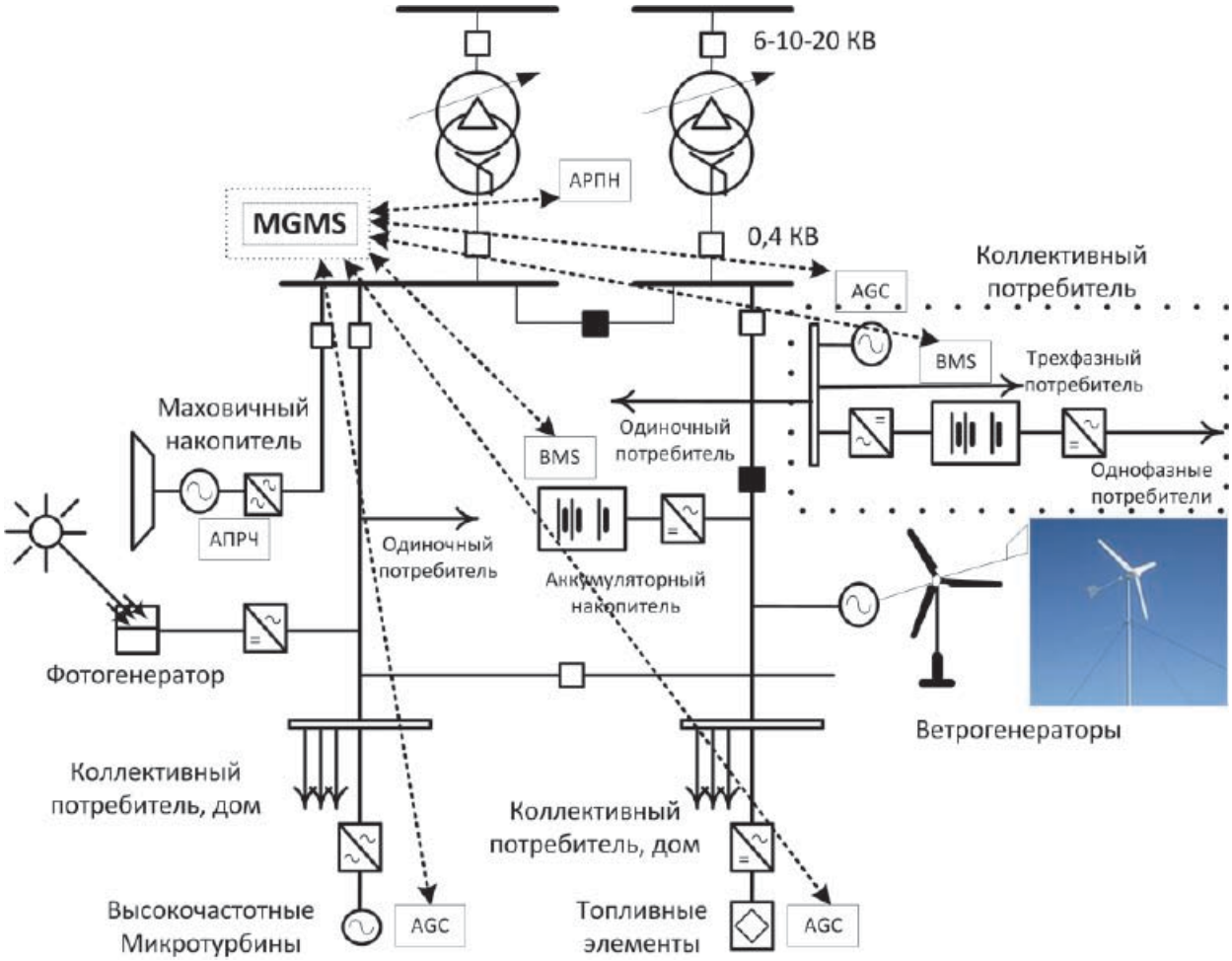


Рис. 1. МГ на напряжении 0,4 кВ

щественное различие в предназначении не означает, однако, гигантской технологической дистанции жду СГП и МГ. Для перехода от СГП к МГ требуется решить всего лишь две принципиальные проблемы:

1. Необходимо обеспечить физическую возможность синхронной работы внешней сети и внутренних источников энергии при сохранении способности внутренних источников справляться с заведомо несимметричной и неравномерной во времени потребительской нагрузкой при выделении МГ на автономную работу.

2. Требуется обеспечить экономичность продолжительной работы внутренних источников МГ.

Экономичность внутренних источников микрогрида

Электрический КПД современных газопоршневых установок и газовых микротурбин мощностью от единиц до нескольких сотен киловатт достигает соответственно 43 и 30–33 %, что делает их соизмеримыми по энергоэффективности с газовыми энергоблоками большой энергетики. Это обстоятельство создаёт экономические предпосылки для развития потребительской распределённой генерации. Однако на практике обеспечить экономичную и надёжную работу МГ оказывается не так просто. Дело в том, что при выделении на островной режим генераторы МГ должны питать сильно неравномерную, меняющуюся во времени, нагрузку потребителей (рис. 2). В больших энергообъединениях, крупнейшим из которых является синхронная Зона ЕЭС России, диапазон суточного хода потребления составляет около 20 % от его максимального значения. В РЭ соотношение максимальных и минимальных суточных нагрузок значительно выше – может составлять 3-4 раза и более. Это обстоятельство определяет специфические условия работы генерации внутри МГ.

В современных схемах с СГП «спасаемая» нагрузка потребления полностью ложится на единственный резервный источник (на рис. 2 вариант выбора состава оборудования 1). Очевидно, что в этом случае бóльшую часть времени, кроме кратковременных режимов максимального потребления, питающий генератор будет работать со значительной недогрузкой, то есть неэкономично – в зоне низких КПД. Более того, если на острове имеются двигатели, то для обеспечения нормального режима их пуска или самозапуска потребуется ещё бóльшее завышение мощности резервного генератора, что приводит к ещё бóльшему снижению энергоэффективности.

Повышения экономичности МГ можно добиться путём разукрупнения генерации, а именно: вместо одного источника, покрывающего всё электропотребление, в МГ используется множество мелких. В этом случае общая потребность в мощности обеспечивается более точно и экономично за счёт оптимального выбора состава включенного генерирующего оборудования (ВСВГО), реализуемого в САУ МГ (или MicroGrid Management System – MGMS). На рис. 2 график включённой генерирующей мощности, формируемый MGMS, представлен вариантом выбора состава оборудования 2 (чёрный пунктир). Автоматическая технология ВСВГО должна включать в себя подсистемы:

– прогноза профиля энерго- и электропотребления;
– определения необходимого резерва мощности, учитывающего:
– – пропускную способность сети МГ;
– – готовность к работе, запасы топлива и допустимую скорость набора/сброса нагрузки на управляемых источниках генерации;
– – вероятные аварийные отключения источников генерации и/или сетевых элементов (принцип N-k).

Уместно добавить, что разукрупнение внутренней генерации МГ способствует не только повышению

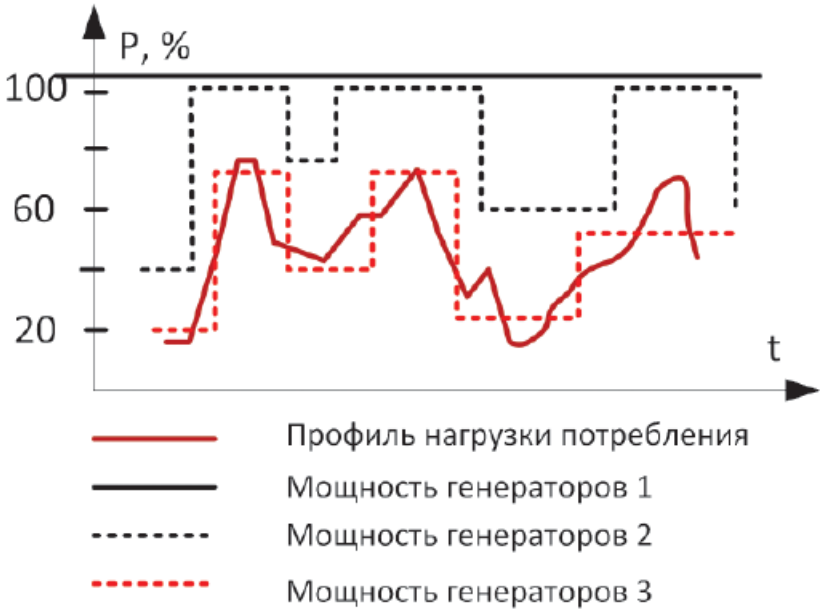


Рис. 2. Профиль нагрузки потребления и состав включенного генерирующего оборудования

экономичности, но в ещё бóльшей мере – обеспечению допустимых отклонений частоты при вероятных аварийных отключениях отдельных внутренних источников генерации.

При наличии существенной суточной волатильности рынка электроэнергии, заключающейся в значимом изменении рыночной цены на электроэнергию внутри суток, дополнительный вклад в повышение экономичности работы МГ может внести *технология управления спросом* (ТУС). Так, при существующем уровне рыночных цен на электроэнергию порядка 1500 руб./МВтч и суточной дифференциации цен (макс.–мин.)/мин. = 40 % годовая экономия от перемещения одного МВтч электроэнергии из пиковой зоны графика суточных цен в провальную даёт при покупке электроэнергии экономию на 1,5 миллиона рублей [2].

Особенности поведения потребления РЭ не исчерпываются одним только большим диапазоном суточного изменения профиля потребления. Сложности в управлении балансами мощности и режимами в МГ создают также:

– большой размах нерегулярных колебаний потребления;
– включение в состав МГ резкопеременной генерации на возобновляемых источниках энергии (ВИЭ), подверженной влиянию случайных метеорологических факторов;
– существенную несимметричность нагрузки и других параметров режима;
– искажение синусоидальности формы переменного напряжения и токов.

Преодоление технических проблем внутренней сети микрогрида

Нерегулярные колебания и интеграция ВИЭ–генерации

Нерегулярные колебания потребления активной и реактивной мощности – явления по своей физической сути случайные, то есть величины непредсказуемые. Это означает, что их подавление в режиме планирования графика генерации принципиально невозможно. Если не предпринимать специальных технических и экономических мер, нерегулярные колебания нагрузки МГ будут напрямую транслироваться на такие показатели качества электроэнергии, как частота и уровни напряжения. Такими специальными техническими средствами, эффективно поддерживающими нормальное качество электроэнергии по частоте и уровням напряжения в больших энергосистемах, являются локальные (ОПРЧ – общее первичное регулирование частоты и НПРЧ – нормированное первичное регулирование частоты) и централизованные системы регулирования частоты и мощности. Однако в условиях МГ скорости реакции силовых агрегатов, управляемых такими системами, будут недостаточны для нейтрализации повышенного уровня нерегулярных колебаний. По этой причине компенсация нерегулярных колебаний балансов мощности и напряжения в МГ обеспечивается в темпе процесса быстродействующими динамическими компенсаторами, силовая электроника которых мобильно использует возможности различных накопителей энергии: маховичных, аккумуляторных, суперконденсаторных и конденсаторных. Обеспечение согласованной работы разнообразных систем регулирования генерации и потребления МГ, включая быстродействующие системы управления накопителями энергии, – ещё одна важная функция MGMS (наряду с функцией ВСВГО). Специфика и подходы к моделированию работы систем смешанного локально-централизованного управления частотой в МГ при их выделении на изолированную работу освещены в [3].

Кроме быстрого и качественного управления балансами мощности, использование накопителей энергии позволяет также дополнительно повысить экономичность работы МГ за счёт снижения включённой управляемой генерации МГ и прохождения экстремальных нагрузок (пики и минимумы) за счёт накопленной или сохраняемой энергии. На рис. 2 график включённой генерирующей мощности, формируемый MGMS при наличии накопителей, представлен вариантом выбора состава оборудования 3 (красная ступенчатая пунктирная линия).

В то же время стабилизирующего эффекта от разукрупнения источников генерации и создания системы смешанного локально-централизованного регулирования режима (в составе MGMS), воздействующей на источники и накопители энергии, может оказаться недостаточным. В этой связи для окончательного преодоления проблем с нестабильностью частоты и напряжений при работе МГ в островных режимах к регулированию необходимо привлекать потребителей энергии. В первую очередь целесообразно обеспечить качественную настройку таких традиционных средств аварийного регулирования частоты (АРЧ), как автоматическая частотная разгрузка (АЧР), дополнительная аварийная разгрузка (ДАР) и частотное автоматическое повторное включение (ЧАПВ). При проектировании и настройке средств АРЧ необходимо учитывать как внешние требования, транслируемые на МГ со стороны Системного оператора, так и внутренние схемно-режимные условия, которые в разных МГ могут иметь существенные индивидуальные особенности. В этой связи потребуется тщательное моделирование режимов внутренней сети МГ с учётом меняющейся частоты и электромеханических процессов.

Другие серьёзные вызовы генерации МГ формируются несимметричностью и нелинейностью нагрузок и других параметров режима сети переменного тока.

Несимметрия и несинусоидальность

Сети низкого напряжения, ввиду большого количества относительно случайно включаемых/отключаемых однофазных нагрузок, являются естественными производителями несимметрий и несинусоидальностей.

Никакое, даже самое тщательное, статическое распределение этих нагрузок между фазами принципиально не может противостоять динамическому нарушению равенства нагрузки фаз, вызывающему соответствующую несимметричность параметров электрического режима. В то же время для обеспечения надёжной работы и предотвращения сокращения сроков службы трёхфазных электрических машин (генераторы и двигатели) требуется ограничивать разность токов в фазах 10-ю процентами. В режимах с изолированной нейтралью, а именно в таких режимах эксплуатируются электрические генераторы, проблемы создаются так называемыми токами обратной последовательности, вызывающими в машине ряд нежелательных явлений, и делают режим работы машины тяжёлым [4]. В частности, наличие обратной последовательности в магнитном поле статора вызывает:

– излишние потери в роторе (особенно в неявнополюсных машинах), вызванные индуцированными токами двойной промышленной частоты, и его нагрев, сопровождаемый также снижением КПД машины (высокие температуры ротора способны вызывать в нём опасные деформации, что резко повышает вероятность повреждения изоляции обмотки возбуждения);
– повышенную вибрацию машины, появляющуюся в результате взаимодействия магнитных потоков возбуждения и обратной последовательности статора, а также – поля прямой последовательности статора и поля токов двойной частоты ротора (при этих воздействиях на ротор и статор действуют знакопеременные вращающие моменты и тангенциальные силы, пульсирующие с частотой 100 Гц);
– искажение симметрии напряжений. В результате различности падений напряжений в фазах напряжения более загруженных фаз будут несколько ниже, в менее загруженных – выше. Несимметрия напряжений ухудшает условия работы приёмников, в особенности асинхронных и синхронных двигателей.

Высшие гармоники тока могут вызывать опасные резонансные явления, если цепи обмоток статора работают на емкостную нагрузку, формируемую, например, электрическими ёмкостями кабельных линий электропередачи. В результате резонанса напряжений на зажимах обмотки статора возникают напряжения повышенных частот, которые могут превышать номинальные напряжения во много раз и приводить к преждевременному повреждению изоляции машины.

Эффективной формой борьбы с резонансами напряжений в большой энергетике считается применение мощных успокоительных (демпферных) обмоток. Например, демпферные обмотки уникальных мощных гидрогенераторов, работающих на длинные линии передачи (емкостной характер нагрузки), позволяют выровнять сверхпереходные сопротивления генера-

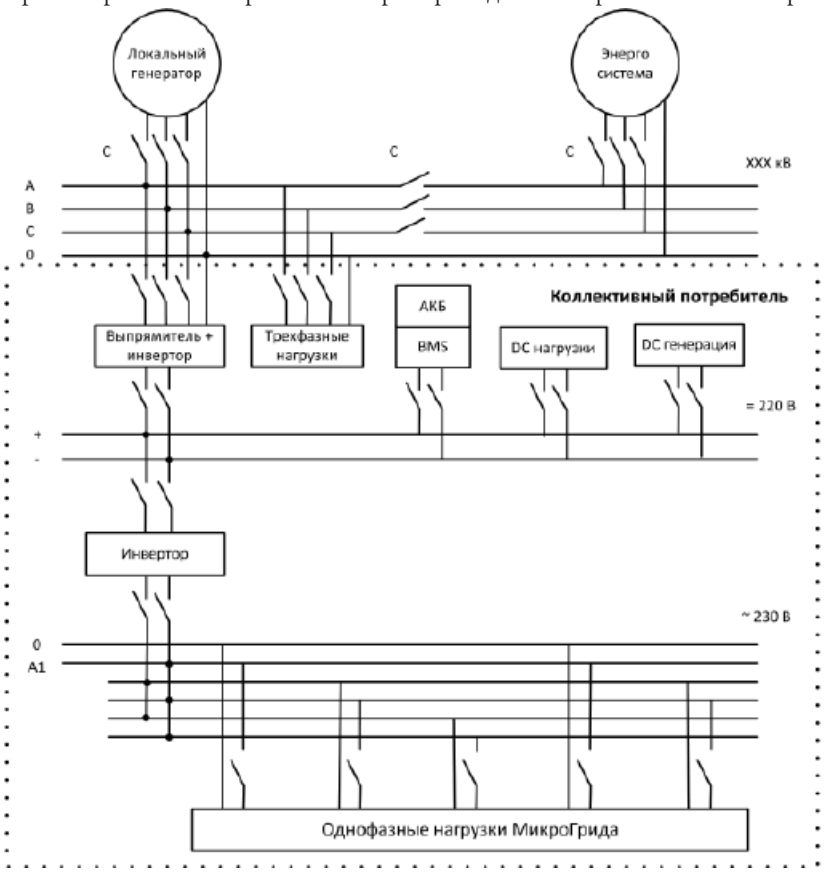


Рис. 3. Пример схемного решения по отделению сети постоянного тока и однофазных нагрузок переменного тока некоего коллективного потребителя от основной сети МГ, изображённой на рис. 1

торов по продольной и поперечной осям, вследствие чего токи остаются синусоидальными и опасность резонансных перенапряжений исчезает.

К сожалению, демпферные обмотки не устанавливаются на малые электрические машины. Поэтому для МГ требуется найти свои методы борьбы с несинусоидальностью.

Радикальным способом преодоления проблем несимметричности параметров режимов и несинусоидальности формы кривых переменных токов и напряжений является физическое отделение трёхфазной генерации от заведомо несимметричных и нелинейных нагрузок. На рис. 3 приведён пример схемного решения по отделению сети постоянного тока и однофазных нагрузок переменного тока некоего коллективного потребителя от основной сети МГ, изображённой на рис. 1. Такая схема обеспечивает надёжную изоляцию трёхфазной сети от любой несимметрии и несинусоидальности. Недостатком этой схемы является то, что присутствующие в ней выпрямители и инверторы имеют не стопроцентный КПД. Потери в преобразователях составят около 10 %.

Другие способы борьбы с нарушениями показателей качества электроэнергии предусматривают использование быстродействующих регулируемых компенсирующих устройств: источников реактивной мощности и *кондиционеров* или динамических компенсаторов искажений напряжений (ДКИН).

Заключение

Потребность общества в расширении жизненного пространства за пределы перегруженных мегаполисов, повышение требований бизнеса к сокращению времени на технологическое присоединение к сетям, дороговизна и объективно медленные темпы строительства электрических сетей, наличие в РФ территорий со стеснёнными условиями, а также удалённых территорий, в том числе с экстремальными климатическими условиями, которые нуждаются в быстром и эффективном развитии, – могут послужить поводом к созданию новой сущности в электроэнергетике – распределённым энергосистемам и, в частности, МГ.

Ввиду особенностей физических процессов, происходящих в сетях среднего и низкого напряжения, МГ не могут быть созданы путём простого присоединения распределённой генерации к существующим РС. МГ – это инновационная технология, предусматривающая создание умной системы автоматического управления (MGMS), взаимодействующей с умными управляемыми энергоустановками генерации и потребления.

Поскольку МГ включает в себя множество разнородных внутренних энергетических источников, управляемых электроустановок потребителей, накопителей энергии и к тому же сам подключён к источникам внешнего электроснабжения, MGMS должна в темпе реального времени решать и технические, и экономические задачи. Технические задачи – по регулированию частоты и напряжения; по обеспечению устойчивости. Экономические задачи – по оптимальному динамическому распределению нагрузки между всеми управляемыми ресурсами.

Наличие интеллектуальной контролирующей, анализирующей, оптимизирующей и управляющей MGMS, наряду с появлением линий электропередачи с двухсторонним питанием, определяет основное отличие МГ от современных РС, внутренних электрических сетей домов и предприятий.

Появление МГ – это значимое явление на современном этапе развития электроэнергетики. МГ позволят:

1. Преодолеть нарастающую стихию неуправляемости режимов в сетях среднего и низкого напряжения. Действительно, МГ проектируются и формируются как агрегаты распределённых нагрузок и генерации, воспринимаемые Операторами энергосистемы и рынка как единые (виртуальные) объекты управления, обладающие внутренним порядком.

2. Усилить конкуренцию «снизу». Причём МГ позволяет не только усилить конкуренцию на площадке генерации, но и распространить конкуренцию в электроэнергетике на электрические сети.

МГ могут найти активное применение в стеснённых условиях мегаполисов, в отдалённых регионах России, в первую очередь в Сибири и на Дальнем Востоке. В регионах, где отсутствует централизованное электроснабжение, на территориях, расположенных вдали от крупных населённых пунктов, на объектах добывающей промышленности, в туристических центрах, на военных объектах и прочих.

Литература

1. Robert Lasseter, Abbas Akhil, Chris Marnay, John Stephens, Jeff Dagle, Ross Guttromson, A. Sakis Meliopoulous, Robert Yinger, and Joe Eto, «White Paper on Integration of Distributed Energy Resources. The CERTS MicroGrid Concept», LBNL-50829, 2002 г.

2. А. С. Бердин, О. Д. Молчан, Н. Г. Шубин, «Об участии потребителей в новом типе управления энергосистемой», журнал «Энергетика и ЖКХ Урала», июль 2013.

3. A. Madureira, C. Moreira and J. Pecas Lopes, «Secondary Load-Frequency Control for MicroGrids in Islanded Operation», 2005 г.

4. Вольдек А. И., «Электрические машины», 3-е издание, переработанное, издательство «Энергия», 1978 г.

Гао Кунлун (GAO Kunlun), China Electric Power Research Institute,
Ванг (WANG Yufei), China Electric Power Research Institute,
Ксу Руши (XU Ruzhi), North China Electric Power University

Исследование и применение методов ситуационного анализа кибербезопасности в интеллектуальных сетях

Когда информационно-коммуникационные технологии (ИКТ) стали всесторонне применяться во всех аспектах производства, передачи, преобразования и распределения электроэнергии, потоки электричества, технической и бизнес-информации достигли высокой степени интеграции в интеллектуальных сетях (smart grid). Поскольку интеллектуальные сети включают в себя большое количество информационных систем и оборудования, может возникнуть множество угроз, связанных с обеспечением кибербезопасности. Чтобы с этим справиться, должна быть построена система активной защиты интеллектуальной сети. Одна из ключевых технологий для построения такой системы – ситуационный анализ кибербезопасности (cybersecurity situation evaluation, CSSE).

На основании анализа большого числа микросостояний (событий) и мониторинга результатов технология CSSE позволяет спрогнозировать и оценить общую кибербезопасность интеллектуальной сети. Оценка методов защиты от кибератак сосредоточена в основном на информировании (cybersecurity situation awareness, CSSAw), оценке (cybersecurity situation assessment, CSSAs) и прогнозировании (cybersecurity situation forecast, CSSF).

Был предложен и реализован новый метод ситуационного анализа с применением алгоритма AdaBoost (Адаптивного усиления):

a. С помощью тщательного анализа процессов CSSAw и CSSF была описана аппроксимационной функцией их общая математическая модель. Кроме того, с учётом процессов CSSAw, CSSAs и CSSF была разработана интегральная модель CSSE, которая описывает как CSSAw, так и CSSF функциями аппроксимации и решает эти задачи по отдельности с помощью многократного применения алгоритма AdaBoost. Интегральная модель значительно упростила сложность модели CSSE.

b. В целях повышения надёжности метода CSSE были полностью учтены требования к точности, оперативности и интеллектуальности: для точности в качестве ключевого алгоритма аппроксимирующей функции использовался алгоритм AdaBoost, особенность которого заключается в непрерывном обучении, что значительно улучшает точность функции аппроксимации; для оперативности в качестве слабого «ученика» алгоритма AdaBoost используется метод CVM (core vector machine), что значительно уменьшает время расчётов и объём вычислений; интеллектуальность заключается в том, что все алгоритмы основаны на теории искусственного интеллекта и могут работать полностью в автоматическом режиме после предварительной настройки параметров работы.

c. На основании проекта по мониторингу кибербезопасности Государственной электросетевой корпорации Китая (State Grid Corporation of China, SGCC) модель CSSE была применена в крупномасштабной системе раннего предупреждения об угрозах кибербезопасности и её практичность была проверена в течение более трёх лет.

Введение

В последние годы интеллектуальные сети с функциями «информатизации, автоматизации, взаимодействия» переживают бурный рост. Информационные и коммуникационные технологии (ИКТ) широко используются во всех аспектах интеллектуальных сетей, таких как генерация, передача, преобразование, распределение и диспетчеризация электроэнергия и т. д., и обеспечивают высокую степень интеграции между потоками энергии, управляющей информации и данных. Интеллектуальные сети значительно расширили границы своего информационного простран-

ства и накопили большой опыт интеллектуального управления и взаимодействия их подсистем. Однако они сталкивается с беспрецедентными проблемами, связанными с кибербезопасностью. Интеллектульная сеть подвержена кибератакам, которые всерьёз ставят под угрозу её существование. Это, например, атаки на системы управления промышленными предприятиями [1, 2], крупные сетевые каскадные аварии, вызванные кибератаками [3, 4], атаки типа внедрения SQL-кода, направленные на интеллектуальную сеть [5, 6], и так далее.

Таким образом, традиционные методы обеспечения кибербезопасности, основанные на статической политике безопасности, постсобытийном тестировании и пассивной реакции, могут больше не удовлетворять потребностям текущей ситуации. Вместо этого предлагается система активной защиты от киберугроз, характеризующаяся встроенным «иммунитетом», динамическим информированием и целевым оповещением. Одной из ключевых технологий системы активной защиты является ситуационный анализ кибербезопасности (CSSE).

На основании анализа большого числа микросостояний (событий) и мониторинга результатов, CSSE позволяет провести оценку текущей ситуации и спрогнозировать общую кибербезопасность в реальном времени. Метод защиты от кибератак сосредоточен в основном на информировании о киберугрозах (cybersecurity situation awareness, CSSAw), оценке ситуации кибербезопасности (cybersecurity situation assessment, CSSAs) и прогнозировании (cybersecurity situation forecast, CSSF) [7, 8]. CSSAw используется для отображения локальной (микроскопической) ситуации с кибербезопасностью в целевой сети; CSSAs может интегрировать результаты CSSAw по всей сети, чтобы получить общую оценку кибербезопасности (cybersecurity situation value, CSSV), а CSSV отражает оценку кибербезопасности в режиме реального времени в целевой области на макроуровне; CSSF используется для получения оценки кибербезопасности в целевой сети в следующий момент.

В последние годы понятие CSSE вводится также в кибербезопасность, связанную с электроэнергией. В работах [9–12] в целях реализации информированности о ситуации с микробезопасностью для локальной области интеллектуальных сетей для разработки классификатора и решения проблем классификации использовались методы CVM (core vector machine) и BVM (ball vector machine), оптимизированные алгоритмами роевого интеллекта (PSO или QGA и т. д.), и классификатор служил системой обнаружения вторжений. В работах [13, 14] при построении системы индексов оценки кибербезопасности микрорезультаты CSSAw искусственно рассчитываются в CSSV для отражения исторической (архивной) и текущей (в реальном времени) оценки кибербезопасности сети. При построении системы индексов применены комплексные инструменты оценки, такие как метод анализа иерархий (МАИ) и «серый кластерный анализ» (gray clustering analysis). В работах [15, 16] для интеллектуальных сетей реализуется CSSF, где ключевая идея заключается в абстракции CSSF через задачу регрессии. Классификатор (SVM-классификатор, оптимизированный алгоритмами роевого интеллекта типа МРЧ (метод роя частиц) или QGA (quantum genetic algorithm) и т. п.) применяется для обучения и получения из архивных данных модели CSSF, и эта модель используется для раннего предупреждения о будущих тенденциях CSSV. Но есть определённый дефицит в результатах данных исследований. Несмотря на то, что предыдущие решения CSSAw и CSSF основаны на алгоритмах искусственного интеллекта, исследования этих двух частей независимы друг от друга и не имеют глубокого анализа их математического характера.

В данной статье представлена интегрированная модель CSSE. Практически она была развёрнута в информационной сети Государственной электросетевой корпорации Китая (SGCC). Этапы заключались в следующем:

a. Был проведён углублённый анализ рабочих процедур CSSAw и CSSF и выяснены математические характеристики для нахождения связей с их математическими моделями.

b. На основе алгоритма AdaBoost была разработана модель CSSE, последовательно выполняющая функции CSSAw, CSSAs и CSSF. Здесь алгоритм AdaBoost применяется несколько раз, чтобы упростить структуру модели CSSE, и использование характера самообучения алгоритма AdaBoost эффективно улучшает точность CSSE.

c. На основе проекта «системы обеспечения безопасности информационной сети (ISS)», модель CSSE была развёрнута в крупномасштабной системе мониторинга кибербезопасности.

Краткие сведения о CSSE

Области исследования CSSE

Для аккуратного описания ситуации с кибербезопасностью современной масштабной сети сегодня недостаточно полагаться только на простые сетевые эксплуатационные характеристики, такие как сетевая топология, рабочее состоянии каждого узла, сетевые соединения и сетевые потоки и т. д., требуются более сложные технические средства.

В 1988 году концепция оценки кибербезопасности была предложена при изучении технологии управления воздушным движением: «Оценка кибербезопасно-

сти сети – это текущее и прогнозное состояние всей целевой сети, содержащей различное функционирующее оборудование, а также поведение пользователей и других факторов в определённый период времени» [17]. Таким образом, CSSE должна включать в себя микро- и макропонимание текущего состояния кибербезопасности в целевой сети – CSSAw и CSSAs, а также прогноз кибербезопасности в целевой сети – CSSF.

Рис. 1. Процесс расчёта CSSV

CSSAw является эффективным средством для получения в режиме реального времени информации о микроситуации с кибербезопасностью для сети, по которой можно судить о существовании кибератак на основе всеобщего сбора данных в режиме реального времени с конкретных узлов в целевой сети. Данные содержат информацию о сетевых сообщениях, распределении сетевых потоков, состоянии системных процессов и функционировании сервисов. Обычно в качестве CSSAw для малых и средних сетей может быть использована технология обнаружения вторжений.

CSSAs может отвечать за использование системы индексов оценки кибербезопасности для расчёта текущей CSSV с помощью микрорезультатов CSSAw и за отображение в реальном времени макроситуации кибербезопасности целевой сети. CSSV – численное описание ситуации кибербезопасности. Это значение непосредственно отражает макроситуацию кибербезопасности в целом. Расчёт процесса CSSV показан на рис. 1.

CSSF предсказывает тенденции развития ситуации макрокибербезопасности прогнозированием будущего CSSV целевой сети.

Таким образом, существует явная причинная связь между тремя рабочими процессами: CSSAw – первый процесс, который должен быть запущен при оценке CSSE, затем процесс CSSAs использует CSSV для описания ситуации макрокибербезопасности посредством всеобъемлющего расчёта результатов CSSAw, и наконец CSSF использует CSSV в качестве источника данных. Полный цикл работы CSSE показан на рис. 2.

Анализ математических характеристик CSSE

Математические характеристики CSSAw

Процесс CSSAw представляет собой следующее: на основе текущего сетевого трафика производится запись мониторинга, которая состоит из n полей данных, затем они используются, чтобы различными аналитическими методами определить, принадлежит ли трафик к некоторым видам кибератак (при условии, что имеется m видов кибератак). Этот процесс аналогичен функции аппроксимации: целевая задача (CSSAw) с n-мерным входом (запись со структурой n полей данных) и 1-мерным выходом (выходное значение представлено m + 1 значениями скаляра, где m это виды кибератак, а 1 – нормальное функционирование сети). Так CSSAw можно абстрагировать в функцию проблемы с фиксированным выходным диапазоном.

Функция аппроксимации, соответствующая CSSAw, имеет фиксированный выходной диапазон (потому что виды кибератак ограничены), поэтому нелинейной функцией аппроксимации типа «S» можно добиться точной классификации данных мониторинга, как показано на рис. 3(а).

Математические характеристики CSSF

Процесс CSSF представляет собой следующее: CSSV v_1, v_2, ...,v_m – известные точки непрерывного мониторинга архивных данных, по которым с помощью различных методов прогнозируются CSSV v_{m+1}, v_{m+2}.

Теперь CSSF можно объяснить с помощью функции аппроксимации: CSSF имеет типичные характеристики одномерного временного ряда. В CSSF выходные значения (будущий CSSV) могут быть спрогнозированы

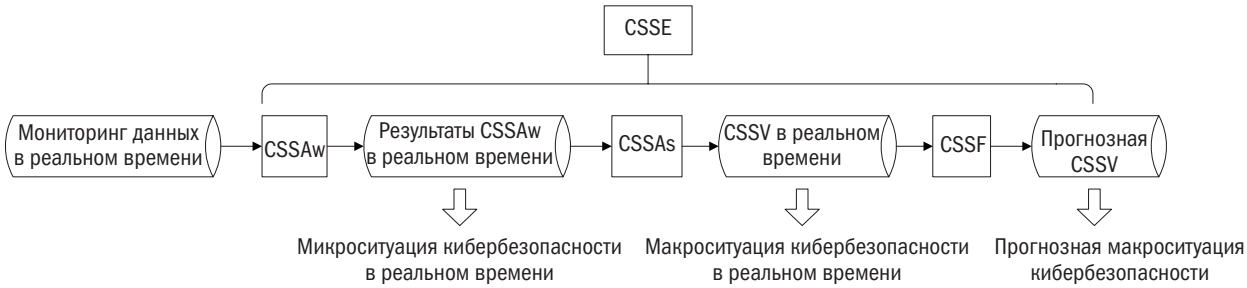


Рис. 2. Цикл работы CSSE

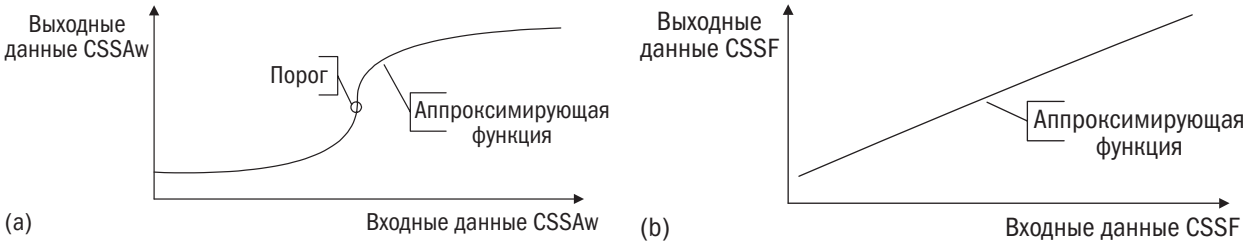


Рис. 3 Функция аппроксимации CSSAw (a) и функция аппроксимации CSSF (b)

через множество непрерывных входных значений (архивные значения CSSV). Необходимым условием решения проблемы временных рядов с помощью аппроксимирующей функции является построение нескольких дуальных групп «вход-выход».

Дуальная группа генерируется динамическим скользящим окном [18]. Если установить размер «скользящего» окна равным m, а длину шага равной 1, то первый вход «v_1, v_2, ..., v_m», даст на выходе v_{m+1}; аналогичным образом, второй вход «v_2, v_3, ...,v_{m+1}», даст на выходе v_{m+2} и так далее. Поскольку диапазон значений CSSV непредсказуем, линейная функция аппроксимации должна быть использована для описания CSSF, как показано на рис. 3(b).

Математическая составляющая между CSSAw и CSSF

Теперь мы видим, что, хотя CSSAw и CSSF находятся на разных стадиях CSSE, они имеют высокую согласованность математической составляющей. У них один и тот же рабочий механизм, который может оценивать один выход через множество входных факторов, и они оба могут быть описаны с помощью аппроксимирующей функции «многомерной вход – одномерный выход». Единственное различие между ними заключается в том, что формы аппроксимирующих функций различны, что обусловлено разными физическими смыслами CSSAw и CSSF. Процесс аппроксимации CSSAw и CSSF показан на рис. 4.

Оценка кибербезобасности модели Смартгрид

Интегральная структура модели оценки кибер–безопасности

CSSE может контролировать микро- и макроситуацию с кибербезопасностью всей целевой сети непрерывно и направить предупреждающий сигнал на ранней стадии для возможных ситуаций угроз кибер-

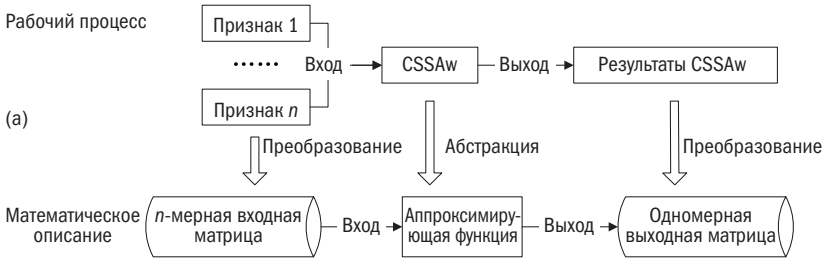


Рис. 4 (a) Процессы аппроксимации CSSAw

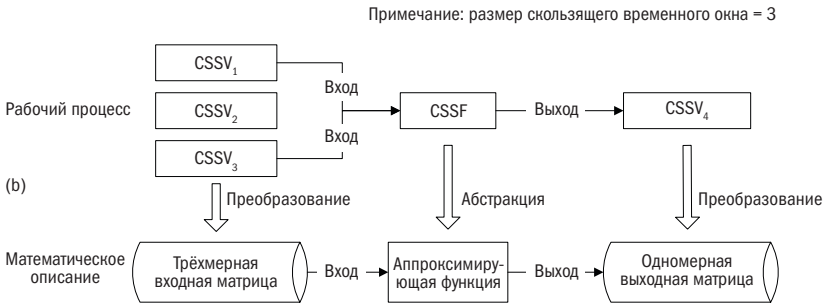


Рис. 4 (b) Процессы аппроксимации CSSF

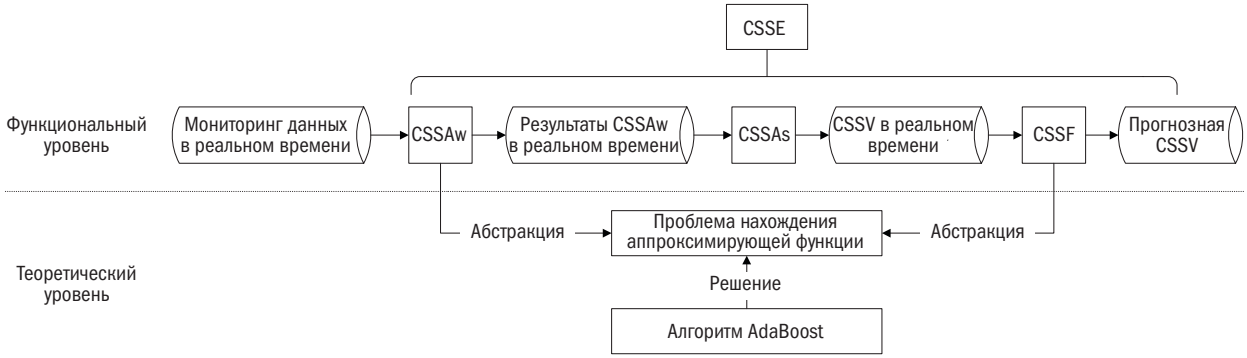


Рис. 5. Механизм работы модели CSSE

безопасности на макро уровне, так что модель CSSE может в полной мере реализовать CSSAw, CSSAs и CSSF. Как мы знаем, CSSAw и CSSF имеют один и тот же математический механизм, а алгоритм AdaBoost используется для решения проблемы аппроксимации в модели CSSE. В модели CSSE алгоритм AdaBoost используется в обоих процессах (как в CSSAw, так и в CSSF), что эффективно снижает сложность модели CSSE. Механизм работы модели CSSE показан на рис. 5. В дополнение, подмодель CSSAs модели CSSE, которая фиксирует индекс системы оценки кибербезопасности, разработана эталонным методом [13]. Полная модель CSSE показана на рис. 6.

Таким образом, у интегральной модели CSSE есть две примечательные особенности: 1) в реализации проекта одинаковый механизм CSSAw и CSSF, используемый в модели CSSE, может упростить модель структуры и улучшить эффективность алгоритма; 2) может быть построена законченная структура из последовательностей CSSAw, CSSAs и CSSF.

Теоретические основы модели оценки кибербезобасности

В целях соответствия модели CSSE требованиям по «точности», «работе в реальном времени» и «интеллектуальности», для аппроксимирующей функции используется алгоритм AdaBoost, являющийся ключевым моментом работы модели CSSE.

***a.* Точность**

Модель CSSE может определить, есть ли угрозы кибербезопасности в текущей области мониторинга, и спрогнозировать тенденцию возникновения угрозы кибербезопасности в будущем. Преимущество алгоритма AdaBoost состоит в непрерывном обучении на ошибках больших выборок, которое улучшает точность аппроксимирующей функции.

***b.* Работа в реальном времени**

Модель CSSE может завершить анализ данных и обработки данных в течение короткого времени. В качестве самообучающейся машины слабого уровня алгоритма AdaBoost выбран метод CVM (Core Vector Mashine), который может значительно снизить трудоёмкость и сложность вычислений.

***c.* Интеллектуальность**

Все задействованные алгоритмы в модели CSSE имеют теоретическое обоснование искусственного интеллекта и позволяют полностью автоматизировать работу после предварительной настройки рабочих параметров.

Алгоритм AdaBoost описывается следующим образом. Во-первых, слабая обучающаяся машина проводит многократную последовательную прогонку данных для получения последовательности базовых классификаторов. Во-вторых, после получения своих «весов» все базовые классификаторы представляют собой сильную обучающуюся машину. В-третьих, сильная обучающаяся машина используется для завершения всех расчётов [19, 20]. Наиболее важной особенностью алгоритма AdaBoost является то, что в процессе обучения подготовка каждой следующей выборки производится в соответствии с ошибками классификации предыдущих выборок. Рис. 7 представляет собой схему алгоритма AdaBoost.

В алгоритме AdaBoost сильная конечная обучающаяся машина получается обучением слабой машины. Поэтому выбор самой слабой обучающейся машины напрямую повлияет на производительность алгоритма AdaBoost. В модели CSSE слабой обучающейся машиной является CVM. Метод CVM – это улучшение метода опорных векторов (support vector mashine, SVM). Улучшение состоит в том, что вместо квадратичного программирования в SVM [21, 22], применяется минимальная ограничивающая сфера (minimum en-

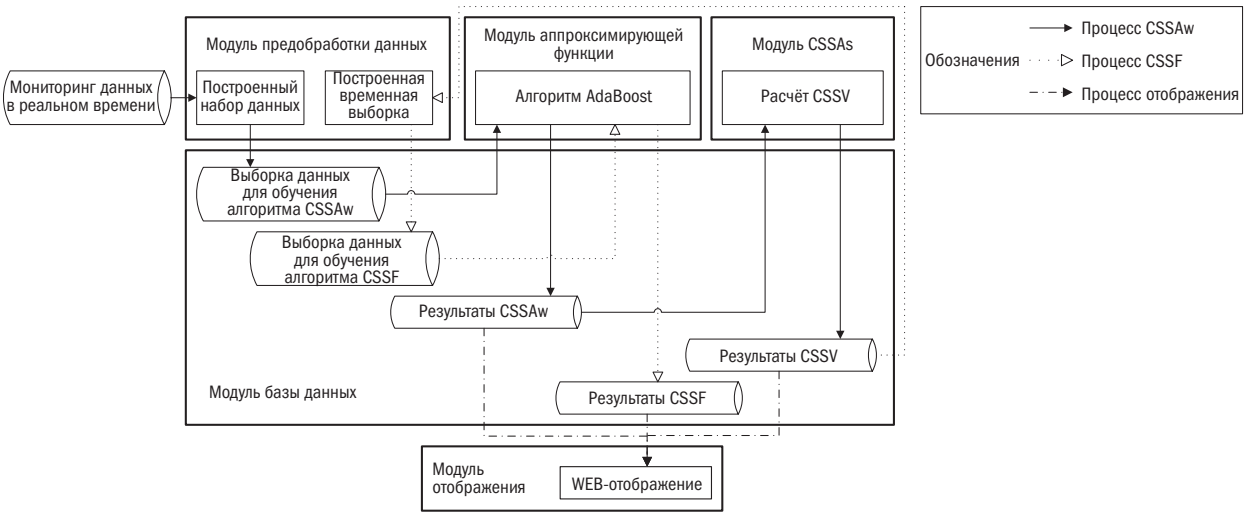


Рис. 6. Интегральная структура модели CSSE

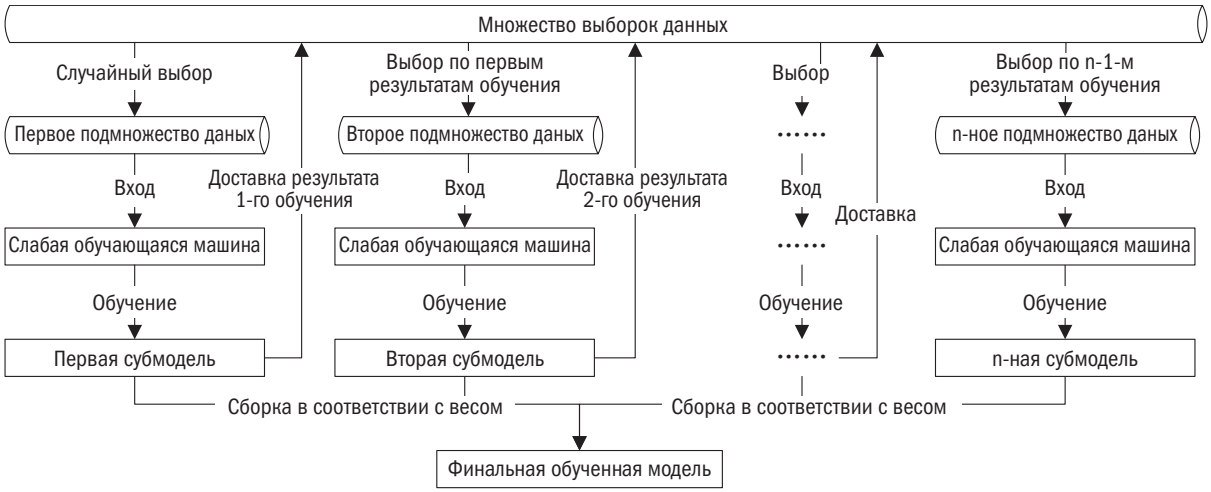


Рис. 7. Рабочий процесс алгоритма Ada–boosting

closing ball, MEB). Если в выборке есть n образцов, то временная сложность метода CVM составляет O(n), а пространственная сложность CVM не зависит от n. Тем не менее временная сложность SVM составляет O(n^3), а пространственная сложность CVM составляет O(n^2). Метод CVM, очевидно, имеет большое преимущество в скорости для данных CSSE.

Рабочий процесс модели CSSE, основанный на алгоритме AdaBoost

Рабочий процесс CSSAw

Модель CSSAw, основанная на алгоритме AdaBoost, включает в себя три фазы: «предварительная обработка данных», «автономное обучение» и «онлайн-работа».

Фаза I: «Предварительная обработка данных».

a. Сбор данных. Собираются все данные в режиме реального времени в области мониторинга с датчиков, которые будут служить в качестве источников данных CSSAw.

b. Построение набора данных. Объединяются данные $x^i_1, x^i_2, ..., x^i_n$ для параметров $x_1, x_2, ..., x_n$ с результатом CSSAw y^i в каждой точке времени i для построения набора данных D для CVM.

Фаза II: «автономное обучение».

Для того чтобы получить подмодель CSSAw с высокой точностью, набор данных D обучается по алгоритму AdaBoost.

c. Устанавливается максимальное число интеграций T для алгоритма AdaBoost и параметры обучения по умолчанию для CVM.

d. Стандартизируется набор данных D и устанавливается ω_1 (l) в качестве начального значения каждой выборки D, $\omega_1(l) = 1/m$, $l \in [1, ..., m]$, где m – общее количество выборок в D.

e. Строится подвыборка D_f из первых 50 % максимальных ω_f (l) в распределении D. Получается базовый классификатор h_f из подвыборки D_f от CVM, $f \in [1, ..., T]$.

На шаге e выбирается условие ω_f (l), при котором результат CSSAw (полученный h_f) не соответствует действительности. Если условие выполняется, ω_f (l) является результатом; в противном случае ω_f (l) =0.

f. Рассчитывается ошибка классификации ε_f для классификатора h_f по формуле (1), $f \in [1, ..., m]$, ω_f (l) есть выбор вероятности:

$$\varepsilon_f = \sum_{l=1}^{m} \omega_f(l) \qquad (1)$$

g. Рассчитывается вес α_f для h_f, по формуле (2).

$$\alpha_f = \frac{1}{2}\ln\frac{1-\varepsilon_f}{\varepsilon_f} \qquad (2)$$

h. Обновляется вес выборки D, по формуле (3).

$$\omega_{f+1}(l) = \frac{\omega_f(l)e^{-\alpha_f h_f(x_l)}}{M_f} \qquad (3)$$

В формуле (3) $\omega_{f+1}(l)$ – новый вес, $\omega_f(l)$ – старое значение веса выборки, h_f (x_l) – результат CSSAw для входных данных x_l от CVM, M_f – коэффициент нормализации, который приводится в формуле (4).

$$\sum_{l=1}^{m} \omega_{f+1}(l) = 1 \qquad (4)$$

i. После выполнения любого из следующих условий происходит переход к шагу j, в обратном случае – возвращение к шагу e:

Условие 1: Алгоритм AdaBoost достигает максимального числа итераций T.

Условие 2: Значение показателя $\omega_f(l)$ не изменяется.

j. Выходной результат (сильный классификатор) H рассчитывается по формуле (5), где *sign* – кусочно-линейная-функция.

$$H = sign\left[\sum_{f=1}^{T} \alpha_f h_f(x)\right] \qquad (5)$$

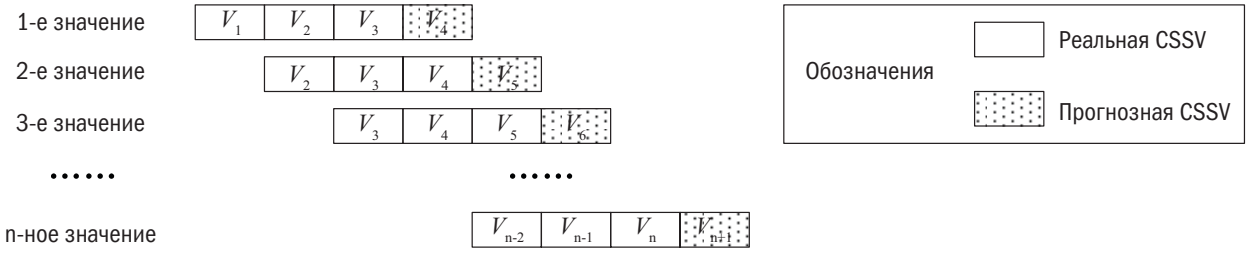


Рис. 8. Сборка обучающей выборки при помощи скользящего временного окна

Фаза III: «онлайн работа».

k. Ввод данных мониторинга в реальном времени $x_1, x_2, ... x_n$ для сильного классификатора *H*.

l. Использование сильного классификатора *H* для CSSAw в режиме реального времени.

Рабочий процесс CSSF

Модель CSSF, основанная на алгоритме AdaBoost, включает в себя те же три фазы – «предварительная обработка данных», «автономное обучение» и «онлайн-работа», но между CSSF и CSSAw существуют различия в «предварительной обработке данных».

Фаза I: «предварительная обработка данных».

Все значения дискретных точек времени CSSV V_i объединяются во временные ряды $S=\{V_1, V_2, ..., V_i\}$ с применением скользящего окна. Устанавливается размер скользящего окна, равный 4, и шаг, равный 1, как показано на рис. 8. Для каждой выборки CSSF выходным является последнее значение, а остальные значения являются входом.

Фаза II: «автономное обучение».

Поскольку алгоритм AdaBoost вызывается последовательно, как и в модели CSSE, все шаги данной фазы (за исключением шага *e*) согласуются с шагом в CSSAw. За исключением шага *e* CSSF, $\omega_f(l)$ определяется по формуле (6).

(a) Домашняя страница ISS

(b) Сеть филиалов

(c) Пограничные угрозы

(d) Страница «глубокого» анализа

Рис. 9. Графический интерфейс ISS

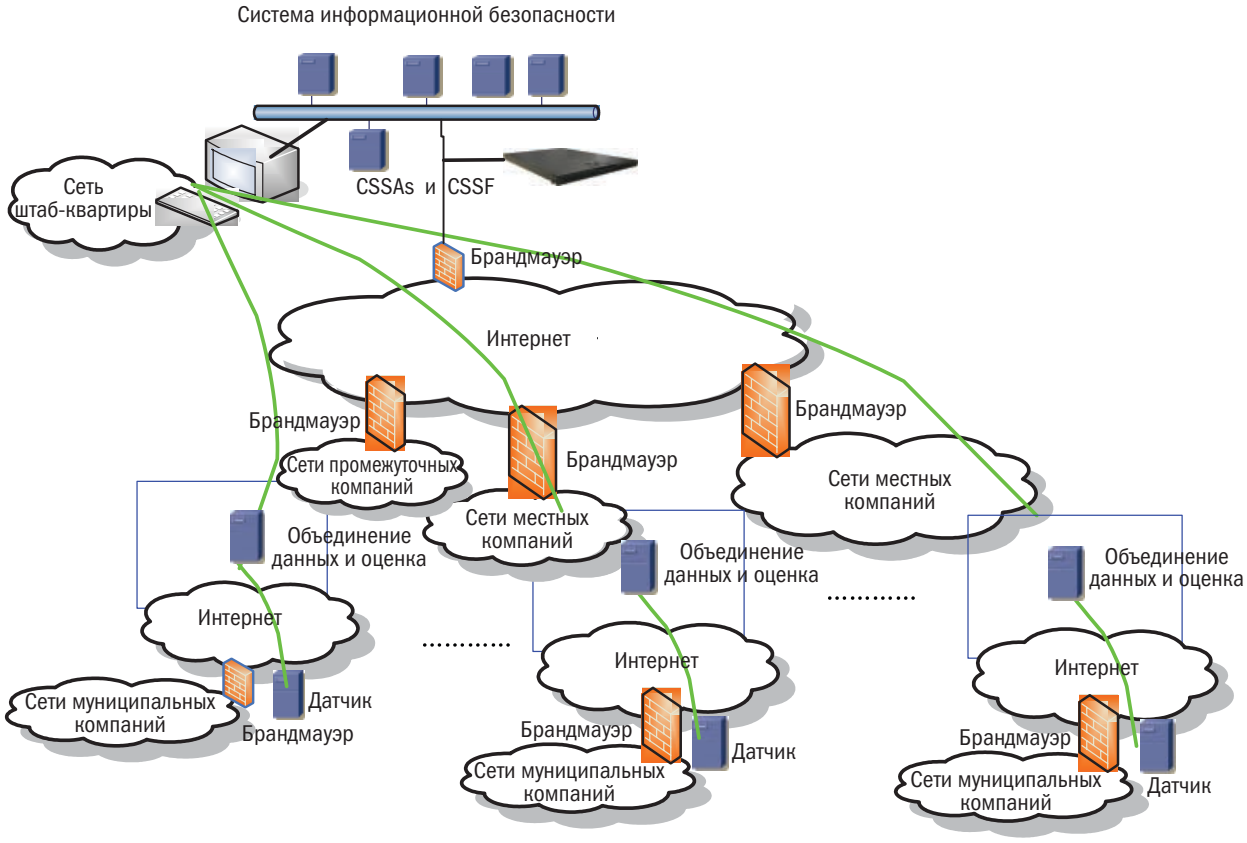


Рис. 10. Структура ISS

$$\frac{\left|\hat{V}_{i+4} - V_{i+4}\right|}{V_{i+4}} \geq 15\% \qquad (6)$$

Если данное условие выполняется, то $\omega_f(l)$ является его результатом, в противном случае $\omega_f(l) = 0$. В формуле (6) V_{i+4} является прогнозным значением CSSV, 15% – это текущий порог ошибок CSSF.

Фаза III: «онлайн-работа/обработка».

Для получения прогноза CSSV архивные данные CSSV служат входными данными для модели CSSF.

Практическое применение метода оценки кибербезопасности в интеллектуальных сетях

Обзор информационной системы мониторинга сетевой безопасности

На основе технологического проекта 2010 «Изучение системы мониторинга кибербезопасности» (The Study of cybersecurity monitoring system) была разработана Система мониторинга информационной безопасности сети (ISS) Государственной электросетевой корпорации Китая (SGCC). Система может в режиме реального времени опознавать киберугрозы Интернет-границам SGCC и более 40 её дочерних компаний, и эффективно улучшать их устойчивость против кибератак. В ISS была развёрнута модель CSSE, основанная на вышеупомянутом алгоритме AdaBoost,.

ISS стала одним из самых важных технических средств защиты SGCC. Основные графические интерфейсы показаны на рис. 9.

Структура развёрнутой ISS

Компоненты ISS развёрнуты на двух уровнях: в штаб-квартире SGCC и её филиалах. Подсистема CSSAw внедрена в каждом филиале, результаты CSSAw передаются в модель углублённого анализа головного сервера в штаб-квартиру SGCC для получения макро-CSSAs и CSSF, как показано на рис. 10.

1. Датчики установлены на Интернет-границах каждого филиала в виде зеркалирующего байпаса и выполняют следующую работу в режиме реального времени:
   - *a.* Объединяют события нарушения границ Интернет-пространства.
   - *b.* Анализируют и определяют сетевой трафик, а также генерируют предупреждения.
2. Узлы аггрегации и подсистемы CSSAw установлены в филиалах и выполняют следующие задачи:
   - *a.* Суммирование и передача всех видов событий кибератак, обнаруженных датчиками;
   - *b.* Выполнение процедуры CSSAw каждого филиала.
3. Установленный в филиалах SGCC серверный кластер анализирует в режиме реального времени результаты CSSAw и события возникновения угроз во всех филиалах, путём выполнения следующих функций:

a. Анализ возникновения угроз нарушения границ Интернет-пространства в режиме реального времени.

b. Анализ сетевого трафика.

c. Анализ и отображение данных отчётов о киберугрозах.

d. Оценка и отображение состояния кибербезопасности в режиме реального времени для всей GSCC.

e. Прогноз возникновения киберугроз в будущем.

Архитектура ПО ISS

Иерархически (снизу вверх) архитектура программного обеспечения ISS состоит из трёх уровней – сбора, анализа и представления, как это показано на рис. 11. Уровень сбора отвечает за сбор данных с датчиков. После фильтрации на этом уровне собранные данные передаются на уровень анализа, где они централизованно хранятся и анализируются, чтобы извлечь максимум полезной информации. Кроме того, на уровне анализа завершаются процессы CSSAw, CSSAs и CSSF. Уровень представления обеспечивает человеко-машинный интерфейс взаимодействия, отображает результаты анализа администраторам и принимает команды от администраторов кибербезопасности.

Выводы

Для решения проблем кибербезопасности, с которыми сталкиваются при построении интеллектуальных сетей, предложен и реализован новый метод оценки кибербезопасности на основе алгоритма AdaBoost, используемый в активной системе защиты от киберугроз.

CSSE может показывать в режиме реального времени угрозы кибербезопасности всех типов сетевых атак на микроуровне, информировать об атаках на макроуровне и прогнозировать будущие угрозы на глобальном уровне. В документе в первую очередь анализируется математическая составляющая процессов CSSAw и CSSF, и показывается, что они оба могут быть интерпретированы аппроксимирующими функциями, с дальнейшей разработкой интегральной модели CSSE. По сравнению с другими существующими моделями CSSE, метод имеет очевидные преимущества: во-первых, CSSAw и CSSF реализованы с помощью функций аппроксимации, что эффективно упрощает структуру модели; во-вторых, CSSAw и CSSF связаны последовательно с системой оценки кибербезопасности, которая основана на кластерном анализе для построения полного процесса CSSE.

Кроме того, для обеспечения точности и быстродействия CSSE, а также для увеличения интеллектуальности модели CSSE и сокращения участия человека модель CSSE использует в качестве аппроксимирующей функции алгоритм AdaBoost, использующий CVM в качестве слабой обучающейся машины. С одной стороны, алгоритм AdaBoost может улучшить точность аппроксимирующей функции путём расчёта ошибки для выборки, повышающей качество обучения; а с другой стороны, слабый алгоритм обучения CVM может значительно снизить трудоёмкость и сложность расчётов, а также повысить эффективность и быстроту вычисления модели CSSE. Все виды интеллектуальных

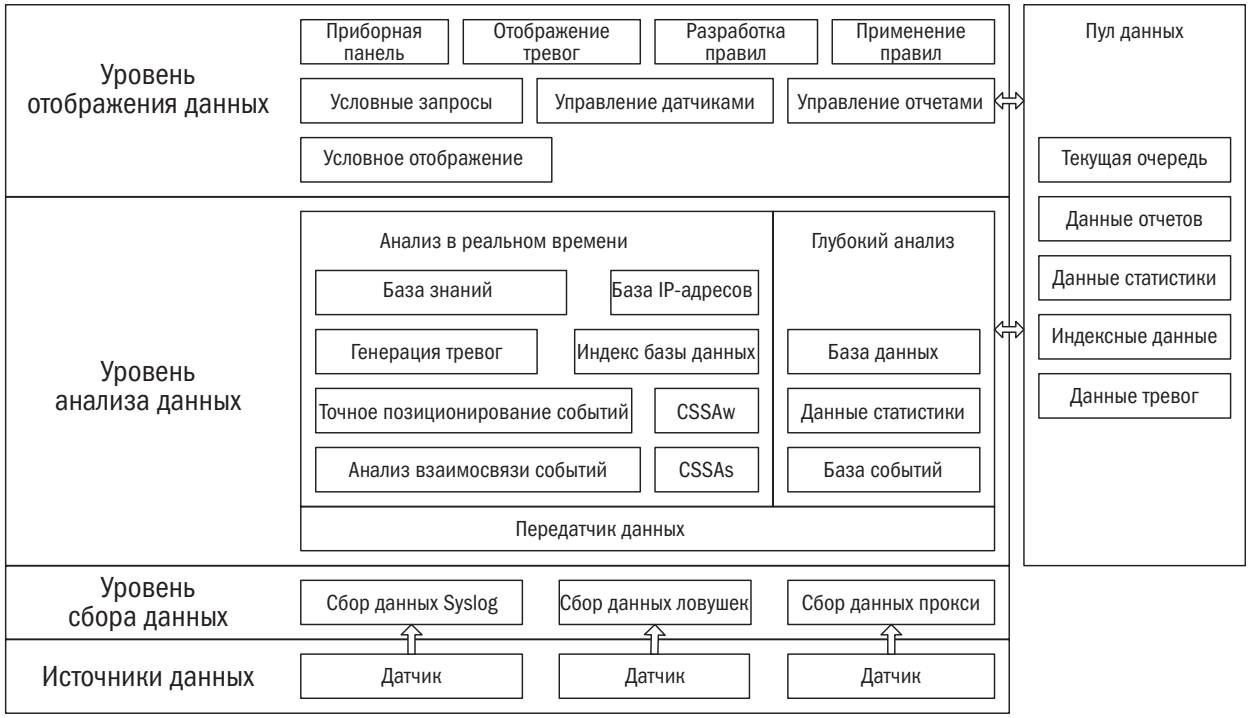


Рис. 11. Архитектура ПО ISS

алгоритмов, применяемых в модели CSSE, основаны на теории искусственного интеллекта, и можно добиться полной автоматической работы после предварительной настройки рабочих параметров.

Модель CSSE была реализована в системе мониторинга безопасности информационной сети SGCC для раннего предупреждения о возможных кибератаках, система работала стабильно на протяжении более трёх лет и сыграла важную роль в управлении рисками в киберпространстве.

Литература

1. Ernest Foo, Mark Branagan, Thomas Morris, «A proposed australian industrial control system security curriculum»[A], the 46th Hawaii International Conference on System Sciences (HICSS)[C], pp.1754–1762, 2013.

2. Piggin R.S.H. «Development of industrial cyber security standards: IEC 62443 for SCADA and industrial control system security»[A], IET Conference on Control and Automation 2013: Uniting Problems and Solutions, pp. 1–6, 2013.

3. Zhao Junhua, Wen Fushuan, Xue Yu-sheng, et al. «Cyber physical power systems: architecture, implementation techniques and challenges»[J], Automation of Electric Power Systems, vol. 34, no. 15, pp.1–7, 2010 (in Chinese).

4. Yu Yong, Lin Weimin, «General frameworks for the safety protection of the information system of power systems» [J], Netinfo Security, no. 9, pp.58–60, 2005 (in Chinese).

5. R. Dharam, S.G. Shiva, «Runtime monitors to detect and prevent union query based SQL injection attacks» [A], 10th International Conference on Information Technology [C], pp. 357–362, 2013.

6. Liu Lanchao, M. Esmalifalak, Han Zhu, «Detection of false data injection in power gridexploiting low rank and sparsity» [A], IEEE International Conference on Communications (ICC), pp. 4461–4465, 2013.

7. G. Jakobson, «Mission cyber security situation assessment using impact dependency graphs» [A], Proceeding of the 14th International Conference on Information Fusion (FUSION), pp.1–8, 2011.

8. Chen Xiuzhen, Zheng Qinghua, Guan Xiaohong. «Quantitative hierarchical threat evaluation model for network security» [J], Journal of Software, vol. 17, no. 4, pp.885–897, 2006 (in Chinese).

Xu Ruzhi, WANG Yufei. «A study on electric power information network-oriented security situation awareness,» Power System Technology, vol. 37, no. 1, pp. 53–57, 2013 (in Chinese).

9. Wang Yufei, Zhao Ting, Li Shaoyu, et al. «An intrusion detection method for electric power information network based on improved minimum enclosing ball vector machine» [J], Power System Technology, vol. 37, no. 9, pp. 2675–2680, 2013 (in Chinese).

10. Wang Yufei, Zhou Liang, Wang Jing. «Intrusion Detection System of Electric Power Information Network Based on Improved Ball Vector Machine» [A], The 4th International Conference on Intelligent System Design and Engineering Applications (ISDEA 4th) [C], pp. 369–373, 2013.

Li Yuancheng, Wang Yufei. «A misuse intrusion detection model based on hybrid classifier algorithm», JDCTA: International Journal of Digital Content Technology and its Applications, vol. 6, no. 5, pp. 25–33, 2012.

11. Gao Kunlun,Xu Ruzhi,Wang Yufei. «A hierarchical network security situation evaluation system for electric power enterprise based on grey clustering analysis» [C]. IEEE Conference Computer Science and Service System (CSSS), pp. 1990–1995, 2011.

12. Wang Yufei, Wang Jing, Xu Zhibo, et al. «Assessing Cyber-threats Situation for Electric Power Information Network» [A], The 9th International Conference on Natural Computation (ICNC'13) [C], pp. 1505–1510, 2013.

13. Gao Kunlun, Liu Jianming, Xu Ruzhi, et al. «A hybrid security situation prediction model for information nerwork based on support vector machine and particle swarm optimization», Power System Technology, vol. 35, no. 4, pp. 176–182, 2011 (in Chinese).

14. Zhang Xiang, Hu Changzhen, Liu Shenghang, et al. «Research on network attack situation forecast technique based on support vector machine» [J]. Computer Engineering, vol. 11, no. 3,pp. 10–12, 2007 (in Chinese).

15. Endsley M R. «Design and evaluation for situation awareness enhancement» [A]. Paper presented at the Human Factors Society 32nd Annual Meeting [C]. Santa Monica, CA, pp. 7–11, 1988.

16. D.F Crouse, P. Willett, Y. Bar-Shalom, «A low-complexity sliding-window Kalman FIR smoother for discrete-time model» [J], IEEE Signal Processing Letters, vol. 17, no. 2, pp.1 77–180, 2010.

17. Mallapragada P-K, Jin R, Jain A-K. «Semiboost: boosting for semi-supervised learning» [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 31, no. 11, pp. 2000–2014, 2009.

18. Weiming Hu, Wei Hu, Steve Maybank. «Adaboost-based algorithm for network intrusion detection» [J]. IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 38, no. 2, pp. 577–583, 2008.

19. Tsang I W H, Kwok J T Y, Zurda J A. «Generalized core vector machines», IEEE Transactions on Neural Networks, vol.1 7, no. 5, pp. 1126–1140, 2006.

20. Chung Fulai, Deng Zhaohong, Wang Shitong. «From minimum enclosing ball to fast fuzzy inference system training on large datasets», IEEE Transactions on Fuzzy Systems, vol. 17, no. 1, pp. 173–184, 2009.

Источник: «Study and Practice of Cybersecurity Situation Evaluation Method for Smart Grid», труды CIGRE 2014, http : //www.cigre.org

А. Р. Вериго., А. А. Небера, Н. Г. Шубин , ЗАО «РТСофт»

«РТСофт» на 45–й сессии СИГРЭ

С 23 по 29 августа 2014 г. в Парижском Дворце конгрессов состоялась 45-я сессия (Сессия) Международного Совета по большим электрическим системам высокого напряжения (СИГРЭ). В Сессии приняли участие делегации более 90 стран, общее число делегатов составило более 3 300 человек. В состав российской делегации, насчитывающей более 130 участников, вошли представители ЗАО «РТСофт» (Компания) во главе с генеральным директором О. В. Синенко.

Основные тренды развития и вызовы мировой электроэнергетики

Общие тренды развития и вызовы мировой электроэнергетики были озвучены в докладах на церемонии открытия Сессии, состоявшейся 24 августа 2014 г., и на пленарном заседании под названием «Изменение условий функционирования энергосистем – региональные перспективы» 25 августа. К числу основных трендов и вызовов можно отнести следующие.

1. Ужесточение требований к надёжности и живучести энергосистем в условиях нарастающих планетарных климатических вызовов (землетрясения, наводнения, торнадо и ураганы, пожары, экстремальные температуры окружающей среды) при сохранении и наращивании физической и экономической доступности электроэнергии для населения мира.

2. Развитие и повышение роли микросетей (microgrids) в структуре распределительных электрических сетей. Причины: мобильность первичного развёртывания и свёртывания микросетей в случае значимого снижения спроса на электроэнергию или других ситуаций, приводящих к потере их экономической эффективности, восстановления после аварий; относительная независимость от внешних условий и возмущений; создание эластичности спроса на электроэнергию и повышение энергоэффективности, обеспечиваемые за счёт разноплановой внутренней генерации. Микросети, включающие в свой состав возобновляемые источники энергии (ВИЭ), топливные элементы и утилизационные технологии наряду с традиционной малой генерацией на органическом топливе, способны снижать потребность в завозе и в запасах органического топлива на 25–75 %.

3. Развитие технологий постоянного тока (ПТ), включающих силовую электронику, постоянно развивающееся на её основе множество устройств активного управления режимами электроэнергетических систем, управляющих систем и средств защиты. Создание локальных систем и вставок ПТ в сетях общего назначения и в микросетях; линий электропередачи ПТ для транспортировки электроэнергии на большие расстояния от экологически чистых и экономически выгодных ВИЭ в районы концентрации потребления.

4. Формирование специфической роли электромобилей и иных аккумулирующих энергию технологий с их двойным использованием: в качестве потребителей в часы минимума системного потребления электроэнергии и в качестве источников в часы пиковых нагрузок энергосистем.

5. Нарастание проблем, связанных с увеличением в энергобалансах регионов относительных объёмов ВИЭ, и развитие нейтрализующих эти проблемы технологий, в частности:

– нестабильности и ограниченной предсказуемости профилей производства электроэнергии ВИЭ во времени и, как следствие, необходимости создания продвинутых систем прогнозирования погодных условий и применения накопителей электроэнергии (НЭ);
– государственной финансовой поддержки ВИЭ, понижающей рыночную конкурентоспособность иных, на сегодняшний день более экономичных, источников энергии.

6. Дальнейшее укрупнение рынков электроэнергии и системных услуг Европы. В частности, включение в объединённый рынок электроэнергии европейских государств Испании; подготовка к подобному действию рынков Турции и других стран средиземноморья.

7. Потребность в быстрой адаптации нормативно-технической базы электроэнергетики к быстро меняющимся условиям. Например, в связи с резким увеличением мощностей использования ВИЭ необходимо оперативное изменение рыночных механизмов, стимулирующих активность участников рынка электроэнергии в направлении оказания системных услуг по управлению режимом энергосистемы.

Активность ЗАО «Ртсофт»

Как показала очередная Сессия, современный этап развития мировой электроэнергетики характерен сложными, неоднозначными явлениями и процессами. Например, избыточное внимание и государственная поддержка строительства ВИЭ, проявлявшиеся в последние годы, во многих странах привели к слишком быстрому изменению структуры балансов мощности, не подкреплённому соответствующими возможностями информационно-аналитических систем и технических средств управления энергосистемами. В результате возникли новые технологические вызовы-проблемы, разрешение которых потребовало ускоренного инвестирования в развитие систем НЭ, быстродействующей силовой электроники и интеллектуальных управляющих автоматических систем. В связи с этим в очередной раз была подтверждена истина, заключающаяся в том, что оптимальное развитие энергосистем требует динамичного системного подхода.

По этой причине в сфере внимания ЗАО «РТСофт» находится работа практически всех важнейших исследовательских комитетов СИГРЭ, занимающихся оперативным и противоаварийным управлением, релейной защитой и автоматикой, синхронизированными измерениями, рынками энергии и системных услуг. Компания является последовательным приверженцем системного подхода к развитию электроэнергетических технологий и именно в этом ключе принимает активное участие в развитии информационно-коммуникационной инфраструктуры электроэнергетики.

В частности, ЗАО «РТСофт» и Российский Национальный Комитет (РНК) СИГРЭ заключили соглашение о создании на базе «РТСофт» российского подкомитета D2 «Информационные системы и телекоммуникации» в области электроэнергетики. В соответствии с этим соглашением Компания получила статус «Ведущий научно-технический партнёр РНК СИГРЭ». Руководителем подкомитета D2 РНК СИГРЭ назначена Синенко Ольга Викторовна, генеральный директор ЗАО «РТСофт», доктор технических наук, действительный член АИН РФ им. Прохорова, член Президиума РНК СИГРЭ. На базе и при поддержке ЗАО «РТСофт» будут решаться следующие задачи.

1. Координация и мониторинг научно-технической активности индивидуальных и коллективных членов РНК СИГРЭ по тематике D2, разработка и реализация планов научно-технической деятельности РНК СИГРЭ в части тематического направления D2 под руководством технического комитета РНК СИГРЭ.

2. Организация коммуникаций в российском профессиональном электроэнергетическом сообществе для формирования независимых экспертных мнений, выработки позиций по актуальным научно-техническим вопросам и проблемам развития отечественной электроэнергетики, которые необходимо знать и учитывать в инвестиционной политике, бизнесе, стратегическом планировании, нормативно-техническом регулировании, производственной и проектной деятельности как объективные научно-технические или технологические ограничения.

3. Представительство российского профессионального энергетического сообщества в работе исследовательского комитета D2, формирование и усиление авторитета российских учёных, специалистов, экспертов в международном научно-техническом обмене по линии СИГРЭ.

В область деятельности Подкомитета D2 РНК СИГРЭ входят следующие направления.

1. Информационно-управляющие системы в электроэнергетике:

– развитие архитектур оперативно-технологического управления, разработка методов создания типовых архитектур для различных уровней иерархии управления в энергетике;
– создание автоматизированных систем технологического управления (АСТУ) для электросетевых компаний (ЭСК);

– развитие систем автоматизированного управления для новых электросетевых устройств (FACTS, АСК, ВПТ, ВИЭ, АББМ) на основе векторных измерений параметров электрического режима;
– оценка и планирование надёжности электроснабжения и качества электроэнергии в многоуровневых системах автоматизированного управления;
– мультиагентные системы мониторинга состояния и технологического управления в энергетике;
– обеспечение ситуационного управления технологическими процессами в ЭСК (в том числе во время масштабных технологических нарушений);
– распределённые информационные системы управления для мобильного применения.

2. Совершенствование сетей связи и телекоммуникации для приложений в электроэнергетике:
– обобщение и анализ опыта внедрения и использования современных систем связи и телекоммуникаций в автоматизированных системах управления;
– развитие систем технологической связи в энергетике для оперативных и неоперативных приложений;
– эволюция телекоммуникационных технологий и внедрение новых сетевых архитектур передачи информации;
– методы и протоколы передачи информации;
– совершенствование телекоммуникации для цифровых подстанций;
– технологии передачи данных (по ЛЭП, с использованием пакетной передачи и специализированных протоколов связи, связь для систем противоаварийной автоматики и РЗА, телеуправление, речь, данные, видео);
– решения «последней мили» для организации связи в сетях Smart Meters;
– применение беспроводных каналов связи для систем передачи информации (в том числе радиорелейных и GSM) в энергетике.

3. Развитие сетей Smart grid и Microgrids, технологии Smart Meters & Meter Data Management:
– интеграция автоматизированных SCADA-систем, систем учёта электроэнергии, мониторинга и управления качеством электроэнергии в единый информационно-управляющий комплекс;
– создание систем технологического управления для распределённой генерации;
– системы управления спросом на розничных рынках электроэнергии на основе решений Smart Meters;
– организация управления электросетевыми объектами в сетях Smart grid, создание систем автоматического восстановления электроснабжения;
– оценка эффективности создания Микросетей (microgrids) и определение оптимальных сроков их эксплуатации в устоявшихся структурах распределительных сетей.

4. Обеспечение информационной безопасности (ИБ) для систем связи и управления в электроэнергетике;
– оценка рисков ИБ, определение надлежащих границ безопасности для новых архитектур и систем автоматизированного управления, разработка общих моделей угроз;
– развитие приложений ИБ для сетей Smart grid;
– совершенствование требований законодательства по ИБ для систем управления в электроэнергетике;
– требования безопасности для дистанционного управления автоматизированными объектами;
– ИБ в использовании мобильных технологий для оперативно-технологического управления;
– изучение международных стандартов ИБ и оценка их применимости для электроэнергетики.

5. Эксплуатация информационных и телекоммуникационных систем и сервисов:
– управление активами и мониторинг состояния сетей и систем связи и телекоммуникации;
– мониторинг и анализ состояния систем вторичного оборудования на объектах управления;
– управление информационными потоками, обеспечение целостности данных, качество связи и производительность сети передачи данных;
– инструменты управления отказами и инцидентами, системы ведения информации для этих инструментов;
– организация эксплуатации информационных и телекоммуникационных систем, оценка эффективности аутсорсинга в эксплуатации;
– эффективные экономические модели эксплуатации информационных и телекоммуникационных систем.

Другим направлением конкретного приложения сил Компании является участие её экспертов в работе международной рабочей группы (РГ) СИГРЭ C6.30, исследующей влияние систем накопления энергии на аккумуляторных батареях (АББМ – аккумуляторные батареи большой мощности) на распределённые электрические сети (The Impact of Battery Energy Storage Systems on Distribution Networks).

Системы накопления электроэнергии становятся принципиально новым элементом электроэнергетических систем, обеспечивающих их стабильную работу в условиях широкого внедрения источников распределённой генерации, в том числе непредсказуемых и нестабильных по производительности ВИЭ. В течение ближайших лет РГ C6.30 будет изучать и анализировать международный опыт использования АББМ в распределительных электрических сетях для получения глубокого понимания таких вопросов, как:

– влияние АББМ на качество электроэнергии и надёжность функционирования сети;
– возможности одновременного использования различных технологий накопления энергии в одной и той же сети;
– использование возможностей АББМ для интеграции в распределительные сети ВИЭ;
– возможности адаптивных стратегий управления режимом сети в зависимости от текущих, в том числе локальных, режимных параметров сети (напряжение, частота, токи) и времени;
– способности существующих аккумуляторов, инверторов и систем управления АББМ к участию в работе автоматических систем режимного и противоаварийного управления, а также послеаварийного восстановления функционирования сети.

Заключение

Организация работы в рамках СИГРЭ носит волонтёрский характер, тем не менее руководители исследовательских комитетов и подкомитетов, международных рабочих групп, как правило, не испытывают затруднений в формировании творческих коллективов. По каким-то, на первый взгляд, не вполне понятным причинам большое количество специалистов по всему миру, в том числе делегированных коммерческими компаниями, выполняют большой безвозмездный труд. Объясняется этот феномен, вероятно, тем, что в обмен на время и опыт специалисты получают доступ к широкому перечню проблем мировой энергетики. Проблемы – обильная пища для ума, способствующая росту и интеллектуальной капитализации профессионалов. В то же время желательно, чтобы количество указанных проблем не умножалось в результате стихийных или плохо продуманных действий. СИГРЭ – влиятельный международный орган, его труды фактически формируют новые тренды в мировой электроэнергетике. От качества работы исследовательских подразделений СИГРЭ зависит цена, которую Цивилизация заплатит за будущую обеспеченность энергией.

В завершение, учитывая сказанное выше, ЗАО «РТСофт» приглашает всех заинтересованных лиц и компании к творческому сотрудничеству по предметам деятельности исследовательского подкомитета РНК СИГРЭ D2 и международной рабочей группы C6.30.

Новости рынка

«РТСофт» и «Россети» договорились о сотрудничестве в области электроэнергетики

ЗАО «РТСофт» и ОАО «Россети» подписали соглашение о сотрудничестве в области развития автоматизированных систем технологического управления электрическими сетями для ОАО «Россети».

Соглашением закреплены намерения сторон в области развития автоматизированных систем технологического управления электрическими сетями, содействия внедрению инновационных технологий и решений, направленных на повышение эффективности, надёжности и безопасности электросетевой инфраструктуры ОАО «Россети».

Документ подписан в ходе Международного электроэнергетического форума RuGrids-Electro, проходившего с 15 по 17 октября 2014 года в Москве. Подписи под документом поставили генеральный директор ЗАО «РТСофт» Ольга Синенко и первый заместитель генерального директора по технической политике ОАО «Россети» Роман Бердников.

«Основной аспект этого соглашения – эффективное взаимодействие в области оперативно-технологического и производственно-технического управления, внедрение инновационных технологий, обеспечивающих подвижность и гибкость построения и эксплуатации систем технологического управления, – отметила Ольга Синенко. – Компания «РТСофт» считает своей первоочередной задачей создание на базе существующего подкомитета D2 РНК СИГРЭ российской ассоциации производителей и разработчиков систем АСТУ. Это позволит реализовать новую концепцию перспективного развития АСТУ для «Россетей» и обеспечить решение вопросов взаимодействия российских и зарубежных разработчиков в рамках создания единых стандартов системы».

Источник: Пресс-служба ЗАО «РТСофт»