Занимаясь любимым делом добиться успеха можно всегда. Тем более, когда у вас есть желание и лучший инструмент.

Александр Ковалев, «РТ-Софт»

VPX - лучший инструмент для создания встраиваемых суперкомпьютеров класса HPEC

- Открытый международный стандарт
- Длительный жизненный цикл до 20 лет и более
- Процессорно-независимая архитектура
- Возможность создания систем высшей производительности, в том числе многоядерных и многомашинных
- Высокопроизводительные коммуникационные технологии 10/40/100 GEthernet, PCI Express, Serial RapidIO, InfiniBand
- Исполнение с кондуктивным и воздушным охлаждениями
- Максимальная надежность и соответствие жестким эксплуатационным требованиям
- Самый широкий выбор ОС: Linux, VxWorks, LynxOS, QNX и др.
- Профессиональная поддержка «РТСофт» на всем жизненном цикле систем

RTSoft

105037, Москва, Никитинская 3, ЗАО «РТСофт». Тел.: (495) 967-1505. Факс: (495) 742-6829. e-mail: rtsoft@rtsoft.ru www.rtsoft.ru

OpenSystems Publishing

МКА : ВКС

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

В НОМЕРЕ

CONTENTS

ОБЩИЙ ВЗГЛЯД

Многогранный «Интернет вещей»
Павел Литвинов, ЗАО «РТСофт» — 4

BIRD'S EYE VIEW

Multifaceted Internet of Things
by Pavel Litvinov, RTSoft

ВСТРАИВАЕМЫЕ КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ

Industry 4.0 – немецкий «Интернет вещей» и Kontron – его лидер
Норберт Хаузер (Nobert Hauser), Kontron — 12

Открытые технологические платформы как глобальный тренд в области разработки систем специального назначения
Виктор Синенко, ЗАО «РТСофт» — 15

Расширенная модель сенсоров в спецификации PICMG 3.7
Сергей Жуков, Игорь Починок, Auriga, Inc., НИВЦ МГУ — 19

«Интернет вещей» – основная тенденция выставки SPS IPC Drives 2014
Анна Нестерова, Юрий Якшин, ЗАО «РТСофт» — 24

«РТСофт» и Intel провели совместный семинар и открыли лабораторию по «Интернету вещей»
Леонид Акиншин — 27

EMBEDDED COMPUTER TECHNOLOGIES

Industry 4.0 – The German IoT and Kontron – Its Leader
by Nobert Hauser, Kontron

Open Technical Platforms as Global Trend in Special Purpose System Development
by Victor Sinenko, RTSoft

Extended Sensor Model in PICMG 3.7 Spec
by Segey Zhukov and Igor Pochinok, Auriga, Inc., MSU RCC

Inernet of Things – Main Trend of SPS IPC Drives 2014 Exhibition
by Anna Nesterova and Jury Yakshin, RTSoft

RTSoft and Intel Carried Out Joint Workshop and Opened IoT Lab
by Leonid Akinshin

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Yocto Project: проблемы и возможности
Кристофер Халлинан (Christopher Hallinan), Mentor Graphics — 30

Процесс разработки медицинского программного обеспечения: краткий обзор требований стандарта IEC-62304
Айрат Садыков. Auriga, Inc. — 34

SOFTWARE

The Yocto Project: Challenges and Opportunities
by Christopher Halliman, Mentor Graphics

Medical Software Development Process: IEC-62304 Standard Requirements Brief Overview
by Ayrat Sadykov, Auriga, Inc.

ИУС ДЛЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ И ИНФРАСТРУКТУРНЫХ ОБЪЕКТОВ

INDUSTRIAL ENTERPRISE AND INFRASTRUCTURE IMSs

Некоторые подходы и технологии разработки современных ИУС с использованием отечественной инструментальной платформы PLATINUM-RT
Сергей Кирюхин, Алексей Ханыгин, Ринат Валеев, ЗАО «РТСофт»

41

PLATINUM-RT Russian Tool Platform for Actual Information Management System Development. Part 2: Some Practices and Techniques
by Sergey Kiryukhin, Alexey Khanygin and Rinat Valeev, RTSoft

ИУС ДЛЯ ЭЛЕКТРОЭНЕРГЕТИКИ

POWER INDUSTRY IMSs

Стандарт МЭК 61850: наука, практика, лирика
Леонид Орлов, Константин Сергеев ЗАО «РТСофт»

44

IEC 6850 Standard: Engineering, Practice and Lyric Poetry
by Leonid Orlov and Konstantin Sergeev, RTSoft

Кибербезопасность в энергетике. Состояние вопроса
Дженс Зербст (Jens Zerbst), Лиро Ринта Жуппи (Liro Rinta Jouppi), Джованна Дондосола (Giovanna Dondossola), Кристоф Пойриер (Christophe Poirier), Паскаль Ситбон (Pascal Sitbon), Деннис Хольстайн (Dennis Holstein), Джон Макдональд John (McDonald), Роберт Иванс (Robert Evans)

50

Status of Cybersecurity
by Jens Zerbst, Liro Rinta-Jouppi, Giovanna Dondossola, Christophe Poirier, Pascal Sitbon, Dennis Holstein, John McDonald, Robert Evans

Применение телекоммуникационных технологий PLC при подключении объектов распределённой генерации к электрическим сетям
Давид Гил (David Gil), Асиер Лано (Asier Llano), Фернандо Кастро (Fernando Castro), Хосе Антонио Морено (Jose Antonio Moreno), Соня Мартинес (Sonia Martinez),Txetxu Арсуага (Txetxu Arzuaga), ZIV CG Automation, Испания

59

Powerline Communications for Connecting Distributed Energy Resources
by David Gil, Asier Llano, Fernando Castro, Jose Antonio Moreno, Sonia Martinez, Txetxu Arzuaga, ZIV CG Automation, Spain

НОВОСТИ РЫНКА

29, 33, 43

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:

Зеленова Т. В. – *главный редактор*
Якшин Ю. Н. – *эксперт по направлению ВКТ*
Жданов А. А. – *эксперт по направлению ПО*
Ханыгин А. Н. – *эксперт по направлению АИУС ПП*
Небера А. А. – *эксперт по направлению АИУС Э.*
Иваничек А. С. – *отв. за рекламу и распространение*
Белов И. В – *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
№ 2 (2/29/47/106) 2015
Издаётся с 2007 (1995) года. Выходит 3 раза 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

Павел Литвинов, ЗАО «РТСофт»

Многогранный «Интернет вещей»

Трудно найти в наше время человека, ничего не слышавшего об «Интернете вещей» – Internet of Things (в иностранной литературе чаще всего используется акроним IoT, мы будем придерживаться русифицированной версии – ИВ). «Призрак» «Интернета вещей» бродит не только по Европе, в мировых средствах массовой информации говорят о грядущей технологической революции, которая затронет всех и изменит нашу жизнь в той же мере, как появление телевидения, персональных компьютеров или сети Интернет. Биржевая аналитика пестрит радужными прогнозами, появляются новые консорциумы по развитию и стандартизации ИВ, анонсируются новые продукты и услуги. Всё это происходит на фоне отсутствия единого мнения о том, что же такое ИВ и где его границы даже на уровне базовых определений. По мере движения от ядра – онтологии к периферии – прикладному использованию, представления расходятся сильнее и переплетаются всё причудливее, как круги на воде от брошенных камней. В настоящей статье автор попробует внести ясность в этот вопрос, путем взгляда на тематику ИВ с разных областей и под разными углами зрения. Преимуществом аналитического подхода к раскрытию темы является возможность, не навязывая субъективного мнения читателю, сформировать у него собственное представление на тему, что такое ИВ, и отношение к вопросу о его полезности и перспективах использования в самых широких областях: от частной жизни до бизнеса.

Предпосылки «Интернета вещей» M2M

Большинство источников сходятся во мнении, что непосредственным предшественником ИВ является концепция Machine-to-machine (M2M), которую образно называют «Интернетом машин». «Интернет вещей» включает в себя M2M и является дальнейшим технологическим развитием ранее заложенных идей и их маркетинговым переосмыслением. Парадигму Machine-to-machine можно представить как «сплав» возможностей, предоставляемых современными технологиями:

– беспроводные коммуникации;
– значительная вычислительная мощность в узлах, устройствах M2M;
– облачные сервисы и технологии.

Каждый из трёх компонентов вносит свой вклад в формирование ценности для потребителя и поставщика решений:

– *Беспроводные коммуникации* – существенное сокращение сроков проектирования и монтажа, возможность гибкой перенастройки, в том числе и на перспективные задачи.

– *Вычислительная мощность в узлах, устройствах M2M* позволяет на уровне датчиков и сенсоров использовать много недорогих устройств. От обработки «в центре» можно перейти к обработке «на месте». Движение от иерархических технологических систем и методов управления в сторону сетецентрических – также один из трендов.

– *Облачные сервисы и технологии* гарантируют максимальную гибкость и снижают не только стоимость владения, но и «порог» вхождения в новые решения.

Дополнительные блоки, которые легли в фундамент ИВ:

– низкая стоимость владения;
– минимальное энергопотребление;
– коммуникации и базовая функциональность, доступная «из коробки»;
– глобальная доступность устройств и сервисов.

На рис. 1 приведена точка зрения компании Beecham Research. Классы приложений группируются по секторам вертикальных рынков, а в каждом из них перечисляется возможное место применения и виды устройств.

Конвергенция технологии

Среди технологий будущего, которые уже меняют или изменят нашу жизнь и деловой ландшафт на ближайшие годы, наиболее часто называют следующие:

1. Искусственный интеллект и развитие робототехники (AI).

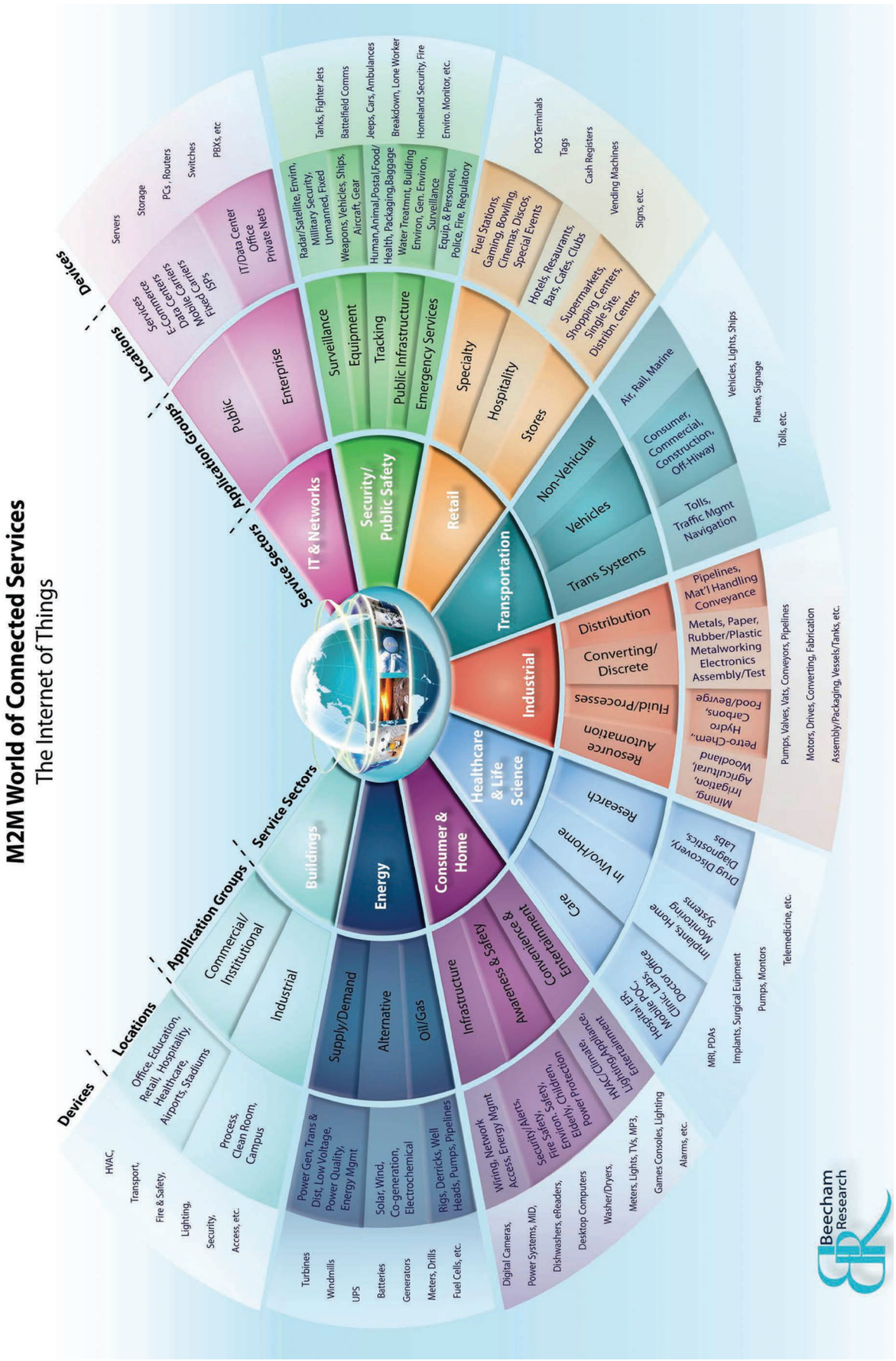


Рис. 1. Мир M2M и IOT по версии Beecham Research

2. Облачные технологии и сервисы (Cloud).

3. Большие данные (Big Data).

4. Интернет 3.0 (Web 3.0).

5. Аддитивные технологии (3D printing или additive manufacturing, AM).

Для первых четырёх технологий из этого списка «Интернет вещей» одновременно и движущая сила, и «бенефициар» их развития! Другими словами, ИВ в его современном понимании не существует без использования облачных сервисов, больших данных и возможностей по их интеллектуальной обработке. Новые потребительские качества и возможности появляются как сложный сплав современных трендов, причём верные пропорции для успеха найти непросто.

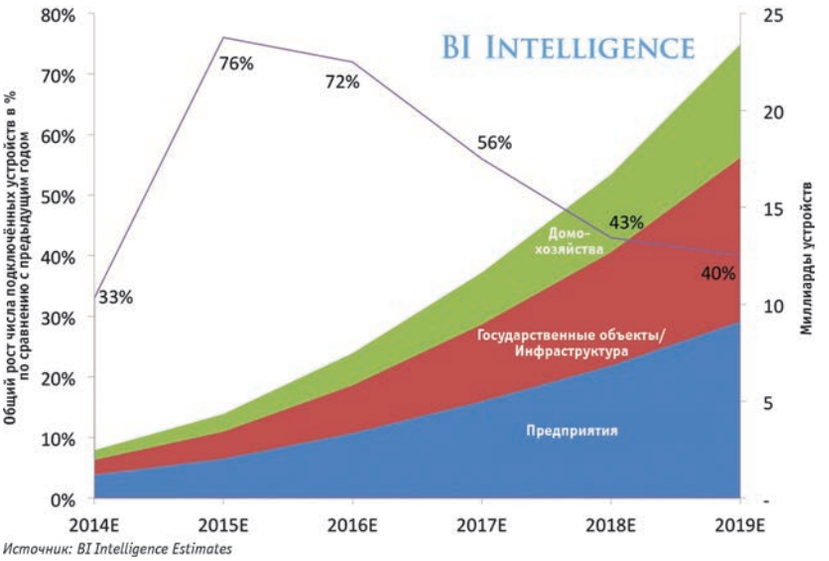


Рис. 2. Прогноз роста числа устройств в структуре секторов

Немного теории

Закон Меткалфа, первоначально сформулированный в 1980 году, гласит, что ценность телекоммуникационной сети пропорциональна квадрату числа подключённых пользователей системы. Уже тогда под пользователями понимались совместимые устройства, например факсимильные аппараты, телефоны и т. п. Закон отражает простой факт: количество уникальных соединений в сети с количеством узлов (n) описывается формулой n (n-1)/2. Разумеется, речь идёт о наиболее оптимистичной оценке полезности в силу объективных причин: несовместимости протоколов устройств или языкового барьера, если речь идёт о людях; захвата значительного числа ресурсов отдельными устройствами или группами пользователей, – и просто для больших значений (n) более правильной оценкой будет пропорциональность N*log(N). Но какие бы поправки мы не вносили, очевидно, что, когда счёт пойдёт на миллиарды подключённых устройств, потенциальная потребительская ценность такой сети будет огромной! (см. рис. 2).

Прогнозы

Каждый продукт, потенциально способный трансформировать мир или по крайней мере наше представление о нём, находясь на ранней стадии своего жизненного цикла, вызывает ожидания в отношении потенциальных преимуществ и волнения инвесторов. Ошибки в прогнозах, с какой скоростью ИВ будет завоёвывать рынок и какое займет на нём в результате место, могут иметь непредсказуемые и дорогостоящие последствия. Дальновидные организации должны уже сейчас думать о шагах, которые необходимо предпринять на протяжении всего жизненного цикла вновь предлагаемых продуктов и сервисов. Неопределённость усиливается тем фактором, что парадигма ИВ вмешивается не только в понимание, но и в сами процессы жизненного цикла. На рис. 3 отражена точка зрения компании IBM.

Изменения затронули не только количество стадий и их названия. Самым существенным отличием является то, что процессы, которые раньше выполнялись последовательно, теперь идут параллельно и зачастую одновременно.

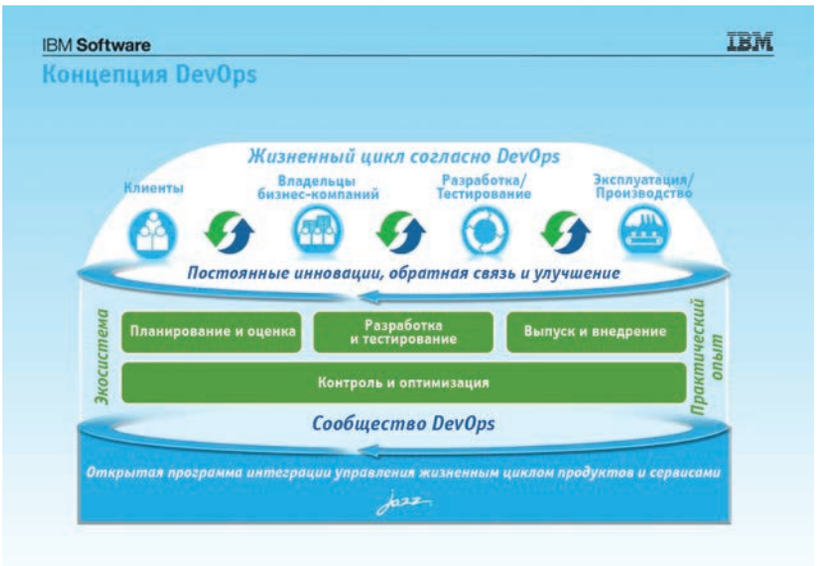


Рис. 3. Жизненный цикл продуктов и сервисов по версии IBM

Архитектура «Интернета вещей»

Референтная модель

Фундаментальными характеристиками «Интернета вещей» являются:

– **Взаимосвязанность.** Все устройства взаимодействуют через глобальную или локальную инфраструктуру информационного обмена.

– **Сервисы, ориентированные на устройства.** ИВ способен обеспечить семантическую согласованность между физическими объектами реального мира и их информационным представлением в виртуальном пространстве и объединить физические устройства с учётом правил и ограничений.

– **Гетерогенность.** Устройства в ИВ неоднородны по определению и могут принадлежать различным сетям и аппаратным платформам, что не является препятствием к взаимодействию.

– **Динамичность.** Состояние устройств меняется постоянно: включение и выключение, контекстная и технологическая информация, в том числе местоположение и скорость. Количество подключённых устройств также может динамически изменяться.

– **Масштабность.** Количество устройств, которые будут «общаться» и получать управляющее воздействие, в десятки раз превысит количество узлов в текущей сети Интернет. Очевидно, что количество коммуникаций, которые могут быть инициированы устройствами, радикально превысит возможное число соединений, инициаторами которых выступают люди. Поэтому на первый план выходят вопросы интерпретации данных, с целью их последующего применения.

Коммуникации и протоколы

С развитием сети Интернет и беспроводных технологий мы получили «коммуникации в любое время», смартфоны и планшеты позволили реализовать принцип «коммуникации в любом месте». ИВ добавляет новое измерение и третью степень свободы в пространстве коммуникаций – «коммуникации с любой сущностью», будь то компьютеры, люди или устройства. Также принципиально новым явлением становится «самостоятельный» обмен данными или информацией между устройствами различных типов.

Базовыми способами коммуникаций между устройствами могут быть следующие:

– с использованием шлюза и концентратора данных (via gateway);
– с использованием только сети передачи данных (without gateway);
– прямые соединения между устройствами (direct communication).

В части подробного описания протоколов можно порекомендовать статью «Протоколы Интернета вещей: основные сведения», опубликованную в журнале «Мир компьютерной автоматизации: встраиваемые компьютерные системы» № 1 за 2015 г. Это одно из лучших описание данной темы, которое можно найти на русском языке.

Стандарты и консорциумы

Блестящие рыночные перспективы, которые аналитики дружно обещают направлению ИВ, не позволяют компаниям самого разного размера и специализации в области информационных технологий остаться равнодушными. В одиночку и путём объединения в консорциумы они пытаются занять свою нишу и освоить это перспективное направление. В таблице представлены наиболее крупные объединения, их задачи и названия основных компаний-участников.

Наиболее крупные консорциумы по освоению «Интернета вещей»

Консорциум	Задачи	Основные компании-участники
AllJoyn	Позволить совместимым «умным» устройствам «узнавать» друг друга, устанавливать соединения и распределять свои ресурсы, и обмениваться данными вне зависимости от производителя, вида сети и используемой операционной системы.	Qualcomm + Cisco, Microsoft, LG, HTC
The Physical Web	Обеспечение возможности потребителям общаться с любым доступным «умным» устройством без предварительной загрузки и установки специализированного программного обеспечения.	Google
Industrial Internet Consortium	Проектирование и создание решений в области интеллектуальной промышленной автоматизации.	SAP, Intel, Cisco, AT&T, GE, IBM, Microsoft
Open Interconnect Consortium	Разработка коммуникационного каркаса приложений, базирующегося на индустриальных стандартах, с целью установления беспроводных соединений и интеллектуального управления информационными потоками.	Intel + Atmel, Dell, Broadcom, Samsung, Wind River
Thread	Разработка нового беспроводного сетевого протокола	Google's Nest, Samsung Electronics, ARM Holdings, Freescale Semiconductor, Silicon Labs, Big Ass Fans и Yale Locks & Hardware

Практическое применение

Сценарии использования

Возможные сценарии использования парадигмы ИВ и их взаимная связь хорошо отражены на инфографике, подготовленной компанией Libelium (рис. 4).

Бизнес–модель и экосистема

Чтобы лучше понять методы и способы извлечения прибыли или преимуществ от использования ИВ, необходимо определиться с несколькими справочниками. Виды справочников напрямую следуют из референтной модели, а состав может отличаться. В первую очередь определимся с конечным потребителем или заказчиком:

- Промышленность и государство (Industrial & Government Applications):
  - Умные города (Smart Cities);
  - Мониторинг окружающей среды (Smart Environment);
  - Умное водопользование (Smart Water);
  - Умный учёт (Smart Metering);
  - Безопасность и чрезвычайные ситуации (Security & Emergencies);
  - Розничная торговля (Retail);
  - Логистика и транспорт (Logistics & Transportation);
  - Производственная автоматизация и контроль (Industrial Control);
  - Сельское хозяйство (Smart Agriculture);
  - Строительство (Buildings);
  - Прогрессивное животноводство (Smart Animal Farming).
- Потребительские устройства (Consumer):
  - Домашняя автоматизация (Domotic & Home Automation);
  - Носимые устройства (Wearable Technology);
  - Электронное здравоохранение (e-Health, Healthcare).

У двух больших категорий разные драйверы развития. Если на вертикальных рынках польза от ИВ определяется наличием специфических задач (включая государственное регулирование) или нишевых проблем, не решаемых эффективно существующими технологиями, то на потребительском рынке тренд задают новые бизнес-модели, которые включают в себя формирование потребностей потребителя и создание принципиально новых услуг и возможностей.

Бизнес-модель деятельности компаний, в которую уже входит или органично может войти «Интернет вещей», можно сегментировать таким образом:

- анализ данных (Data Analysis);
- выполнение НИР и ОКР, консалтинг (Management Consulting / Research);
- облачные платформы и сервисы (Cloud Platform Service);
- производство и поставки оборудования (Hardware Producer / Vendor);
- проектирование продуктов и услуг (Product / Service Design);
- разработка аппаратного обеспечения (Hardware Development);
- разработка программного обеспечения (Software Development);
- системная интеграция (System Integrator);
- услуги и сервисы связи (End-to-end Service Provider).

Отметим также, что традиционные облачные сервисы:

- программное обеспечение как услуга (SaaS);
- платформа как услуга (PaaS);
- инфраструктура как услуга (IaaS);
- мониторинг как услуга (Maac);
- коммуникация как услуга (CaaS), –

существенно сокращают время и стоимость развёртывания решений, основанных на парадигме ИВ. В этом ряду сервисов, расположенных в порядке убывания комплексности, с точки зрения заказчика, появляется ещё один, самый элементарный, присущий только ИВ, – «датчик как услуга».

На рис. 5 приведена экосистема ИВ согласно [1].

Роли участников экосистемы (нумерация совпадает с рис. 5):

1. Обеспечивает возможность передачи «сырых» данных, соответствующих логике и назначению устройства, оператору связи или непосредственно поставщику приложений.

2. Играет центральную роль в экосистеме ИВ и выполняет следующие функции: обеспечение доступа и интеграция ресурсов, предоставляемых другими поставщиками; поддержка и контроль сервисов инфраструктуры ИВ; размещение сервисов, в том числе для (от) других провайдеров.

3. Обеспечивает возможности интеграции и открытые интерфейсы. Наиболее типичными являются функции интеграции, хранения и обработки данных и управление конфигурацией самих устройств.

4. Использует функциональные возможности и ресурсы, предоставляемые операторами связи, платформами и самими устройствами в интересах решения задач клиента с помощью специализированных приложений.

Перебирая различные сочетания 1–4, можно получить пять базовых бизнес-моделей:

1. Весь комплекс услуг предоставляется заказчику одним провайдером (1, 2, 3, 4).

2. Устройства, услуги связи и платформу предоставляет один провайдер, а приложения – от независимого поставщика (1, 2, 3) + (4).

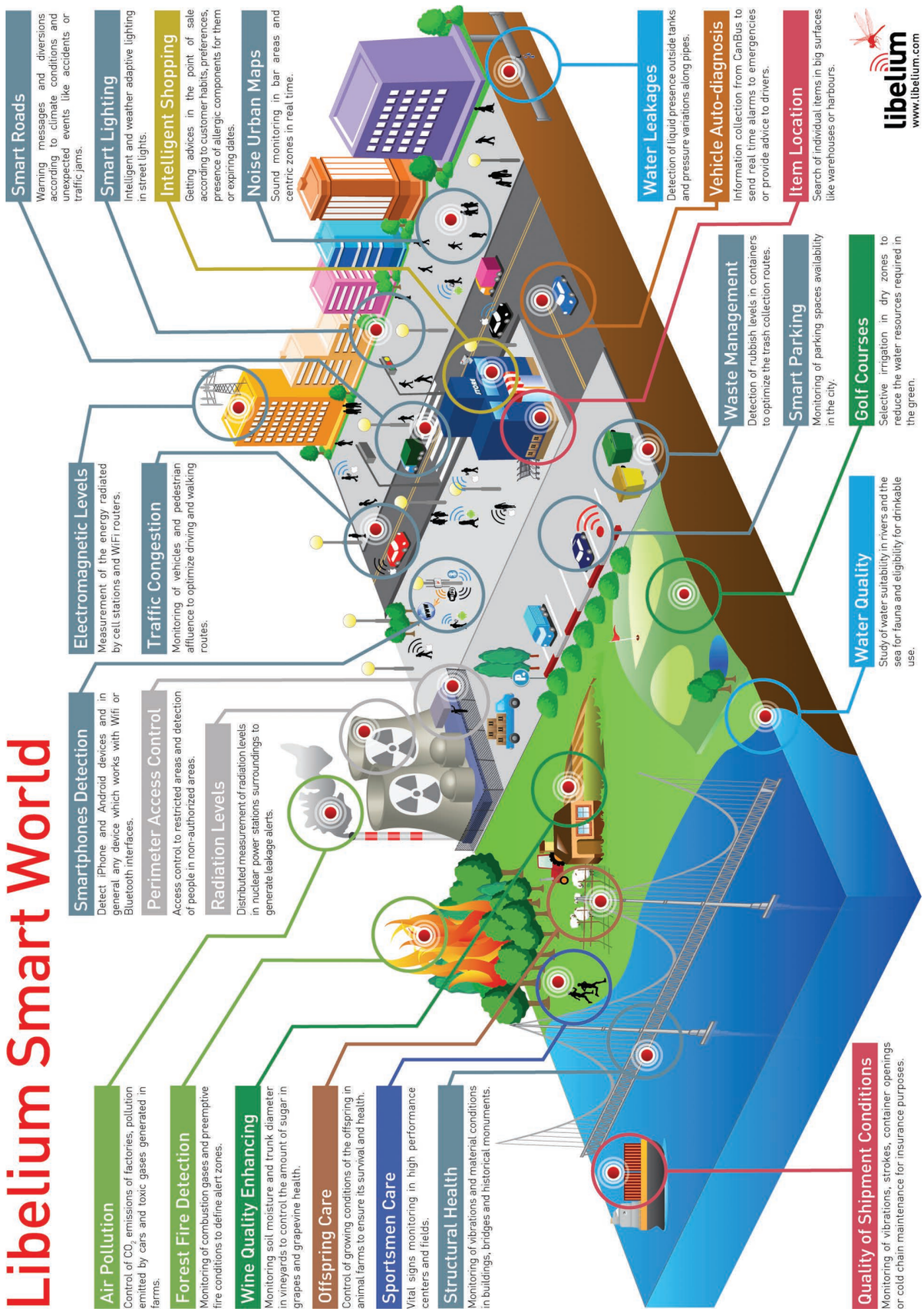


Рис. 4. «Умный» мир

3. Производитель устройств снабжает их соответствующими приложениями, услуги сети и платформу предоставляет другой вендор (1, 4) + (2, 3).

4. Аналогично п. 3. – производитель является также и разработчиком платформы (1, 3, 4) + (2), оператор связи независим и выбирается заказчиком.

5. Заказчик или системный интегратор «собирает» систему из компонентов от четырёх независимых производителей (1)+(2)+(3)+(4).

Риски

Оптимизм в части перспектив ИВ сдерживается существованием разного вида барьеров, стоящих на пути этой технологии. Перечислим и кратко охарактеризуем только основные.

Новые стандарты. Нет единого стандарта на протоколы информационного обмена. Активные попытки создания идут. Существующие требуют развития или замены, так как не соответствуют новым задачам. Ситуация напоминает эпоху развития видеотехники, когда каждый консорциум развивал свои стандарты записи видеосигнала – VHS, Hi8, VHS-C, BetaMax и др. – и все они нашли свою нишу. Такое «распыление усилий» не только замедляет развитие, но и приведёт к проблемам совместимости для большинства компонентов потенциальных систем. Добавим также сравнительно медленный переход к повсеместному использованию протокола IPv6.

Стоимость. Относительно высокая стоимость каждого узла, концентраторов данных, подключение к коммуникационным сетям и (или) оплата дополнительного трафика, потребление электроэнергии, подписка на сервисы и т. д. приводит к тому, что массового появления самых эффективных, с точки зрения теории, сетей, насчитывающих десятки тысяч устройств, мы пока не наблюдаем. В большинстве потенциально чрезвычайно перспективных отраслей (например, сельское хозяйство и животноводство) сроки окупаемости пока значительные, что подталкивает потенциальных потребителей, с учётом бурного развития и переосмысления концепции ИВ, занимать выжидательную позицию.

Безопасность. Последняя в нашем списке, но самая значимая из проблем. Аспектов, по которым ИВ может отрицательно сказаться на безопасности, множество. От увеличения риска для закрытых корпоративных сетей до утечек персональных данных. Очевидно, что в промышленности использование беспроводных технологий увеличивает уязвимость. Конечно, различные производители уже готовы предложить решения, но их эффективность сильно зависит от ресурса атакующего и его мотивации. В случае значительного ресурса и высокой мотивации – гарантированной защиты пока не существует. На потребительском рынке – казуальное использование «умных» устройств, «умный дом», персональная медицина – ситуация сложней и труднопредсказуема. У людей по объективным, а зачастую и субъективным, причинам может расти тревога в отношении возможности утраты персональной информации или вреда от излучений беспроводных устройств и т. п. Разоблачения Эдварда Сноудена, например, изменили поведение значительного числа людей, которым объективно нечего и незачем скрывать. «Синдром Сноудена» реально «ударил» по социальным сетям и некоторым производителям программного обеспечения для мобильных устройств. Справедливости ради следует отметить, что открылись новые возможности для продажи решений по защите персональной информации, включая рынок «псевдорешений».

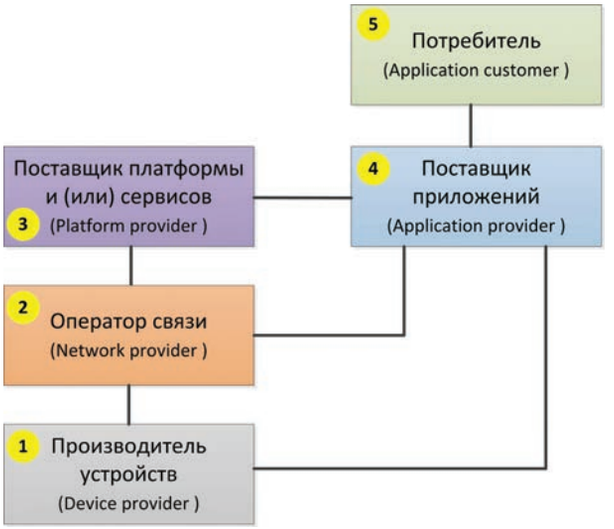


Рис. 5. Экосистема «Интернета вещей»

Коммерциализация

Успешная монетизация невозможна без получения ответов на вопросы:

- кто является потребителем?
- что представляет для него ценность?
- каким образом вы планируете её создать?
- как донести эту ценность до потребителя и продать ему по разумной экономически обоснованной цене?

Новые бизнес-модели появляются как результат развития технологий и открывают широкий спектр получения прямых и косвенных доходов. Новым явлением стали многочисленные открытые сообщества разработчиков, вовлечённые не только в процессы проектирования и создания ценностей, но и в процессы их потребления. Основные модели коммерциализации для ИВ были заложены развитием традиционного Интернета.

Лицензирование. Старейшая и наиболее распространённая модель в индустрии программного обеспечения. В случае ИВ речь может идти не только о программах и сервисах, а также о данных и резуль-

татах аналитики. Их использование внутри домена приложения может быть бесплатным, плата взымается за данные, имеющие ценность для других приложений и потребителей. Это даёт совершенно уникальную возможность расширять границы приложений в соответствии с запросами клиентов.

Подписка. Одна из вариаций модели лицензирования. Плата за доступ к данным (услугам) для определённого периода времени – по сути, превращает разовые продажи продукта в повторяющиеся. При этом появляется возможность менять цены в зависимости от того, как часто и как долго клиент использует службу. Хорошая практика скидки на более долгие сроки подписки позволяет «привязывать» к себе заказчика и привлечь и аккумулировать средства на дальнейшее развитие.

Премиум-сервисы. Идея этой бизнес-модели заключается в предоставлении простых и базовых услуг бесплатно, с целью продажи более продвинутых или дополнительных функций. В этом случае рост возможен не только за счёт привлечения новых пользователей, но и повышения дохода от существующих. Если потребитель удовлетворён базовыми сервисами, он не только будет готов внести небольшую плату, чтобы получить дополнительные сервисы, но и станет рекламировать его своим друзьям и семье. Эта модель поощряет пользователей бесплатной части продукта взаимодействовать таким образом, чтобы создать спрос на дополнительные платные услуги.

Реклама. Мы уже знакомы с тем, как передовые методы бизнес-аналитики используются для контекстной рекламы и поведенческого маркетинга. ИВ даёт новые возможности, когда содержимое отображаемой рекламы будет динамически меняться в зависимости от поведения пользователя и содержания получаемых данных от сенсоров.

Генерация трафика. Бизнес-модель генерации трафика – хороший пример косвенного способа монетизации. Увеличивается шанс получения доходов от прямых бизнес-моделей, таких как электронные платежи, премиум-сервисы или реклама. Не забудем также, что весь этот трафик кем-то оплачивается, как и модернизация сетевого оборудования и каналов связи, необходимых для его прохождения.

Электронные платежи. Идея состоит в том, чтобы получить прибыль от микроплатежей от индивидуального использования наборов данных или результатов аналитики. Потребители могут произвести платёж в любое время дня или ночи, в любой точке мира. Модель электронных платежей не новая в Интернете, но переход к микрооплатам позволит вовлечь пользователей даже с низкими доходами.

Массовая кастомизация. ИВ позволяет создавать индивидуальные продукты для каждого клиента исходя из его требований и даже предпочтений. Слишком дорогое решение для традиционного товарного производства, в случае продажи сервисов и услуг, являющихся по сути информационными, становится рентабельным и возможным.

Совместное потребление. Яркими представителями Peer-to-Peer (P2P) в традиционном Интернете являются файлообменные сервисы. Модель, сложная для извлечения прибыли, используется главным образом для обмена контентом и постоянно подвергается критике правообладателей. В мире ИВ ситуация может радикальным образом измениться. Каждый легко может стать поставщиком собственного информационно-аналитического контента или просто данных от сенсоров или других устройств, который можно будет продавать или обменивать.

Мобильная коммерция. Модель быстро развивается и просто получит дополнительный импульс. Как и в случае с рекламой, возможности по точному предложению товаров и услуг, в том числе нужных «здесь и сейчас», возрастут многократно.

Заключение

Граней, на которые можно отразить парадигму ИВ, конечно, больше. Каждый месяц появляются новые исследования, которые всё глубже прорабатывают не только отдельные аспекты этой темы, но и семантические связи между ними. Если после прочтения этой статьи у читателя появится желание подумать о том, как применить новые возможности к текущим или перспективным задачам бизнеса, автор будет считать задачу выполненной. При всех сомнениях в перспективности и целесообразности использования технологий ИВ следует в первую очередь искать решение не в области замены «классических решений» – а в нахождении некоего «симбиоза» или проектирования принципиально новых систем и сервисов. Компания «РТСофт» имеет и активно развивает свои компетенции в области «Интернета вещей» и готова оказывать широкий спектр услуг в этой области – от консультационных услуг до разработки приложений и системной интеграции.

Литература

1. Recommendation ITU-T Y.2060, «Overview of the Internet of things», Geneva, 2013 г.

2. Francis daCosta, «Rethinking the Internet of Things: A Scalable Approach to Connecting Everything», © 2013 by Apress Media.

3. Fernando Almeida, José D. Santos and José A. Monteiro, «E-Commerce Business Models in the Context of Web 3.0 Paradigm», International Journal of Advanced Information Technology (IJAIT) Vol. 3, No. 6, December 2013.

4. Информация с сайтов: www.ibm.com, www.beechamresearch.com, www.libelium.com, wikipedia.org.

Норберт Хаузер (Nobert Hauser), Kontron

Industry 4.0 – немецкий «Интернет вещей» и Kontron – его лидер

«Интернет вещей» – это основа информационного мира завтрашнего дня: идёт ли речь об «умном» доме, «умной» электросети, «умной» фабрике или «умном» автомобиле. Если говорить о Германии, то к своим техническим достижениям немцы относят технологии производства и поэтому стремятся к развитию «Интернета вещей» и его внедрению на будущих «умных» фабриках, используя концепцию, получившую название Industry 4.0.

Industry 4.0 – немецкий «Интернет вещей»

Распространение технологии «Интернета вещей» будет оказывать влияние на все стороны нашей жизни: на то, как мы водим автомобили, как живём и, конечно, как производим продукцию. Поскольку технология производства – это один из столпов немецкой промышленности, Германия поставила перед собой амбициозную задачу – внедрить «Интернет вещей» в производство и, более того, занять в этом процессе ведущую роль. Впервые термин Industry 4.0 был использован в 2011 году на Ганноверской ярмарке (Hannover Fair) – крупнейшем в мире шоу промышленных технологий. Концепция Industry 4.0 – это дерзкий проект, часть стратегии федерального правительства Германии в области высоких технологий. Этот термин означает четвёртую промышленную революцию – цифровую революцию в области технологии производства. По сути это не что иное, как непрерывный процесс автоматизации производства с использованием электроники и информационных технологий (ИТ).

Проект Industry 4.0 продвигается и в других странах, но под другими названиями. В США это деятельность в рамках программы Advanced Automation, которая сравнима с германским проектом Industry 4.0. Однако Industry 4.0 – это именно немецкий проект, концепция которого была предложена по инициативе Германии. Вся деятельность в нём сосредоточена и координируется в рамках «Платформы Industry 4.0», созданной объединёнными усилиями накануне выставки Hannover Fair 2013 и в настоящее время поддерживается тремя отраслевыми организациями: BITKOM (информационные технологии), VDMA (машиностроение) и ZVEI (электротехника).

В чём истинная цель этой инициативы? Отраслевые эксперты полагают, что в результате внедрения технологии «Интернета вещей» в производство технические и бизнес-процессы будут объединены. Проект Industry 4.0 предназначен для того, чтобы помочь немецким компаниям осуществить переход в новую эру промышленного производства и, по-возможности, взять на себя роль лидера в решении новых задач.

Итак, в чём же суть проблемы? В современной логистике промышленного производства используются различные ИТ-решения: цеховые системы автоматизации, над ними системы управления производственными процессами (Manufacturing Execution System – MES) и на самом верхнем уровне системы планирования ресурсов предприятия (Enterprise Resource Planning – ERP). На стадии разработки используются разнообразные инструменты проектирования, а при техническом обслуживании и ремонте оборудования применяется свой ИТ-инструментарий. Можно предположить, что «Интернет вещей» вызовет замену такой иерархической и весьма неоднородной ИТ-системы на унифицированную коммуникационную структуру на единой идеологической основе, что поставит под сомнение само существование нынешней инфраструктуры связи. По этой причине одной из важнейших задач проекта Industry 4.0 ста-

новится объединение всех логистических цепочек с помощью интегрированной ИТ-поддержки. Другими словами, существующая на сегодняшний день архитектура программного обеспечения включает в себя средства, которые, вследствие их специализации на определённых задачах, существенно различаются по структуре, семантике и методам исполнения. Отраслевые специалисты сходятся во мнении, что мир производства нуждается в унифицированной эталонной архитектуре, которая определяет, каким образом в будущем могут быть интегрированы эти разнородные программные концепции. Поэтому заинтересованные стороны ставят перед собой задачу создания системной среды, в которой обмен информацией между отдельными процессами может быть осуществлён просто, напрямую и безопасно. В конечном итоге объединение системы автоматизации с ИТ-системой должно достичь такого уровня, при котором мы не сможем в явном виде отделить их друг о друга.

Руководящие органы, под попечительством которых находятся проекты в области Industry 4.0, задаются рядом вопросов. Как концепция Industry 4.0 может работать в условиях производства? Насколько защищёнными будут данные? Как управлять полученными в результате большими массивами данных? Как можно объединить виртуальный мир «Интернета вещей» с уровнем реального производства? Как классические ИТ-средства будут взаимодействовать с инструментами Industry 4.0? И как изменится рабочее место на производстве? Вначале следует прояснить две наиболее важные темы.

Во-первых, ИТ-безопасность. В силу необходимости применения интегрированных ИТ-решений, тема защиты информации в системах Industry 4.0 приобретает всё большую важность. На сегодня правительство Германии оценивает ежегодные убытки немецких компаний из-за кибератак на уровне 50 млрд евро. Фактическая сумма, вероятно, намного выше, поскольку многие компании не фиксируют или не публикуют эту информацию из-за боязни ещё больших потерь и снижения доверия со стороны заказчиков.

Во-вторых, стандартизация. Предполагаемая однородная коммуникационная структура будущих «умных» фабрик требует, чтобы эти фабрики состояли из множества интеллектуальных объектов, так называемых киберфизических систем (cyber physical systems – CPS). Иными словами, модульных распределённых интеллектуальных систем, в которых объединены физические и виртуальные возможности. Эти системы, или производственные модули, будут всё в большей степени обладать способностью к самоорганизации и обмену необходимой информацией. Однако такая всеобъемлющая модульная организация и переход к цифровому формату требует создания коммуникационных стандартов между киберфизическими системами, что представляет собой серьёзную задачу, требующую своего решения. Предварительный перспективный план этой стандартизации был представлен на выставке Hannover Fair 2014.

Kontron: «Industry 4.0 – будущая площадка для наших игр!»

Промышленное подразделение компании Kontron реализует свою компетенцию в области технологий промышленной автоматизации в рамках отдельного бизнес-направления. Что означает для Kontron направление Industry 4.0 и какую роль компания играет в развитии этой перспективной технологии? Своим мнением делится Норберт Хаузер (Norbert Hauser), руководитель направления промышленной автоматизации.

Г-н Хаузер, какую роль может и хочет играть Kontron в становлении Industry 4.0?

Хаузер: Когда мы рассматриваем Industry 4.0, то становится ясно, что ключевую роль в этой перспективной концепции будут играть киберфизические системы (CPS). Как один из мировых лидеров среди производителей интеллектуальных встраиваемых систем с доступом к сети – по сути киберфизических систем – компания Kontron хотела бы играть на этом поле ведущую роль. Определять рынок Industry 4.0 будут инновационные системы на базе открытых стандартов – область, в которой мы хорошо разбираемся уже сегодня.

Почему вы считаете, что вам предназначена роль лидера?

Мы обладаем ноу-хау не только в области встраиваемых систем и собственным опытом промышленных разработок в этой сфере (функциональные блоки для систем управления, визуализации, продукты для промышленных систем связи). Наше бизнес-подразделение по коммуникационной тематике обладает также компетенцией в сфере серверов для облачных систем, стеков беспроводных протоколов и M2M-технологий с использованием таких видов связи, как WiFi, GSM, GPRS и UMTS. Это позволяет нам, используя собственный опыт, объединить информационные технологии (ИТ) и промышленную автоматизацию (см. рис.), что весьма важно для достижения успеха на этом рынке в будущем.

Что предпринимает Kontron для реализации Industry 4.0 сегодня?

Мы уже обеспечили решение множества задач Industry 4.0. В нашем портфолио имеются масштаби-

руемые многоядерные системы с RFID-функциями, например для идентификации и отслеживания изделий на заводе или для идентификации пользователей с разными уровнями прав доступа на компьютере, при сервисном обслуживании или проектировании.

Мы также предлагаем системы, подготовленные к технологии «Интернета вещей», которые могут поддерживать связь с помощью интерфейсов GbE, WiFi или через беспроводную локальную сеть (WLAN) на базе различных стеков протоколов с использованием защищённых коммуникационных каналов. И наконец, мы предлагаем энергоэффективные системы, например с применением новейшей мобильной технологии от Intel.

Кроме того, особое внимание мы обращаем на техническое обслуживание – диагностирование неисправностей станков и агрегатов, которое наши клиенты в рамках специального сервиса могут предоставить свои конечным пользователям, например через коммуникационное взаимодействие нашей системной информации с их рабочими данными. Однако мы не забываем и про системы, не требующие технического обслуживания. Это два очень важных фактора, которые нужно принимать во внимание при разработке киберфизических систем.

В заключение важно отметить, что мы играем активную роль в становлении проекта Industry 4.0. Мы активные участники не только рабочей группы по Industry 4.0, но также рабочей группы по киберфизическим системам в BITKOM (отраслевой консорциум ИТ-индустрии). В последнее время мы также активно работаем в этой области в рамках VDMA – Союза машиностроителей Германии.

Какие дополнительные шаги по дальнейшему развитию проекта Industry 4.0 планирует Kontron?

Как я уже отметил, мы инвестируем значительные средства в системы, не требующие технического обслуживания, а также, в функции сопровождения таких систем. Мы хотим реализовать эти функции в прикладных программах (apps), поскольку рабочими инструментами всё чаще становятся смартфоны и планшеты, с помощью которых можно запрашивать состояние системы станка или агрегата и при необходимости предпринимать какие-либо действия.

Кроме того, пристальное внимание мы уделяем разработке компактных систем. Образно говоря, шкаф электроавтоматики всё в большей и большей степени будет интегрироваться в сам промышленный агрегат или станок. В дополнение ко всем этим продуктам и техническим разработкам, мы хотим расширить наше предложение в области «Интернета вещей» в сфере связанных с этой технологией M2M-решений.

Пример объединения информационных технологий (ИТ) и промышленной автоматизации

Виктор Синенко, ЗАО «РТСофт»

Открытые технологические платформы как глобальный тренд в области разработки систем специального назначения

Квалифицированные кадры и время – безусловно, самые ценные ресурсы в проектах разработки ответственных аппаратно-программных решений. Возможность сконцентрироваться на конкретных вопросах в рамках собственной специализации – это сокращение проектных сроков и рациональное использование инженерного потенциала команды разработчиков. Один из подходов, увеличивающих таким образом конкурентоспособность и экономическую ценность создаваемых продуктов, рассматривается в данной статье.

Ключевые слова: открытые технологические платформы, встраиваемые компьютерные технологии для спецприменений, ускоренное проектирование аппаратно-программных комплексов.

Технологические платформы и расширение идеологии COTS

В современной экономике оборонно-промышленный комплекс (ОПК) – это не просто научно-производственная база обеспечения национальных вооружённых сил, но прежде всего самостоятельный наукоёмкий высокотехнологичный бизнес с высокой политической ответственностью и колоссальным экспортным потенциалом.

В 20-м веке продукция ОПК представляла собой сплав передовых достижений отраслевых научно-исследовательских и опытно-конструкторских центров и потенциала высокоточного производства, причём доля электронных компонентов и программного обеспечения в составе этой продукции постоянно возрастала. Трендом начала нового тысячелетия стало повышение добавленной стоимости наиболее продвинутых образцов вооружения и военной техники (ВВТ) за счёт использования комплексных услуг от специализированных инжиниринговых и сервисных компаний. При этом наиболее востребованы и успешны те решения и проекты, в рамках которых создаётся действительно эффективный симбиоз разработчиков и производителей ВВТ, с одной стороны, и их партнёров из области передовых информационных технологий (ИТ), с другой.

К числу подобных подходов относится хорошо зарекомендовавшая себя на российском рынке парадигма COTS (Commercial Off The Shelf) – использование готовых коммерческих продуктов «с полки», в рамках которой разработчики выбирают для своих проектов наиболее подходящие и легко интегрируемые базовые решения из числа уже имеющихся на рынке аппаратных средств модульного уровня. Построение более сложных и крупных систем, включая территориально распределённые, вполне может осуществляться по тому же принципу. Главное отличие будет состоять в переносе фокуса внимания разработчика с уровня модулей и плат на уровень устройств – базовых платформенных решений, быстро и эффективно модифицируемых архитектором под конкретную задачу.

Речь идёт о тех случаях, когда разработчики комплексов и систем «не заинтересованы в дискуссиях с ярыми приверженцами конкретных формфакторов или спецификаций, предпочитая решать свои конкретные проблемы независимо от наличия тех или иных ограничений в стандартах и спецификациях...» [1]. В таких обстоятельствах услуга по модификации базовой технологической платформы становится ключевым предложением партнёра по ИТ, а гибкость модификации оборудования под множество задач – существенным рыночным преимуществом для разработчика.

Платформенный подход на практике

Для наглядного представления данной концепции рассмотрим разработанную специалистами

ЗАО «РТСофт» аппаратно-программную платформу для построения специализированных вычислителей различного назначения (рис. 1). В данном решении используется четыре класса устройств, выполняющих функции строительных блоков проектируемого комплекса или системы:

– блок вычислительный серверный, который предназначен для создания целевых серверных устройств с определёнными функциями (например, универсальный сервер, сервер радиолокационной информации, сервер видеоданных, сервер-коммутатор данных, сервер экрана коллективного пользования, сервер координированного управления и т. д.);
– блок вычислительный операторский, предназначенный для организации клиентских рабочих мест с развитым графическим интерфейсом и прикладным ПО (реализует различные функциональные возможности, в том числе работу с навигационными данными и картографической информацией, управление разнородными корабельными системами и агрегатами);
– блок вычислительный – хранилище данных – для обеспечения надёжного и резервированного хранения больших объёмов информации (включая видеоданные) с доступом по сетям Ethernet 1000Base-T; состоит из устройства управления памятью и устройства хранения данных;
– блок коммутационный – для организации обмена данными и командами управления с периферийными устройствами и взаимодействия смежных систем (системный мост).

Блоки Платформы представляют собой наборы COTS-модулей в популярных стандартах встраиваемых систем CompactPCI или CompactPCI Serial (в зависимости от требований проекта и опыта заказчика) в защищённом исполнении. В аппаратной архитектуре блоков платформы традиционная для магистрально-модульных систем гибкость сочетается с повышенной стойкостью к ударным воздействиям и вибрации, пыле- и влагозащищённостью. Конструктив для всех блоков унифицирован – это «Евромеханика» высотой 4U, которая включает блок питания с различными вариантами рабочего напряжения, объединительную плату и интерфейсную панель. Устройства спроектированы с применением принудительного воздушного охлаждения, аксиального либо с забором воздуха через переднюю панель и удалением тёплого воздуха через тыльную панель, что позволяет выдерживать серьёзную тепловую нагрузку до 300 Вт.

Рис. 1. Один из вариантов исполнения блоков Платформы для построения специализированных устройств: серверный блок (слева сверху), операторский блок (справа сверху), коммутационный блок (справа снизу), хранилище данных (слева снизу). Возможна ускоренная кастомизация типов разъёмов, расположения внешних интерфейсов на корпусах блоков или доработка исполнения в соответствии с ГОСТ РВ 20.39.304–98 под требования конкретного проекта.

Для сопряжения с внешними устройствами в блоках предусмотрено большое количество разнообразных интерфейсов: Ethernet 1000Base-T с возможностью замены на 10GbE, МКИО, RS232/422/485, USB 2.0/3.0 и других. Расширение или изменение аппаратной конфигурации блоков, добавление аналоговых каналов ввода-вывода, специализированных модулей и интерфейсов может быть достигнуто за счёт применения плат с интерфейсами XMC/PMC.

Отметим, что в зависимости от предъявляемых требований возможна реализация блоков с использованием архитектуры COM Express, обеспечивающей максимальные возможности модернизации и наращивания вычислительной мощности в течение длительного жизненного цикла проектируемых устройств без необходимости изменения интерфейсов, реализованных на плате-носителе COM Express. Хотя о преимуществах такого подхода известно многим разработчикам специализированных устройств, считаем необходимым ещё раз обратить внимание на красоту заложенной в него идеи [2].

Но вернемся к Платформе и её программному инструментарию. Поддержка функционала блоков Платформы обеспечивается пакетом базового системного программного обеспечения (БСПО) – набором библиотек под ОС МСВС и Astra Linux. С помощью БСПО разработчики могут ускоренно реализовывать функции резервирования каналов передачи данных и взаимодействия с сопрягаемыми устройствами в соответствии со специфическими синхронными и асинхронными протоколами, функции формирования исходящих и обработки входящих потоков данных, поступающих от сопрягаемых систем, а также функции обеспечения взаимодействия алгоритмов прикладного ПО с сопрягаемыми системами. В состав БСПО входят инструменты для

создания оболочки программного резервирования вычислительных процессов и разнесения обработки прикладных алгоритмов и системного программного обеспечения на различные процессорные ядра или модули. Также с помощью этих программных средств может быть реализован мониторинг технического состояния блоков.

Для предотвращения несанкционированного доступа предусмотрено использование одного из популярных на рынке модулей доверенной загрузки, сертифицированного ФСТЭК России для применения в автоматизированных системах до класса 1Б включительно, а также по 2-му уровню контроля на отсутствие недекларированных возможностей.

Как удобство разработки способствует повышению экономической эффективности

Основное преимущество, которое получает разработчик при использовании Платформы, заключается в максимальной технологической гибкости, заложенной в её аппаратно-программный инструментарий: целевая система собирается из базовых блоков на манер конструктора (рис. 2). В результате системный архитектор может сфокусировать свой инженерный потенциал на прикладных программных алгоритмах, сопряжении проектируемой системы со сторонними устройствами, контроле соответствия её параметров и логики отраслевым стандартам и внутрифирменным регламентам. При этом все действия по модификации аппаратной части блоков и доработке БСПО осуществляются поставщиком Платформы.

Примером может служить наиболее часто встречающаяся задача подобного рода – ускоренная кастомизация типов разъёмов и расположения внешних интерфейсов на корпусах блоков или доработка исполнения в соответствии с проектными требованиями по ГОСТ РВ 20.39.304-98. В программной части такие работы связаны, как правило, с адаптацией БСПО для обеспечения взаимодействия со специализированными модулями или протоколами передачи данных под популярными на рынке операционными системами семейства Linux, QNX, LynxOS и VxWorks.

Разработчики хорошо знают, что такие технологические операции на этапах проектирования и макетирования ответственных систем требуют затрат большого количества времени и внушительных объёмов финансирования. Однако наличие готового базового инструментария позволяет уйти от разработки «с нуля» и адаптировать готовые инструменты под задание на основе наработанной базы схемотехнических и программных решений. То есть существенно сократить время и стоимость разработки на старте: так, максимальный период, который компания «РТСофт» стремится обеспечить для модификации блоков и БСПО Платформы под специфические требования, не превышает полугода. Из нашей практики мы можем отметить и другие преимущества использования инструментов Платформы – сокращение затрат на тестирование и обновление БСПО, отладку и модернизацию аппаратных средств, масштабирование системы и снижение её общей стоимости.

Особое значение платформенный подход приобретает в свете отраслевых требований к управлению жизненным циклом продукции и её обслуживанию в течение длительного периода, вплоть до 25 лет, с возможностью своевременной модернизации базовой вычислительной платформы. Довольно ёмко комплексность таких вызовов сформулирована зарубежным экспертом в области встраиваемых компьютерных технологий для спецприменений Дэвидом Пёрсли: «Производительность и надёжность имеют большое значение как для уже развёрнутых, так и для вновь разворачиваемых систем, которые должны постоянно обновляться и совершенствоваться, дабы отвечать современным требованиям в части совмест-

Рис. 2. Вычислительные, серверные и коммутационные устройства – это далеко не полный перечень возможных применений аппаратно–программных средств Платформы при построении корабельных систем. Гибкий и универсальный инструментарий позволяет на манер конструктора собирать из исходных базовых блоков системы различных классов.

ного использования данных, защищённости и производительности. Например, эсминец может пережить первое крупное обновление технологий сразу после его постройки и перед спуском на воду. Его сенсоры и радарные башни навсегда останутся там, где их возвели строители, а вот компьютерные платформы и всё остальное, что подпадает под определение «бортовых ИТ», будут обновляться в промежутках между длительными походами» [3]. Здесь необходимо отметить, что работа с блоками платформы предполагает перекладку «головной боли», связанной с контролем рыночной доступности аппаратных компонентов, обновления БСПО и тому подобных хлопот на плечи сервисного партнёра по информационным технологиям. Разработчик комплекса или конечной системы получает готовые к установке функционального ПО блоки устройств (что особенно ценно с точки зрения минимизации затрат при сопровождении уже поставленной продукции), проводит серию тестов – и оборудование готово к отправке хоть на Кольский полуостров, хоть на берег Южно-Китайского моря. То есть платформенный подход позволяет сохранять высокие уровни готовности, производительности и обслуживаемости систем на протяжении их жизненного цикла.

Мировые тенденции на российской почве

Стремясь идти в ногу с прогрессом, предприятия-разработчики конечных систем могут выбрать один из двух путей: накапливать компетенции в области базовых аппаратных и программных технологий, второстепенных в контексте их основной деятельности, либо использовать готовый базовый инструментарий с опорой на открытые стандарты. Последний, более рациональный и дальновидный, сценарий предполагает возрастание роли консалтинговой поддержки со стороны высокотехнологичных компаний-партнёров, позволяющей на старте разработки минимизировать риски в инженерных стратегиях развития изделия. Данная схема организации взаимодействия между предприятиями-разработчиками и изготовителями спецсистем и сервисными ИТ-компаниями, предлагающими базовые аппаратно-программные платформы в комплексе с услугами по их адаптации под требования проекта, весьма популярна в оборонной отрасли и является одним из глобальных трендов. Например, французская фирма Thales использовала многопроцессорные системы 6U VME немецкого холдинга Kontron на базе процессорных модулей POWERNODE3, PENTXM2 и PENTXM4 для создания многофункциональной РЛС Herakles и инфракрасной системы наблюдения и сопровождения Artemis для французского проекта FREMM [4].

Особенно ярко достоинства платформенного пути проявляются в проектах с несколькими предприятиями-разработчиками, где естественным образом возникает необходимость опоры на удобную для всех сторон унифицированную аппаратно-программную платформу. Так, компания General Electric Intelligent Platforms предоставляет партнёрам по североамериканскому консорциуму разработчиков перспективной авионики FACE процессорные модули 3U SBC312 и 6U SBC625 в стандарте VPX и программные средства разработки, а также соответствующее решение системного уровня FACEREF [5].

Высокую степень экономической привлекательности данного подхода для разработчиков российских систем специального назначения подтверждает опыт работы компании «РТСофт», давно и успешно участвующей в реализации такой модели на практике. Платформенный метод уже нашёл своё применение в проектах создания аппаратно-программных комплексов для информационных и управляющих систем как в наземных пунктах управления разнородными средствами, так и для управления различными корабельными системами, в том числе реального времени. Не исключено, что в условиях растущего объёма государственного оборонного заказа и повышения требований к сопровождению продукции военного назначения на всех стадиях жизненного цикла именно такие способы взаимодействия будут приводить к появлению наиболее конкурентоспособных отечественных систем специального назначения.

Литература

1. Ханер, Ирен. От коммутации к услугам: современный заказчик «тяготеет» к вендорам, способным поддерживать свои предложения услугами по разработке и интеграции готовых аппаратных платформ // Мир компьютерной автоматизации: встраиваемые компьютерные системы. – 2011. – № 6. – С. 34–35.

2. Пёрсли, Дэвид. Стратегии обновления технологий облегчают труд разработчиков военных систем // Мир компьютерной автоматизации: встраиваемые компьютерные системы. – 2012. – № 1. – С. 34–38.

3. http://www.kontron.com/applicationstorydetail/turnkey-platform-for-navy.

4. http://defense.ge-ip.com/news/ge-intelligent-platforms-joins-face-consortium-to-help-drive-innovation-and-lower-cost-for-avionics-systems/n3060.

5. http://defense.ge-ip.com/news/new-rugged-platform-from-ge-allows-face-developers-to-minimize-cost-risk-and-time-to-market/n3013.

Сергей Жуков, Игорь Починок, Auriga, Inc., НИВЦ МГУ

Расширенная модель сенсоров в спецификации PICMG 3.7

Спецификация PICMG 3.7 – AdvancedTCA Base Extensions, выпущенная в январе 2015 г., содержит описание расширений и новых возможностей архитектуры AdvancedTCA. Одна из основных её новаций – это расширенная модель сенсоров, позволяющая преодолеть некоторые недостатки модели сенсоров, которая используется в настоящее время.

Введение

В 2003 г. консорциумом PICMG была разработана спецификация PICMG 3.0 AdvancedTCA (ATCA) [1]. Эта спецификация описывает открытую архитектуру, которая позволяет быстро создавать высокопроизводительные системы путем интеграции модульных компонентов в состав стандартных конструктивов (шасси). Архитектура была разработана для использования главным образом в телекоммуникационной отрасли и активно развивается и применяется в настоящее время.

Идеология централизованного системного управления в спецификации AdvancedTCA основана на спецификации IPMI, разработанной Intel для управления серверными системами. Управление реализовано с использованием выделенных управляющих контроллеров. На каждом компоненте системы устанавливается отдельный управляющий контроллер (IPMC); он выполняет задачи по управлению компонентом. Управлением всего шасси занимается управляющий модуль шасси (Shelf Manager). Управляющий модуль шасси взаимодействует с управляющими модулями по шине IPMB, используя команды протокола IPMI. Управляющий модуль, с одной стороны, отвечает за автономное управление конкретным шасси и модульными компонентами в ней, а с другой стороны, предоставляет интерфейсы для управления системой управляющим модулям более высокого уровня и обслуживающему персоналу. Для обеспечения надёжности рекомендована установка в шасси двух управляющих модулей, один из которых является активным, а другой находится в горячем резерве.

Спецификация PICMG 3.7 AdvancedTCA Base Extensions разрабатывалась в течение нескольких лет и была выпущена в январе 2015 г. Она содержит описание расширений и новых возможностей архитектуры AdvancedTCA, необходимость в которых возникла за время применения и развития данной архитектуры (более 10 лет). В частности, один из основных разделов спецификации (раздел 3) описывает новые возможности в области системного управления. Одна из основных новаций в этой области – расширенная модель сенсоров, позволяющая преодолеть некоторые недостатки модели сенсоров, которая сейчас используется в AdvancedTCA.

Другие нововведения спецификации PICMG 3.7 включают в себя:

- шасси нового типа (двусторонние), способные разместить до 32 плат с обеих сторон шасси (ранее количество плат в шасси было ограничено 16);
- новый тип плат и переходных модулей, обладающих новыми возможностями; также они способны занимать несколько слотов в шасси и потреблять значительно большую мощность;
- более детальная проработка архитектуры электропитания, поддержка в стандарте блоков питания на переменном токе и преобразователей с переменного тока на постоянный;
- записи нового типа в стандартной информации о шасси, предназначенные для более подробного описания архитектуры электропитания шасси.

Модель сенсоров в спецификации IPMI

Спецификация IPMI [2], определяя протокол и набор команд для взаимодействия с управляющим контроллером, уделяет особое внимание поддержке аппаратных сенсоров (датчиков). Такие датчики подсоединяются к управляющему контроллеру и измеряют различные физические величины – температуру, ток, напряжение, мгновенную мощность и т. д. Существуют также и дискретные

датчики, выдающие на выходе логическую величину (например, наличие или отсутствие некоторого сигнала).

В модели IPMI каждый управляющий контроллер может поддерживать до четырёх логических номеров устройства (LUN), на каждом из которых могут находиться до 255 различных логических сенсоров. Для работы с сенсорами предназначено специальное подмножество команд IPMI.

Сенсоры описываются специальными структурами данных SDR (Sensor Data Records). Эти структуры имеют стандартный формат и содержат атрибуты сенсора (имя, тип, пороги по умолчанию, начальная маска событий и т. д.) и другую информацию. Эти описатели находятся на управляющем контроллере и могут быть считаны специальными командами.

Сенсоры IPMI делятся на аналоговые и дискретные.

Аналоговые сенсоры выдают числовые значения физических датчиков – температуры, напряжения, тока, мощности и других физических характеристик. Значение аналогового сенсора может быть считано командой Get Sensor Reading. Эта команда возвращает однобайтовое, так называемое «сырое» (raw) значение сенсора. Для получения реального значения, выраженного в соответствующих единицах измерения (вольты, градусы, ватты и т. д.), значение должно быть преобразовано с использованием коэффициентов, хранящихся в SDR.

Для определения нахождения значения аналогового сенсора в допустимых пределах используются пороги. Для каждого аналогового сенсора может быть определено до 6 пороговых значений. Эти пороговые значения идут в следующем порядке по возрастанию:

– нижний неисправимый,
– нижний критический,
– нижний некритический,
– верхний некритический,
– верхний критический,
– верхний неисправимый.

В нормальном случае значение сенсора должно находиться в диапазоне между нижним и верхним некритическими порогами. Если оно выходит из этого диапазона, управляющий контроллер извещает об этом управляющий модуль шасси посылкой *события*. Начальные пороговые значения хранятся в SDR и могут быть динамически изменены командой Set Sensor Threshold. Пороги хранятся, считываются и устанавливаются в виде «сырых» однобайтовых значений.

Если значение величины, измеряемой сенсором, находится вблизи значения какого-либо порога и часто пересекает его в ту и другую сторону, то каждое такое пересечение может повлечь за собой посылку *события*. Для предотвращения неинформативного потока событий в этом случае используется гистерезис. При ненулевом значении гистерезиса после пересечения порога новые события не посылаются, пока значение сенсора не отойдёт в обратную сторону от значения порога на величину гистерезиса. Начальные значения гистерезиса хранятся в SDR и могут быть динамически изменены командой Set Sensor Hysteresis.

Дискретные сенсоры в качестве значения возвращают маску активных состояний, в которых находится данный сенсор. Она включает до 15 состояний, не обязательно взаимоисключающих. Подмножеством этого класса сенсоров являются логические сенсоры, для которых определены два взаимоисключающих состояния, например включён/выключен, есть ошибка/нет ошибки и т. д.

При изменении набора состояний для дискретного сенсора или при пересечении порогов для аналогового сенсора посылаются *события*. *Событие* представляет собой специальную IPMI-команду, которая посылается в обратном направлении – от управляющего контроллера к модулю управления шасси. События могут посылаться при входе или выходе из какого-либо состояния или при пересечении порога в том или ином направлении (с учётом гистерезиса). Специальная маска событий задаёт, в каком из указанных случаев будет послано событие. Начальная маска событий хранится в SDR и может быть изменена динамически командой Set Sensor Event Enable.

В поздних версиях спецификации введены *сенсоры с записью*. Они служат для абстрагирования управляющих сигналов, у которых можно устанавливать значения, или чисто программных сенсоров. Эти сенсоры поддерживают дополнительную команду Set Sensor Reading And Event Status для установки аналогового значения сенсора или текущего набора состояний для дискретного сенсора.

Формула преобразования значения для IPMI-сенсоров имеет вид: $y = L\,[(M*x+(B*10^{K1})*10^{K2}]$.

Коэффициенты M, B, K1, K2 – это целые числа со знаком, хранятся в SDR. L – это функция линеаризации (для многих сенсоров это тождественная функция, но используются также функции $1/x$, x^2, x^3, $\log x$ и т. д.). Если преобразование не может быть описано данной формулой для всех возможных значений, для сенсора реализуется команда Get Sensor Reading Factors, которая возвращает значения коэффициентов преобразования для текущего значения сенсора. В табл. 1 представлен набор команд IPMI, связанный с сенсорами.

Модель сенсоров IPMI существенно ограничивается тем, что аналоговые значения должны помещаться в 1 байт. Это ограничивает точность и диапазон измерений. Когда спецификация создавалась, это ограничение было приемлемым с учётом существующих физических датчиков. Сейчас многие датчики способны выдавать значения гораздо большей разрядности, и при передаче значения сенсора по протоколу IPMI происходит потеря точности.

Модель сенсоров в спецификации PMBus

Спецификация PMBus [3] описывает устройства, обычно блоки питания, доступные по шине I2C и работающие в режиме «только ведомые» (slave-only). Доступ к значениям физических датчиков осуществляется с помощью команд по шине I2C. Формат возвращаемых значений стандартизован, значения двухбайтовые (разрядность в два раза больше, чем в IPMI) и имеют один из двух возможных типов – прямой и линейный. Команды для получения значений частично стандартизованы.

Значения прямого типа – это целочисленные «сырые» значения, преобразуемые с помощью специальной формулы с использованием коэффициентов. Формула для преобразования значения имеет вид: $y = 1/m \cdot (x \cdot 10^{-R} - b)$.

Здесь m, R и b – целочисленные коэффициенты. Видно, что формула преобразования PMBus обратна упрощённой формуле преобразования IPMI: вместо умножения на коэффициент M используется деление на m, и вместо добавления B – вычитание b.

В отличие от IPMI, стандартного метода получения коэффициентов во время выполнения нет (коэффициенты описываются в документации на устройство или хранятся в памяти устройства, но нестандартным образом).

Значения линейного типа представляют собой уже преобразованные значения в формате с плавающей запятой в двухбайтовом формате (11 бит мантиссы + 4 бита характеристики + знаковый бит).

Использование устройств PMBus в системах AdvancedTCA ограничено:

– устройства работают в режиме slave-only и не могут использоваться как интеллектуальные управляющие контроллеры (в частности, не могут находиться на шине IPMB);
– у реальных устройств, как правило, очень много нестандартных функций (невозможно охватить все устройства единым программным кодом).

Устройства PMBus могут использоваться управляющим контроллером, находясь на его внутренних I2C-шинах, и показываться управляющим контроллером в виде набора сенсоров IPMI. Однако при передаче значений сенсоров от управляющего контроллера к модулю управления шасси по протоколу IPMI, из-за меньшей размерности значения сенсора в IPMI и различий в формуле преобразования, происходит неминуемая потеря точности значения.

Модель сенсоров в спецификации HPI

HPI (Hardware Platform Interface) – это стандарт управляющего интерфейса верхнего уровня, разработанный организацией Service Availability Forum [4, 5], в виде API-интерфейса, реализованного на языке C. Интерфейс HPI используется в системах AdvancedTCA для взаимодействия между прикладными программами и модулем управления шасси.

Таблица 1. Набор команд IPMI, связанных с сенсорами

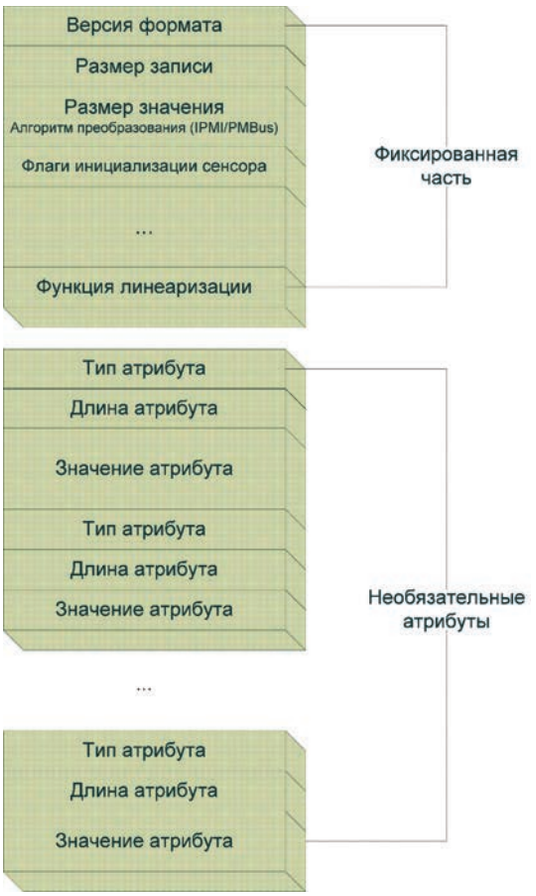
Название команды	Описание
Get Device SDR Info	Получает информацию о наборе SDR управляющего контроллера (количество SDR для каждого логического номера устройства и т.д.)
Get Device SDR	Получает содержимое конкретного SDR
Reserve Device SDR Repository	Резервирование доступа к набору SDR управляющего контроллера (для обеспечения целостности при считывании всего набора)
Get Sensor Reading	Считывает текущее значение сенсора и набор активных состояний
Get Sensor Threshold	Считывает текущие значения порогов для аналогового сенсора
Set Sensor Threshold	Устанавливает значения порогов для аналогового сенсора
Get Sensor Hysteresis	Считывает текущие значения гистерезиса для аналогового сенсора
Set Sensor Hysteresis	Устанавливает значения гистерезиса для аналогового сенсора
Get Sensor Event Enable	Считывает текущую маску разрешённых события
Set Sensor Event Enable	Устанавливает маску разрешённых событий
Re-arm Sensor Events	Перепосылает активные события при определённых условиях (необязательная команда)
Get Sensor Event Status	Считывает текущий статус событий
Get Sensor Type	Считывает тип сенсора (необязательная команда, для большинства сенсоров тип фиксирован в SDR)
Set Sensor Type	Устанавливает тип сенсора (необязательная команда)
Get Sensor Reading Factors	Считывает текущие значения коэффициентов преобразования значения (необязательная команда, для большинства сенсоров значения коэффициентов фиксированы в SDR)
Set Sensor Reading and Event Status	Устанавливает значение сенсора и/или набор активных состояний. Только для сенсоров с записью.
Platform Event	Событие (эта команда посылается от управляющего контроллера к приёмнику событий, как правило к управляющему модулю шасси)
Get Event Receiver	Получает адрес текущего приёмника событий (как правило, управляющего модуля шасси)
Set Event Receiver	Устанавливает адрес приёмника событий (как правило, управляющего модуля шасси)

Модель сенсоров в стандарте HPI очень сильно напоминает модель IPMI. Набор функций для работы с сенсорами похож на набор команд IPMI. Формат и поля описателя атрибутов сенсора RDR (Resource Data Record) аналогичны SDR. В стандарте также описано прямое отображение сенсоров IPMI на сенсоры HPI.

В отличие от модели IPMI, возвращаемое значение сенсора не требует преобразования на стороне клиента. Для сенсоров, полученных отображением из сенсоров IPMI, значение имеет размерность 64 бит и может быть целым числом или числом с плавающей запятой. Другие (собственно HPI-) сенсоры могут иметь значения более сложных типов, например массива текстовых строк.

Также в модели присутствуют управляющие объекты (controls). Эти объекты содержат значения различных типов (числовые, дискретные, логические), которые программа может читать и устанавливать. Эти объекты отображаются на сенсоры IPMI с записью или напрямую на IPMI-команды PICMG (управление светодиодами, управление вентиляторами). Например, для каждого вентилятора в шасси HPI-сервер создаёт управляющий объект, значение которого определяет скорость вращения вентилятора и может быть считано и установлено.

Хотя разрядность HPI-сенсоров составляет 64 бит, из-за низкой разрядности значений IPMI-сенсоров соответствующие HPI-сенсоры могут иметь точность и диапазон меньшие, чем соответствующие аппаратные датчики.



Формат расширенной информации о сенсоре

Расширение модели сенсоров в PICMG 3.7

Для поддержки аппаратных датчиков с размером значения больше 1 байт, а также PMBus-сенсоров, в PICMG 3.7 определена новая модель сенсоров с соответствующим набором команд. Основное отличие заключается в том, что аналоговые значения для расширенных сенсоров могут иметь размер от 2 до 8 байт. Для каждого конкретного сенсора размер значения фиксирован, но различные сенсоры могут иметь различный размер. Формат значения остаётся целочисленным, знаковым или беззнаковым в зависимости от атрибутов сенсора.

Расширенные сенсоры имеют смысл только как сенсоры, возвращающие аналоговые значения. Для дискретных сенсоров в спецификации PICMG 3.7 ничего не меняется – количество возможных состояний по-прежнему 15 и дискретные сенсоры представлены как обычные сенсоры. Также и аналоговые сенсоры, размер значения которых не превышает 1 байт, представляются обычными, а не расширенными сенсорами.

Для расширенных сенсоров отдельное пространство номеров не создаётся. Расширенные сенсоры присутствуют в списке обычных сенсоров, и для каждого из них есть SDR. Однако SDR-ы для таких сенсоров имеют специальный тип (event-only), который означает что такие сенсоры не поддерживают стандартные команды для чтения значения, а способны только на генерацию событий. Таким образом, расширенные сенсоры видимы в рамках старой модели (для программного обеспечения, не поддерживающего PICMG 3.7), но только как источники событий, но не как источники значений.

Новое программное обеспечение может считывать и устанавливать значение расширенного сенсора, а также работать с его порогами и гистерезисом, с использованием набора новых команд PICMG 3.7. При этом значение сенсора представляется в виде набора байтов (от 2 до 8) в формате little-endian (младший байт идёт первым). Размер значения и другие атрибуты сенсора задаются в расширенной информации о сенсоре (расширенный аналог SDR), для считывания которой также определены новые команды. В табл. 2 представлен набор команд IPMI в спецификации PICMG 3.7, связанных с расширенной моделью сенсоров.

Расширенная информация о сенсоре

Расширенная информация о сенсоре имеет формат, аналогичный формату SDR, и состоит из фиксированной и переменной части. Фиксированная часть содержит размер значения, формулу преобразования и некоторые другие обязательные атрибуты. Все необязательные атрибуты хранятся в переменной части в формате TLV

(type-length-value – тип-длина-значение) в произвольном порядке; каждому атрибуту присвоен однобайтовый идентификатор типа, позволяющий распознать тип атрибута при последовательном разборе расширенной информации. К необязательным атрибутам относятся: коэффициенты преобразования, значения порогов и гистерезиса по умолчанию, максимальное и минимальное значения сенсора и другие. Формат расширенной информации о сенсоре представлен на рисунке.

Интересно, что спецификация расширенных сенсоров PICMG 3.7 напрямую поддерживает PMBus-сенсоры. Специальное поле в фиксированной части расширенной информации указывает, какая формула используется для преобразования значения:

IPMI ($y = L\,[(M*x+(B*10^{K1})*10^{K2}])$ или

PMBus ($y = 1/M*(x*10^{-K2}-B)$).

Расширенная информация может иметь значительную длину, больше, чем максимальная длина команды IPMI. Для её считывания команда Get Extended Sensor Information использует тот же подход, что и её аналог Get Device SDR Info – считывание фрагментами с указанием в запросе смещения и длины фрагмента. Для обеспечения целостности используется идентификатор резервации – тот же, что используется при чтении SDR-ов. Он может быть получен стандартной командой Reserve Device SDR Repository.

Отображение на HPI

Отображение сенсоров HPI на расширенные сенсоры PICMG 3.7 пока не реализовано, но концептуально, с учётом того, что все команды модели расширенных сенсоров имеют аналоги в IPMI, а структура расширенной информации о сенсоре подобна структуре SDR, это отображение практически ничем не должно отличаться от отображения на стандартные сенсоры IPMI. Когда оно будет реализовано, проблемы, связанные с потерей точности и диапазона аппаратного датчика при его отображении в HPI через IPMI, будут решены.

Заключение

Таким образом, расширенная модель сенсоров в PICMG 3.7 преодолевает существенный недостаток модели сенсоров IPMI – слишком малый диапазон значений, возвращаемых сенсором, а также поддерживает напрямую сенсоры популярной архитектуры PMBus. Использование расширенной модели сенсоров PICMG 3.7 позволит осуществить полноценную программную поддержку современных аппаратных датчиков в архитектуре IPMI, без потерь точности и диапазона измерений.

Список литературы

1. PICMG Advanced Telecommunications Computing Architecture (AdvancedTCA) Base Specification. Revision 3.0. http://www.picmg.org

2. IPMI – Intelligent Platform Management Interface Specification, v2.0, Document Revision 1.1, October 1, 2013. http://www.intel.com/design/servers/ipmi/index.htm.

3. PMBus™ Power System Management Protocol Specification, Parts I,II. http://www.powersig.org

4. Service Availability™ Forum Hardware Platform Interface Specification SAI-HPI-B.03.01. September 18, 2008. http://www.saforum.org

5. Service Availability™ Forum Specification for HPI Mapping to AdvancedTCA® and MicroTCA® SAIM-HPI-B.03.02-xTCA. November 5, 2009. http://www.saforum.org

Таблица 2. Набор команд в PICMG 3.7, связанных с расширенной моделью сенсоров

Название команды	Описание
Get Extended Sensor List	Получает информацию о наборе расширенных сенсоров для управляющего контроллера (количество расширенных сенсоров для каждого логического номера устройства и список номеров сенсоров для одного логического номера). Аналог команды Get Device SDR Info
Get Extended Sensor Information	Получает расширенную информацию по номеру сенсора. Эта расширенная информация, в частности, содержит размер значения сенсора и коэффициенты трансляции. Аналог команды Get Device SDR
Get Extended Sensor Reading	Считывает текущее расширенное значение сенсора и набор активных состояний. Аналог команды Get Sensor Reading
Get Extended Sensor Threshold	Считывает текущие значения порогов для расширенного сенсора. Аналог команды Get Sensor Threshold
Set Extended Sensor Threshold	Устанавливает значения порогов для расширенного сенсора. Аналог команды Set Sensor Threshold
Get Extended Sensor Hysteresis	Считывает текущие значения гистерезиса для расширенного сенсора. Аналог команды Get Sensor Hysteresis
Set Extended Sensor Hysteresis	Устанавливает значения гистерезиса для расширенного сенсора. Аналог команды Set Sensor Hysteresis
Get Extended Sensor Reading Factors	Считывает текущие значения коэффициентов преобразования значения (необязательная команда, для большинства сенсоров значения коэффициентов фиксированы в расширенной информации о сенсоре). Аналог команды Get Sensor Reading Factors
Set Extended Sensor Reading	Устанавливает значение расширенного сенсора. Только для расширенных сенсоров с записью. Аналог команды Set Sensor Reading and Event Status.

Анна Нестерова, Юрий Якшин, ЗАО «РТСофт»

«Интернет вещей» – основная тенденция выставки SPS IPC Drives 2014

В конце ноября 2014 года в Германии (г. Нюрнберг) состоялась 25-я международная выставка SPS/IPC/DRIVES – одно из крупнейших мировых событий, посвящённых технологиям автоматизации производства, с широким спектром охвата – от встраиваемых компонентов до комплексных систем автоматизации.

Разделы выставки SPS IPC Drives 2014 (рис. 1) были посвящены следующим тематическим направлениям:

– Управляющая техника (Control technology);
– Промышленные компьютеры (IPCs);
– Приводные системы и компоненты (Drive systems and components);
– Человеко-машинные интерфейсы (Human-machine-interface devices);
– Системы связи промышленного назначения (Industrial communication);
– ПО промышленного назначения (Industrial software);
– Интерфейсы (Interface technology);
– Электромеханические компоненты (Mechanical infrastructure);
– Датчики (Sensor technology).

sps ipc drives

Electric Automation
Systems and Components
International Exhibition and Conference
Nuremberg, Germany, 25–27 November 2014

25 YEARS

Выставку, представленную 1602 экспонентами из 42 стран (1094, или 68,3% – из Германии) на площади 117 800 кв. м, посетило 56 787 человек (76,7% из них граждане Германии). Впервые для размещения выставки потребовалось 14 залов.

Рис. 1. Рабочий момент выставки

Организаторы выставки отметили растущий авторитет мероприятия на международной арене. Так, в 2014 году количество зарубежных участников выросло до 32 % (508 экспонентов). В первой пятёрке такие страны, как Италия (107 экспонентов), Китай (69 экспонентов), Швейцария (49 экспонентов), Австрия (31 экспонент) и США (25 экспонентов). От 10 до 22 экспонентов представили Нидерланды, Чехия, Великобритания, Франция, Турция, Индия, Тайвань, Словения, Южная Корея и Швеция.

Ключевой тенденцией мероприятия был показ ведущими игроками рынка продуктов и сервисов для создания решений, соответствующих идеологии «Интернета вещей» (Internet of Things – IoT). В области промышленной автоматизации эта идеология подразумевает объединение в глобальную вычислительную сеть взаимодействующих друг с другом, зачастую без участия человека, физических объектов – датчиков, приборов, машин, механизмов и тому подобных устройств, в целях повышения эффективности всех сфер производства (рис. 2).

Наиболее крупная экспозиция, посвящённая IoT, была представлена на стенде Kontron в виде продуктов холдинга и экосистемы партнёров, предлагающих базовые строительные блоки для создания IoT-решений: встраиваемые продукты – от модулей, промышленных компьютеров KBox и серверов до программного обеспечения для мониторинга состояния собственного оборудования (Kontron) (рис. 3–5); ПО McAfee для обеспечения безопасности данных (Intel); встраиваемые ОС Windows Microsoft Embedded и облачная платформа Windows Azure (Microsoft); услуги связи и сервисы для разработчиков решений IoT (Telekom Deutschland); ПО и сервисы по безопасности, передачи данных (WIBU и RTI).

Среди других ведущих участников рынка продукты и сервисы для IoT были также представлены на стендах ADLINK, GE, HEITEC (рис. 6–8) и других компаний. При этом некоторые из них используют региональные либо собственные концепции, схожие по смыслу с IoT. Так, например, в Германии популярна концепция Industry 4.0, а компания HEITEC продвигает концепцию HEITEC 4.0.

Рис. 2. Сенсорный дисплей с подключением к «Интернету вещей»

Рис. 3. Общий вид стенда Kontron

Рис. 4. Семейство промышленных компьютеров Kbox компании Kontron

Рис. 5. ПО для удалённого мониторинга оборудования Kontron

Рис. 6. Решение для «Интернета вещей» на стенде компании ADLINK

Рис. 7. Промышленный Интернет на стенде компании GE

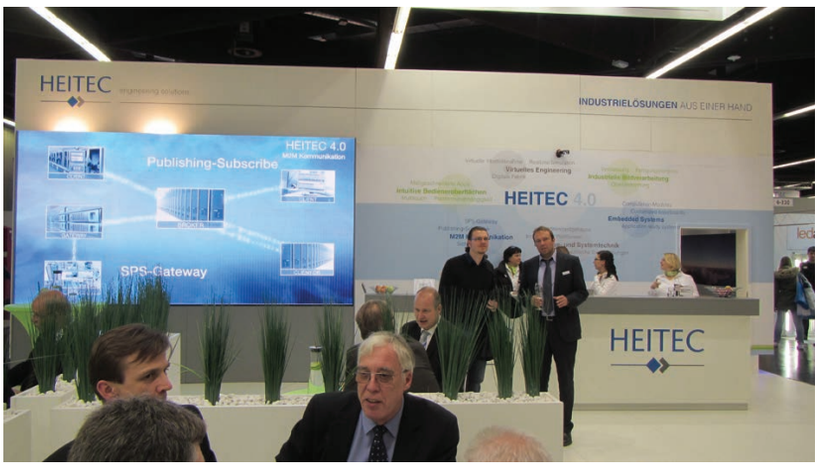


Рис. 8. Концепция «Интернета вещей» от компании HEITEC

Рис. 9. Стенд компании S&T

Среди активно развивающихся embedded-компаний, принявших участие в выставке, можно отметить компанию S&T (рис. 9), которая представила широкий спектр современных продуктов и сервисов – от промышленных компьютеров BoxPC и мониторов до сервисов по разработке одноплатных компьютеров и материнских плат, в том числе для использования в рамках IoT.

Анализ участия в выставке таких ведущих компаний, как Kontron, Adlink, GE, HEITEC и других, позволяет сделать вывод о том, что IoT – это глобальная идеология развития информационных технологий, которая ещё находится на стадии формирования. В настоящее время для использования в рамках IoT ключевые участники рынка встраиваемых компьютерных технологий, промышленной автоматизации и телекоммуникаций предлагают главным образом свои существующие продукты (например, шлюзы для m2m или серверы) и сервисы по разработке и системной интеграции, а также стремятся занять некоторые относительно новые ниши вроде ПО для облачных вычислений в промышленной автоматизации.

Этот вывод подтверждается и тематикой докладов на конференции, которая проходила в рамках выставки. Глубокие и плодотворные дискуссии велись вокруг докладов на такие темы, как «Облако в автоматизации» (Automation Cloud), «Большие данные» (Big Data), «Необычные приводы и умные материалы» (Unkonventionelle Antriebe und Smart Materials), «Энергоэффективность и управление энергией» (Energieeffizienz und Energiemanagement), «Платформа Industry 4.0», что так или иначе вписывается в идеологию «Интернета вещей».

Следующая выставка и конференция SPS IPC Drives 2015 состоится с 24 по 26 ноября 2015 года.

Леонид Акиншин

«РТСофт» и Intel провели совместный семинар и открыли лабораторию по «Интернету вещей»

В декабре 2014 г. в Инженерном доме «РТСофт» впервые состоялся уникальный семинар «Развитие идеологии „Интернета вещей“ в промышленности, энергетике, транспорте и системах специального назначения».

Организаторами семинара выступили компании «РТСофт» и Intel при участии компаний-партнёров – Kontron, «Кварта Технологии» и ФГУП ЭЗАН. Доклады на новаторскую тему «Интернета вещей» сделали эксперты ключевых бизнес-подразделений «РТСофт» и представители компаний-партнёров.

Во вступительном слове Надежда Соседко, директор отделения ВКТ «РТСофт», указала на глобальный характер идеологии «Интернета вещей» (Internet of Things – IoT) и связанных с ней изменений в деятельности компаний и людей. Продолжив эту мысль, Юрий Якшин, директор по маркетингу ВКТ «РТСофт», подробнее остановился на перспективных стратегиях, продуктах и сервисах для создания IoT-решений, предлагаемых «РТСофт» и компаниями-участниками семинара в рамках партнёрской экосистемы IoT в России (рис. 1, слева).

Павел Литвинов, начальник аналитического отдела «РТСофт», продемонстрировал на примерах тесную связь «Интернета вещей» с такими современными концепциями и трендами, как Big Data, облачные технологии, «умные дома» и «умные города». Само определение «умный» уже свидетельствует о принадлежности называемого явления к миру IoT, а первым массовым прикладным применением «Интернета вещей» можно считать системы умного учёта электроэнергии. Докладчик отметил, что у России есть огромный потенциал роста по направлению IoT и компания «РТСофт» вместе с партнёрами благодаря своим компетенциям вполне могут стать локомотивами этого роста.

Выступление Игоря Рудыма, менеджера по встраиваемым решениям Intel, было посвящено технологиям и подходам, которые корпорация Intel предлагает для разработки и создания вычислительных и коммуникационных систем для «Интернета вещей». Докладчик представил аналитические данные, в соответствии с которыми ожидается значительный рост рынка IoT в мире и в России. С точки зрения Intel, исходные неструктурированные данные генерируются на уровне сенсоров и первоначально обрабатываются (структури-

Рис. 1. Семинар открыли Надежда Соседко и Юрий Якшин

Рис. 2. Выступает Марсель ван Хелтен (Kontron)

Рис. 3. Надежда Соседко и Игорь Рудым открывают лабораторию «Интернета вещей»

руются) в интеллектуальных шлюзах перед их отправкой в «облака». Этот предварительный этап значительно уменьшает информационную нагрузку на каналы связи, снижает требования к ёмкости облачных хранилищ и делает данные более пригодными для последующего подробного анализа. Распределённые вычислительные мощности, необходимые для реализации подобных архитектур, могут создаваться на основе решений компании Intel и её индустриальных партнёров.

Свое видение концепции «Интернета вещей» представил Марсель ван Хелтен (Marcel van Helten), руководитель бизнес-блока «Промышленная автоматизация» компании Kontron (рис. 2). Он рассказал о влиянии IoT на мировой рынок встраиваемых компьютерных технологий, а также о взаимосвязи понятий M2M и IoT. На примере интеллектуального фермерского хозяйства докладчик показал, как «Интернет вещей» помогает повысить эффективность и экологичность предприятий с помощью увеличения их продуктивности и уменьшения потребления расходных материалов.

О продуктах и решениях корпорации Microsoft для «Интернета вещей» рассказал Валерий Дробышевский, коммерческий директор компании «Кварта Технологии». Особое внимание докладчик уделил Windows Azure – технологии организации облачного уровня «Интернета вещей» и встраиваемых операционных систем семейства Windows Embedded, хорошо подходящих для использования в «умных устройствах». Аппаратной составляющей «умных устройств» был посвящён доклад Руденко Сергея, ведущего менеджера направления встраиваемых модулей «РТСофт». Он рассказал о преимуществах сервисов по разработке интеллектуальных шлюзов и иных изделий «РТСофт» для IoT, основанных на стандартах COM Express и SMARC – они способны удовлетворять широчайшему диапазону требований заказчиков по таким показателям, как энергопотребление, габариты, производительность и жёсткость исполнения. А Олег Холодный, менеджер направления серверных платформ «РТСофт», представил профессиональные малошумные промышленные компьютеры серии KISS и встраиваемые необслуживаемые компьютеры серии KBox, позволяющие интегрировать любые устройства и системы в глобальную сеть.

Геннадий Кузнецов, заместитель директора центра программных разработок «РТСофт», описал на примерах различные аспекты разработки ПО для «Интернета вещей», а Михаил Усатов, начальник отдела разработки пользовательских приложений «РТСофт», рассказал о сервисах по созданию интегрированных систем для транспорта, в том числе не имеющих мировых аналогов.

Рис. 4. Решения, представленные в лаборатории «Интернета аещей»

Рис. 5. Посетители лаборатории «Интернета вещей»

Сергей Алёшин, инженер-конструктор ФГУП ЭЗАН, обратил внимание аудитории на преимущества убиквитарных информационных сетей и протоколов IPv6/6LoWPAN применительно к «Интернету вещей», а Денис Алексеев, продуктовый менеджер «РТСофт», представил инструментальную платформу «Платинум-РТ», новую разработку компании, призванную содействовать быстрому и эффективному воплощению идеологии «Интернета вещей» в промышленности в условиях импортозамещения.

Кульминацией семинара стало торжественное открытие лаборатории «Интернет вещей» – совместного проекта «РТСофт» и Intel при участии Kontron и «Кварта Технологии», состоявшееся в Инженерном доме «РТСофт». Лабораторию открыли Игорь Рудым (Intel) и Надежда Соседко («РТСофт») (рис. 3). Основными задачами лаборатории (рис. 4) являются создание и тестирование типовых IoT-решений на основе базовых блоков от «РТСофт», Intel и партнёров компаний.

Первые посетители лаборатории смогли воочию увидеть решения и системы, о которых говорилось в докладах (рис. 5), это:

– уникальная система онлайн-мониторинга транспорта с использованием спутниковых каналов связи,
– система безопасности на стационарных и подвижных объектах,
– система сбора и анализа данных в облаке с выдачей управляющих воздействий,
– решение для защиты данных в системах класса «Интернет вещей»,
– интеллектуальное решение для электрических сетей.

В ходе неформального общения гости и участники семинара обменялись мнениями по поводу перспектив «Интернета вещей» и обсудили, каким образом данная концепция изменит бизнес компаний и жизнь людей в недалёком будущем и то, какие подходы, решения и продукты будут при этом использоваться.

Новости рынка

«РТСофт» представил на выставке «Навитех» инновационную систему мониторинга транспорта

Компания «РТСофт» приняла участие в выставке «Навитех» и продемонстрировала инновационную систему онлайн-мониторинга транспорта с использованием спутниковых каналов связи – Intelligent Air.

Решения «РТСофт» для навигационной отрасли представлял на выставке центр программных разработок (ЦПР) компании. Высококвалифицированные и во многом уникальные программисты ЦПР создают оптимизированные аппаратно-программные платформы, осуществляют системное программирование и разработку специализированных протокольных стеков и библиотек для удалённого доступа к оборудованию, выполняют поддержку middleware для облачных технологий и решают многие другие задачи. На выставке «Навитех» они продемонстрировали созданную в партнёрстве с компанией «Сателлит Телеком» инновационную систему онлайн-мониторинга транспорта Intelligent Air (IntAir).

Система IntAir предназначена для непрерывного мониторинга транспортных средств и других подвижных объектов, в том числе в удалённых и труднодоступных районах, вне зон покрытия сетями сотовой связи. Причём именно там, где нет сотовой связи и бессильны традиционные системы мониторинга, IntAir рентабельно работает, становясь просто незаменимой для предприятий, имеющих транспортный парк и спецтехнику в таких районах.

Это достигается за счёт принципиально нового, инновационного подхода к слежению за объектами: Intelligent Air автоматически определяет доступные на данный момент для передачи сообщений каналы связи и выбирает самый оптимальный из них, оптимизируя расходы на мониторинг в зависимости от географических районов применения.

Посетители стенда «РТСофт» смогли на реальном примере увидеть работу IntAir и оценить её преимущества. Неудивительно, что повышенный интерес система Intelligent Air вызвала у представителей предприятий, эксплуатирующих спецтехнику, суда и другие транспортные средства вне зон действия сотовой связи. Заинтересовались передовой разработкой «РТСофт» и представители отрасли специальных применений, а также провайдеры услуг по мониторингу транспортных средств: внедрение системы Intelligent Air позволит им рентабельно решать задачи слежения за объектами.

Центр программных разработок «РТСофт» способен выполнять проекты по созданию системного программного обеспечения для различных применений в любых отраслях промышленности.

Источник: Пресс-служба «РТСофт»

Кристофер Халлинан (Christopher Hallinan), Mentor Graphics

Yocto Project: проблемы и возможности

С ростом сложности процессоров и систем возрастает сложность программного обеспечения, в частности такого крупного программного объекта с открытым исходным кодом, как Linux. Разрешить ряд серьёзных проблем, связанных со сложностью и совместимостью аппаратных средств, взаимозависимостями исходного кода и лицензированием открытого кода разработчикам специальных дистрибутивов Linux помогает проект Yocto Project.

Всего за четыре года с момента своего появления проект Yocto Project стал де-факто стандартом среди систем сборки дистрибутивов Linux для заказных встраиваемых систем. К этому проекту присоединились практически все основные компании-поставщики полупроводников и встраиваемых операционных систем, некоторые производители устройств и печатных плат, а также независимые поставщики программного обеспечения. Среди участников проекта много других организаций, и крупных, и небольших. С Yocto Project совместимо несколько серийно выпускаемых дистрибутивов Linux (официальный знак совместимости с Yocto Project показан на рис. 1). Проект Yocto Project это совместный проект некоммерческого консорциума Linux Foundation, который обеспечивает его поддержку (рис. 2).

Если вспомнить историю проектов с открытым исходным кодом,

Рис. 1. Официальный знак совместимости с Yocto Project

Рис. 2. Yocto Project – совместный проект с открытым исходным кодом, который предоставляет шаблоны, инструменты и методы, помогающие разработчикам создавать заказные системы на базе Linux

то можно отметить, что уровень отраслевого участия в рамках молодого проекта Yocto Project, по сути, беспрецедентный. Это можно расценивать как свидетельство ценности проекта. Некоторые коммерческие продукты, которые получили совместимость с Yocto Project, в настоящее время перечислены на сайте этого проекта.

С чем связан такой быстрый успех? Технический обзор

Yocto Project – совместный проект с открытым исходным кодом, который предоставляет шаблоны, инструменты и методы с целью помощи разработчикам в создании заказных встраиваемых систем на базе Linux, независимо от аппаратной архитектуры. Проект Yocto Project обеспечивает прочный фундамент, на котором строятся специализированные встраиваемые Linux-платформы. Такой вид совместной работы объединяет не только участвующие организации, но и большое количество проектов с открытым исходным кодом, которые можно эффективно использовать для создания заказных встраиваемых решений.

В Yocto Project интегрируется несколько проектов с открытым кодом, которые образуют рабочую среду для построения заказных встраиваемых дистрибутивов Linux. Основой этой рабочей среды служит система Poky, в которой используются технологии из двух проектов верхнего уровня: OpenEmbedded и подсистемы сборки BitBake. Проект OpenEmbedded управляет большим набором команд сборки, подмножество которых формирует уровень *oe-core* в пределах системы Poky. BitBake – это система сборки, отвечающая за интерпретацию команд сборки, которые в совокупности называют метаданными, содержащихся в уровнях *oe-core* и *meta-yocto*.

Poky – это система сборки и эталонный дистрибутив Linux для встраиваемых систем. На рис. 3 показаны элементы, которые входят в состав Poky. Кроме Poky могут быть сформированы дополнительные уровни метаданных, в том числе уровни BSP (пакеты поддержки платформы), уровни микропрограммного обеспечения и уровни приложений пользователя. Следует отметить, что документация Yocto Project, которая входит в состав пакета Poky, выполнена на высоком уровне, принимая во внимание то, что обычно ПО с открытым исходным кодом имеет плохую документацию или её вовсе не существует.

Наиболее распространённый тип метаданных – рецепт. Это набор команд для сборки пакета программ, главным образом в рамках среды кросс-разработки для создания специализированной аппаратной платформы встраиваемой системы на базе отдельной платформы (рис. 4). Рецепт – это файл, содержащий команды сборки (метаданные) или, что чаще, набор файлов, наподобие входного файла на C, который определяет #include-файлы. Проект Yocto Project содержит рецепты для многих сотен программных пакетов, которые облегчают сборку этих пакетов в среде кросс-разработки.

Помимо программных пакетов Yocto Project содержит также рецепты для сборки ядра Linux для различных широко распространённых эталонных плат, например плат серии Beagleboard на базе процессоров Texas Instruments и плат серии Sabre на базе процессоров Freescale Semiconductor. Он также имеет рецепты для сборки межинструментальных и стандартных библиотек рабочих программ (C/C++), хотя большинство поставщиков серийных ОС, которые продвигают продукты на базе Yocto Project, поставляют их вместе с серийно выпускаемыми средствами, интегрированными вместе с базовыми эталонными дистрибутивами и системами сборки Yocto Project.

Разработка с помощью Embedded Linux: проблемы

Сказать, что разработка дистрибутивов Embedded Linux – задача непростая, подобно утверждению, что сто миллионов строк программного текста – это много. Конечно, так оно и есть! Сложность программного обеспечения быстро растёт, кроме всего прочего, в результате внедрения последних технологических достижений в аппаратные платформы и процессоры

Рис. 3. Элементы, входящие в состав Poky

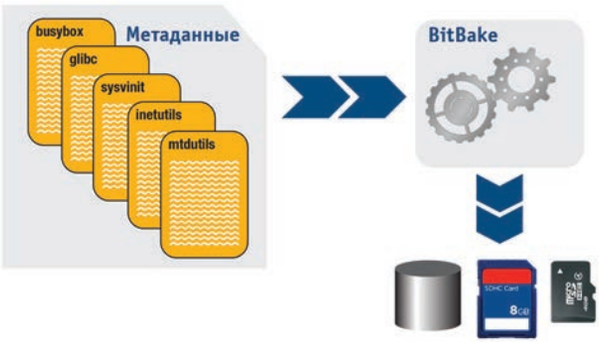


Рис. 4. Упрощенная сборка Yocto Project

класса система-на-кристалле (СнК). Многие современные встраиваемые устройства предназначены для «Интернета вещей» и содержат СнК с интегрированной периферией, такие как усовершенствованные графические подсистемы с поддержкой OpenGL/ES, интерфейсы SD/MMC-карт, флэш-памяти, Wi-Fi, Bluetooth, Ethernet, USB host/device, а часто и видео- и аудиокодеки с аппаратным ускорением.

Сборка систем Embedded Linux включает в себя интегрирование сотен различных программных пакетов из бесплатных и коммерческих программ, разбросанных по всему миру. Кроме того, заказная аппаратная платформа требует, чтобы совместимое с ней ядро Linux было портировано на эту специализированную аппаратную платформу, а загрузчик ОС был также адаптирован под эти аппаратные средства. Также нужно, чтобы под данную архитектуру был настроен и оптимизирован набор инструментов.

Наиболее проблемным аспектом интегрирования множества уникальных и независимых программных пакетов может стать выбор версии пакетов. Действительно, многие, если не большинство, программных пакетов разработаны и поддерживаются изолированными сообществами и поэтому выпускаются совершенно независимо друг от друга и часто с непредсказуемой частотой. Программные пакеты, которые зависят от других базовых пакетов программ (например, приложения, которые используют системные библиотеки) должны иметь согласующиеся между собой версии, чтобы их работа была корректной. Хотя большинство разработчиков никогда специально не нарушает принцип совместимости снизу вверх, тем не менее несовместимость «родственных» пакетов встречается достаточно регулярно.

Такая несовместимость наиболее очевидна в программных пакетах, которые содержат многие зависимости, такие как графические программы и пользовательские интерфейсы. Они часто имеют длинные цепочки зависимых соединений, требующих шрифтовых библиотек, библиотек виджетов, библиотек устройств (к примеру, USB) и других системных библиотек, таких как сетевые утилиты и утилиты конфигурации системы. Возьмем, например, mplayer – медиа-плейер с открытым исходным кодом. Команды сборки в рамках Yocto Project для mplayer насчитывают 21 взаимозависимость (главным образом, библиотек), которые требуются для построения многих из этих библиотек, причём сами библиотеки тоже имеют взаимозависимости. Все эти библиотеки и их взаимозависимости должны быть протестированы для проверки возможности совместной работы, даже если они в значительной степени разрабатывались независимо, с разной частотой выхода новых версий и вне рамок официального сотрудничества.

Разработчики и организации, для которых они работают, должны осознавать трудности, связанные с вопросами лицензирования открытого кода. Это ещё одна существенная проблема для производителей встраиваемых Linux-устройств. Типовой дистрибутив Embedded Linux содержит свыше одной сотни различных лицензий открытого кода. Для примера можно взять Android-смартфон или какой-либо другой смартфон и найти сотни страниц текста лицензии на эти устройства. Некоторые организации проводят политику, которая направлена на предотвращение распространения определённых типов лицензий открытого кода, и это тоже проблема. Проект Yocto Project имеет инструменты и возможности, помогающие управлять распространением программного обеспечения с открытым исходным кодом.

Новые возможности

Пожалуй, наиболее весомый вклад за последние шесть месяцев проект Yocto Project получил в виде новых компаний-членов и участников проекта. Компания Freescale Semiconductor присоединилась к проекту как участник золотого уровня. Также к проекту присоединились компании LG, Dell, Renesas и OS Systems в качестве серебряных участников. За последние несколько месяцев в качестве участников Yocto Project зарегистрировались шесть новых организаций. В прошлом году зарегистрированы и получили одобрение консультативного совета Yocto Project десяток новых продуктов и открытых проектов. Сюда входит проект GENIVI, который обеспечивает эталонную базу для автомобильной Linux-платформы, а также, в числе прочих, Linux-продукты от Enea, Wind River, Intel и Mentor Graphics. На веб-сайте Yocto Project представлен список членов, участников и продуктов, зарегистрированных в брендинг-программе Yocto Project.

Toaster. Одна из самых интересных подсистем Yocto Project – прикладной программный интерфейс Toaster. Он был введён в Yocto Project 1.6 в апреле 2014 года. Интерфейс Toaster обеспечивает разработчика инструментами визуализации, работающими на базе веб-сети, для детального контроля создаваемой сборки. Используя Toaster, можно узнать, как был собран пакет, исследовать цепочки зависимых соединений и составить список пакетов в заданном виде. Одна из наиболее полезных функций модуля Toaster – возможность просмотра метаданных пакета и выявления, какие файлы отвечают за коррекцию каждой переменной матаданных. До

появления интерфейса Toaster эта работа была трудоёмкой и рутинной.

Hob. Являясь относительно новым дополнением Yocto Project, Hob продолжает привлекать внимание разработчиков, использующих этот проект. Hob – это графический пользовательский интерфейс для системы сборки BitBake. Интерфейс Hob наиболее полезен для новичков Yocto Project, поскольку позволяет вносить первичные изменения в конфигурацию проекта. Использовать Hob можно, например, для того, чтобы выбрать тип создаваемого изображения (например, графический или неграфический), а также тип пакета поддержки платформы (BSP). Hob можно также использовать для добавления функциональности базового образа. Например, используя Hob, можно легко добавлять программные пакеты в образ файловой системы. Hob содержит множество меню настройки, которые позволяют разработчику осуществлять необходимый выбор пунктов из предлагаемого списка, когда новичку может быть не совсем ясно, какой выбор оптимальный.

Притягательная сила Yocto Project для отрасли объясняется тем, что он обеспечивает широкий выбор программного обеспечения, которое можно легко транслировать в когерентную систему. Этот проект останется важным источником передовых технологий как для любителей, так и для коммерческих поставщиков аппаратных средств, программного обеспечения, операционных систем и инструментов.

• Студенты • Лето • РТсофт •

Компания «РТСофт» активно сотрудничает с ведущими техническими ВУЗами столицы и уже несколько лет подряд проводит открытые конкурсы среди студентов, поощряя их интерес к области встраиваемых систем. В данном процессе задействованы ведущие инженеры «РТСофт», имеющие успешной опыт работы в Linux-комьюнити и распределённых международных командах.

В рамках Академической программы компании этим летом с 6 по 19 июля пройдёт «Летняя Школа» для студентов ВУЗов.

Цель занятий – обучение будущих специалистов современным встраиваемым технологиям, знакомство с передовыми практиками в разработке программного обеспечения.

Школа будет состоять из **двух групп**.

В **первую** приглашаются студенты 1-2 курса, минимальным условием участия которых является знание языка программирования C. В ней будут прочитаны лекции по особенностям системного программирования Linux. Будут рассмотрены основные этапы разработки ПО, в том числе тестирование и отладка, а также особенности систем реального времени.

В фокусе **второй** группы – углублённое изучение ядра Linux и разработка драйверов и основные принципы построения встраиваемых систем. От участников требуется знание языка C и желательны базовые знания курсов «Операционные Системы» и «Архитектура ЭВМ».

После теоретического курса участники попробуют на практике разработать небольшой проект, архитектура и код которого будут прорецензированы экспертами ЗАО «РТСофт».

Участие в школе бесплатное, нужно лишь отправить заявку по адресу rt.practic@dev.rtsoft.ru, указав ФИО, курс и учебное заведение.

Если Вам интересны системное программирование, ядро Linux, технологии виртуализации, задачи распознавания изображений, встраиваемые технологии –следите за академической программой ЗАО «РТСофт». В 2015 году планируются новые конкурсы, семинары и другие интересные события!

Айрат Садыков. Auriga, Inc.

Процесс разработки медицинского программного обеспечения: краткий обзор требований стандарта IEC–62304

В статье рассматриваются особенности разработки программного обеспечения (ПО) для медицинских устройств в соответствии с международным стандартом IEC-62304 (ГОСТ Р МЭК 62304-2013), основные подходы и требования к организации процесса такой разработки.

1. Вступление

Трудно представить себе более сложную и жизненно необходимую индустрию, чем медицина. По оценкам аудиторско-консалтингового сообщества Deloitte, в ближайшие годы основными драйверами роста рынка здравоохранения станет стареющее население – к 2050 году количество людей старше 60 лет увеличится по крайней мере в 3 раза. Вместе с общим ростом населения (по оценкам ООН к 2050 году население Земли достигнет 9,6 миллиардов человек) это безусловно создаст дополнительный спрос на услуги сектора здравоохранения.

Помимо этого, медицинские технологии вносят значительный вклад в мировую экономику. Согласно исследованию рынка, опубликованному лондонской компанией Evaluate, к 2020 году мировые продажи медицинских технологий достигнут 514 миллиардов долларов, а затраты на исследования и разработку будут расти в среднем на 4,2 % в год и в итоге достигнут 30,5 млрд к 2020 году.

Само понятие «медицинские технологии» включает в себя свыше 500 000 различных видов услуг и продуктов диагностики, мониторинга и лечения заболеваний, распределённых по 16 категориям. С каждым днём медицинские устройства — от набирающих популярность носимых гаджетов до систем жизнеобеспечения и реанимационных комплексов — становятся всё сложнее, вбирая в себя всё большую функциональность и становясь всё более независимыми.

Демонстрируемый рост числа устройств и технологий стимулируется повышенным спросом на новые, более эффективные и быстрые программные решения, хотя в то же время и цена, и последствия принимаемых решений могут стать чрезвычайно высокими и оказать воздействие не только на сотрудников, саму компанию, пациентов, но и на всю систему здравоохранения. На рынок выходят новые игроки, прежде «незамеченные» в области медицинских технологий – Samsung, Verizon, Reebok, Sony и другие.

Необходимость строгой стандартизации отрасли отражает и тот факт, что в сентябре 2014 года Международный форум регуляторов медицинских изделий (IMDRF) опубликовал окончательную версию документа «Программное обеспечение как устройство медицинского назначения: возможные стандарты категоризации рисков и соответствующие факторы», который присваивает первоочередной приоритет рискам, связанным с регулированием программного обеспечения для медицины, отмечая значительный рост такого ПО, многообразие его видов и платформ, на которых оно может использоваться.

Таким образом, мы подходим к крайне важному вопросу стандартизации разработки ПО. Для чего нужны стандарты в данной отрасли? Во-первых, для обеспечения надёжности медицинского ПО: медицинское оборудование должно работать чётко и безотказно, выполнять именно тот набор действий, для которого оно предназначалось, в результате чего будет достигнут ожидаемый эффект. От этого зависит не только здоровье пациента, но зачастую и его жизнь.

Во-вторых, стандарты необходимы для обеспечения совместимости медицинского оборудования: все эти новые устройства генерируют данные в разных форматах и используют технологии, несовместимые между собой. Для своевременного и качественного оказания помощи пациенту экспертное сообщество должно урегулировать вопросы, связанные с функциональной совместимостью и межсетевым взаимодействием этих устройств.

Приступая к созданию медицинского ПО, разработчик должен осознавать, что его новый продукт может потенциально нанести вред людям. Он должен понимать, что требования стандартов вызваны необходимостью обезопасить будущих пользователей, пациентов, минимизировать как возможный вред и его последствия, так и вероятность возникновения опасной для пользователя ситуации.

2. Общая информация о стандартах разработки медицинского ПО

«Три кита» разработки медицинского ПО – это три международных стандарта:

1. IEC-62304: Процессы жизненного цикла программного обеспечения – требования к процессу разработки медицинского ПО (ГОСТ Р МЭК 62304-2013).

2. ISO-14971: Требования для уменьшения рисков при разработке медицинского ПО (ГОСТ ИСО 14971-2011).

3. ISO-13485: Требования к системе управления качеством при разработке медицинского ПО (ГОСТ Р ИСО 13485-2004).

Взаимосвязь различных стандартов разработки программного обеспечения для медицинского оборудования показана на рис. 1.

2.1. Общие требования

В целом разработка медицинского ПО строится по так называемой «evidence based»-системе. Это означает, что вы как разработчик должны фиксировать артефакты на всех фазах разработки продукта. Наличие записей позволяет:

– отследить весь процесс разработки;

– формализовать все требования, отслеживать соответствие им как в процессе создания продукта, так и после его выхода на рынок;

– убедить регулятора в том, что ваше ПО соответствует всем требованиям стандартов.

И это исключает ситуацию, при которой «в какой-то момент было принято определённое решение, но кем, зачем и почему, никто уже не знает».

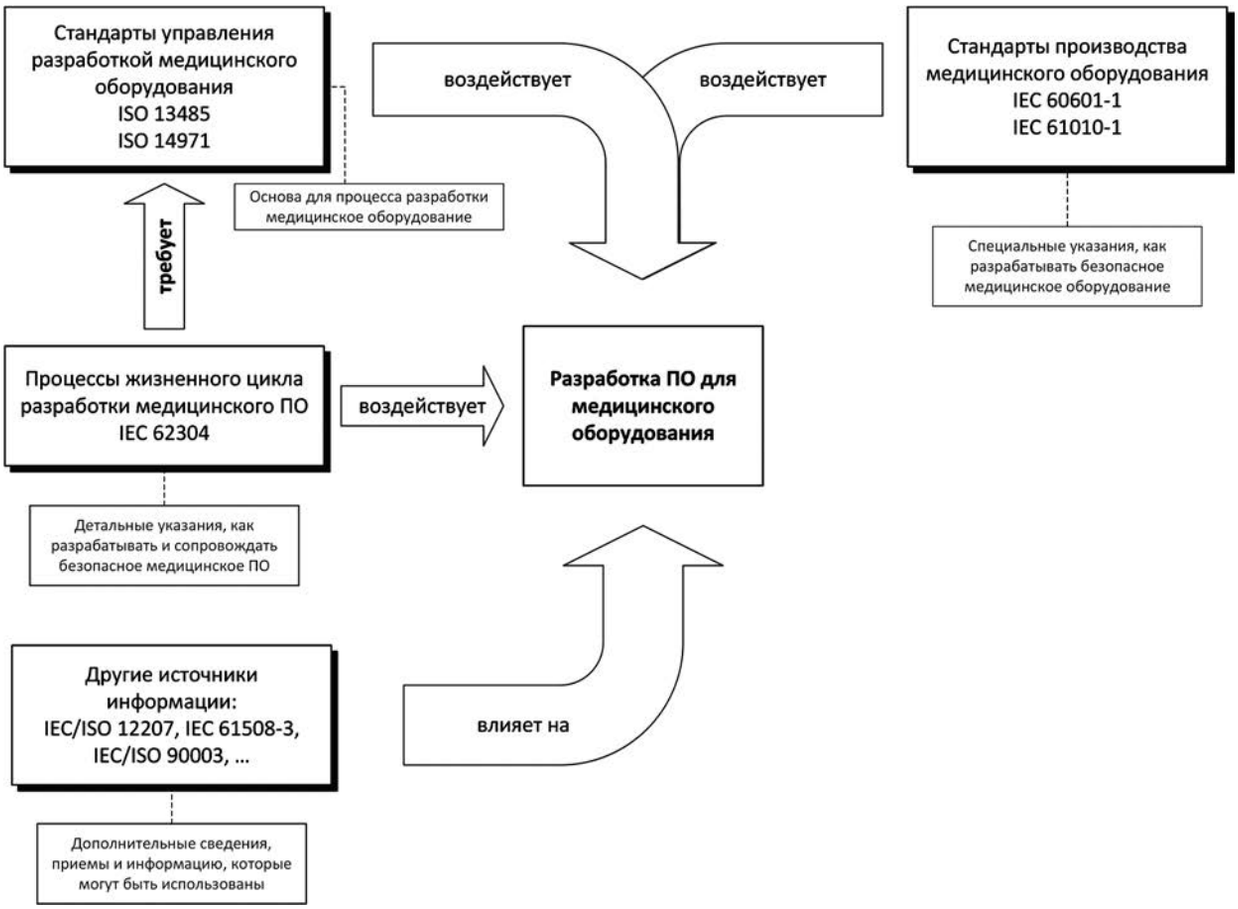


Рис. 1. Взаимосвязь различных стандартов разработки ПО

Довольно часто стандарты содержат лишь требования о том, *что* должно быть сделано, но не говорят о том, *как* это должно быть сделано. Это объясняется просто – стремительное развитие технологий и появление новых устройств приводят к невозможности предусмотреть детальные процедуры и инструкции для всех компаний и изделий.

Однако в стандартах содержится требование к производителям описать и задокументировать свои процедуры и инструкции: это понадобится для обоснования выбранных проектных и технических решений.

В дополнение к этому стандарты прямо предписывают использовать предыдущий опыт разработки аналогичных продуктов и весь набор оставшихся артефактов (включая в первую очередь оценки и управление рисками) при разработке новых продуктов. В частности, такое требование содержат разделы 4.1, 4.4 и 9 в ISO-14971, раздел 7.3.2 в ISO-13485. Это относится не только к изучению опыта самой компании-разработчика, но и к изучению различных данных и публикаций в открытых источниках, требований регуляторов и отчётов производителей аналогичного оборудования. Разработчиками стандартов в этом случае движет не желание сэкономить ресурсы производителей медицинского оборудования, а стремление напомнить о необходимости использовать уже накопленный опыт для снижения рисков для новых пользователей.

2.2. Терминология

В сфере разработки медицинского ПО и оборудования используется ряд терминов (здесь и далее используются соответствующие определения терминов из стандартов ISO), которые имеют особое значение. Рассмотрим основные из них:

- «медицинское изделие» – любой инструмент, аппарат, прибор, устройство, имплант, программное обеспечение или изделие, которое предназначается производителем для использования в целях диагностики, профилактики, лечения или облегчения болезни, компенсации повреждений и т. д. С более точным определением вы можете ознакомиться в тексте стандарта ISO-13485:2003, определение 3.7;
- «вред» (harm) – нанесение физического повреждения или другого вреда здоровью людей, вреда имуществу или окружающей среде;
- «опасность» (hazard) – потенциальный источник вреда;
- «риск» (risk) – сочетание вероятности причинения вреда и тяжести этого вреда;
- «серьёзная травма» (serious injury) – повреждение или заболевание, которое прямо или косвенно:
  - несёт угрозу жизни;
  - приводит к стойкому ухудшению функционирования организма или постоянному ущербу (необратимому повреждению) структуры тела, или
  - требует медицинского или хирургического вмешательства с целью предотвращения стойкого ухудшения функционирования организма.
- «программное обеспечение неизвестного происхождения» (software of unknown provenance, SOUP – В ГОСТ Р МЭК 62304-2013 используется аббревиатура «ПОНП») – программный элемент, который уже разработан и общедоступен, но не был предназначен для включения в состав медицинского изделия (также известен как «готовое ПО»), или программное обеспечение, разработанное ранее, для которого недоступны требуемые документы, сопровождающие процесс разработки;
- «прослеживаемость» (traceability) – степень, до которой может быть установлена взаимосвязь между двумя или более результатами (продуктами) процесса разработки.

Кроме того, определяется три уровня декомпозиции ПО:

- программная система (верхний уровень) – совокупность программных элементов, предназначенных для выполнения конкретной функции или набора функций; может быть разделена на подсистемы медицинского изделия;
- программный элемент – составная часть программной системы; каждый элемент состоит из программных модулей или может быть разложен на другие программные элементы;
- программный модуль – неделимый программный элемент (самый нижний уровень декомпозиции). Это элемент программной системы для тестирования или управления конфигурацией ПО, который не может быть разделён на другие элементы.

2.3. Немного о «китах»

2.3.1. IEC–62304

Этот стандарт описывает жизненный цикл разработки медицинского ПО. В отличии от двух других, он относится только к программному обеспечению, которое понимается в нём как составная часть медицинского изделия. Даже если это изделие состоит только из программного обеспечения (ГОСТ Р МЭК 62304-2013. Раздел 1.2.). Своеобразным «эхом» именно такой интерпретации является тот факт, что в данном стандарте «забыли» про такие важные фазы процесса разработки, как валидация создаваемого продукта и его финальный выпуск. В нем указывается, что этот стандарт «обычно используется совместно с другими применимыми стандартами при разработке меди-

цинских изделий» (ГОСТ Р МЭК 62304-2013. Раздел 1.3.). Примером такого более общего стандарта может являться МЭК 60601-1.

В данной статье мы затронем лишь небольшую часть стандарта IEC-62304. Этот стандарт основан на ISO-12207, в котором определён жизненный цикл программного обеспечения в целом, но добавлен ряд отличий, специфичных для разработки именно медицинского ПО.

2.3.2. ISO–14971

В этом стандарте рассказывается о том, каким образом должно осуществляться управление рисками на протяжении всего жизненного цикла медицинского изделия. В него включается, в частности, анализ риска, оценка риска и собственно управление риском. Следует помнить, что когда в медицинских стандартах говорится о рисках, то подразумевается только риски вреда и опасности для пациентов и пользователей в целом. Различные проектные риски, такие как риск превысить бюджет или не успеть в отведённые сроки, в них даже не рассматриваются. Этот стандарт не имеет близких аналогов в семействе ИСО.

2.3.3. ISO–13485

Как и IEC-62304, данный стандарт имеет своего «родителя» -- пожалуй, самого известного в семействе ИСО стандарта «ISO-9001: Системы менеджмента качества». В ISO-13485 даже сохраняется такая же структура и нумерации разделов, как и в ISO-9001. Но, разумеется, он тоже был переработан для применения в разработке медицинских изделий.

3. IEC–62304: Процесс разработки ПО

Стандарт IEC-62304:2006 Medical device software – Software life cycle processes (Программное обеспечение на медицинские изделия – Процессы жизненного цикла программного обеспечения) описывает процесс создания медицинского ПО (ГОСТ Р МЭК 62304-2013. Введение):

«Настоящий стандарт определяет основу ПРОЦЕССОВ жизненного цикла совместно с ДЕЯТЕЛЬНОСТЬЮ (ДЕЙСТВИЯМИ) и ЗАДАЧАМИ, необходимыми для проектирования и технического обслуживания безопасного ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ МЕДИЦИНСКИХ ИЗДЕЛИЙ. Настоящий стандарт определяет требования для каждого ПРОЦЕССА жизненного цикла. Каждый ПРОЦЕСС жизненного цикла далее подразделяется на некую совокупность видов ДЕЯТЕЛЬНОСТИ, большинство из которых, в свою очередь, разделены на ЗАДАЧИ».

Обзор процессов разработки программного обеспечения схематически представлен на рис. 2.

Обзор процессов обслуживания программного обеспечения схематически представлен на рис. 3.

3.1. Классы ПО

Когда вы приступаете к разработке медицинского ПО, одной из первых задач должно стать определение максимального вреда, который может быть нанесён будущим пользователям (пациентам, операторам или окружающей среде) вашим ПО или оборудованием.

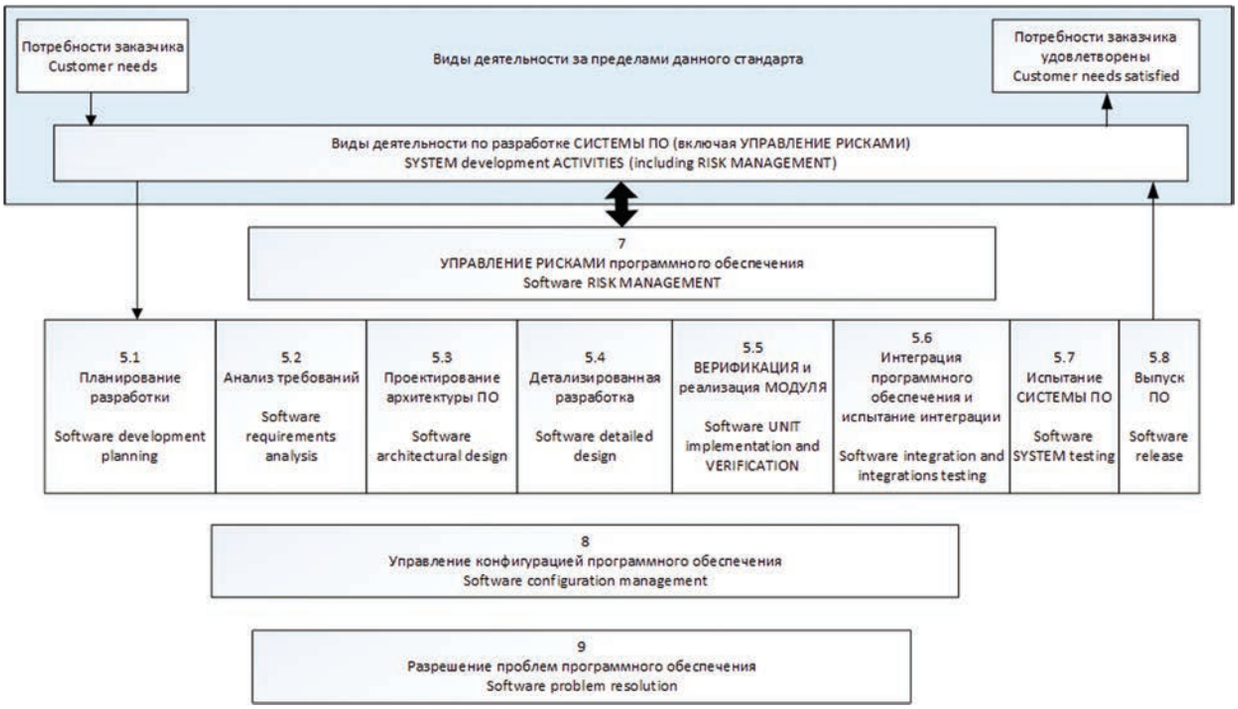


Рис. 2. Обзор процессов разработки ПО

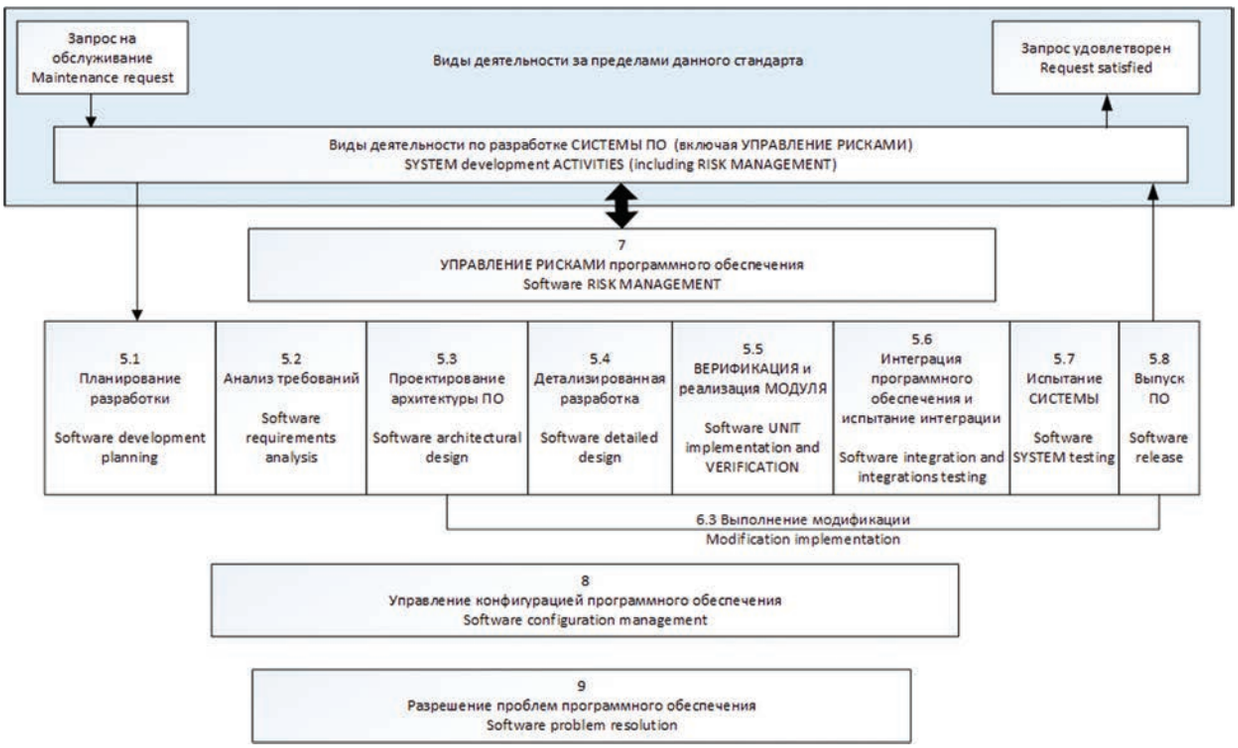


Рис. 3. Обзор процессов обслуживания ПО

В зависимости от степени возможных последствий для пользователей в стандарте IEC-62304:2006 определяется три класса медицинского ПО:

- класс A: отсутствует какой-либо риск причинения вреда здоровью;
- класс B: серьёзные травмы невозможны, но возможны незначительные травмы или повреждения (т. е. такие, которые проходят легко и не требуют дополнительного лечения);
- класс C: возможны серьёзные травмы или смерть.

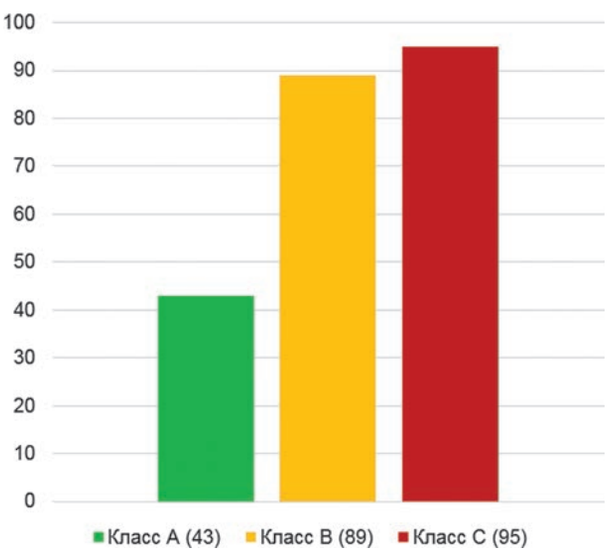


Рис. 4. Сравнение количества процессных активностей в зависимости от класса ПО

Чем выше класс – тем выше должна быть надёжность и отказоустойчивость разрабатываемого программного обеспччения. Классификация ПО на стадии разработки необходима не только для максимального обеспечения безопасности пользователей и пациентов (в IEC-62304 отдельно подчёркивается, что если опасность может быть следствием отказа в работе ПО, то вероятность такого события должна быть принята за 100%), но также для планирования трудозатрат компании. Из диаграммы сравнения количества требуемых стандартом процессных активностей (рис. 4), отчётливо видно, что в ваших интересах как можно раньше определить класс разрабатываемого ПО. Если учитывать при этом, что трудозатраты растут нелинейно с увеличением требуемых процессных активностей, то разница будет даже больше, чем показано на рис. 4.

3.2. SOUP

Когда вы начинаете разработку ПО, то, разумеется, не начинаете создавать всё с нуля, включая разработку собственной операционной системы, компиляторов, сред разработки и сопутствующих библиотек. Вы будете использовать какое-либо написанное ранее ПО, причём разработанное не только вами, но и другими разработчиками. Для обозначения всего разнообразия такого ПО был введён термин «SOUP» (software of unknown provenance – ПО неизвестного происхождения, ПОНП).

SOUP – это любое ПО, которое создавалось без учёта требований процессов, необходимых для раз-

работки медицинского ПО. Оно включает в себя составляющие, необходимые для создания любого программного продукта: операционная система, драйверы, динамические (runtime) библиотеки, компоненты с открытым или закрытым исходным кодом.

Инструменты, применяемые при разработке ПО, такие как интегрированные среды разработки (IDE) и компиляторы, не являются SOUP-компонентами. Исключением являются JIT-компиляторы (Just-in-time, динамическая компиляция), которые попадают в категорию SOUP-компонентов. Причины, думаем, тоже понятны: исполняемый код, получаемый в результате работы классического компилятора, всегда остаётся неизменным, тогда как при использовании JIT-компилятора поток исполнения может изменяться от запуска к запуску, даже при сохранении идентичной аппаратной и программной среды исполнения. И в этом случае бремя доказательства корректной работы JIT-компилятора падает на разработчика медицинского ПО.

Использование SOUP-компонентов в зависимости от класса ПО:

– класс A: без каких-либо ограничений;
– класс B: должны быть изучены риски использования SOUP-компонентов и предоставлены документы, обосновывающие их применение; требования к аппаратным и программным средствам системы, необходимым для правильной работы SOUP-компонентов, должны быть задокументированы;
– класс C: ещё более тщательная оценка рисков. На практике это будет означать, что могут использоваться только простые, хорошо документированные функции.

3.3. Понижение класса ПО

После того как вы определились с классом вашего ПО и использованием SOUP-компонентов, то, конечно же, зададитесь вопросом, есть ли возможность сократить затраты на разработку, не подвергая при этом будущих пользователей дополнительному риску. По определению, класс задаётся максимально возможным для данного ПО ущербом. Однако в стандарте определяется два способа понижения класса (раздел 4.3):

1. Управление рисками: если в результате этой процедуры риск ущерба, который может быть вызван отказом ПО, уменьшается до приемлемого (по определению ISO-14971) на аппаратном уровне или уменьшается вероятность или последствия такого риска, то возможно уменьшение класса на один (и только на один) шаг, т. е. с C на B или с B на A;

2. Применение сегрегации: разделение ПО на изолированные элементы таким образом, чтобы отказ ПО в одном элементе не влиял на другие.

3.3.1. Управление рисками

Например, мы пишем программу для управления роботом-хирургом и очевидно, что наше ПО относится к классу C. Каким образом можно его понизить? Проведём исследование различных способов уменьшения риска. Допустим, манипулятор нашего робота с закреплённым скальпелем имеет значительное число степеней свободы и большой размах механической «руки». Один из рисков заключается в том, что в результате отказа ПО наш робот может выйти за пределы оперируемой области и нанести серьёзный ущерб пациенту. Каким образом можно минимизировать риск такого вреда? Предложим добавить в конструкцию аппаратный ограничитель – специальную рамку, ограничивающую движения скальпеля оперируемой областью и обладающую механической прочностью, заведомо превышающей усилие манипулятора. Таким образом, выполняется требование стандарта: отказ ПО не приводит к неконтролируемому и потенциально смертельно опасному ущербу для пациента, а ограничен заранее известной локальной областью. Здесь мы делаем небольшое, но довольно важное допущение: «любые действия скальпелем в заданной «рамкой» области не приведут к серьёзному ущербу для пациента». В реальных условиях нам, скорее всего, не удастся доказать обоснованность такого смелого допущения, либо наша «рамка» сама будет представлять собой довольно сложное техническое устройство.

Другой пример: мы пишем ПО для управления специальной манжетой, в которую накачивается воздух. Манжета предназначена для удержания шеи пациента в определённом положении. Самый большой риск заключается в том, что отказ ПО может привести к неконтролируемому нагнетанию воздуха и задушить пациента или пережать ему кровеносные сосуды. С помощью дополнительных исследований мы установим безопасный и максимально допустимый уровни давления в манжете. Для минимизации риска удушения можно предложить два технических решения: установка клапана для сброса «лишнего» давления и введение дополнительных требований к выбору насоса – таких, чтобы он по своим техническим характеристикам не мог поднять давление выше допустимого уровня. Таким образом, выполняются требования стандарта: последствия возможного отказа ПО (а вероятность такого отказа, напомню, мы обязаны принимать за 100%) мы предотвратили на аппаратном уровне.

3.3.2. Сегрегация

Пусть это будет снова наш робот-хирург. Разумеется, это будет сложное ПО со множеством настроек, развитым графическим интерфейсом пользователя,

интегрированное с системой визуализации данных с компьютерного или магнитно-резонансного томографа, базой данных пациентов больницы и в нём даже будет внедрён комплекс телемедицины с возможностью проводить видеоконференции. Неужели нам придётся разрабатывать всё наше ПО, проводя его по всем требуемым процессам класса С?

Стандарт снова говорит нам: нет, это необязательно. Мы можем разделить всё наше ПО на модули по степени влияния их отказов на ту часть, которая отвечает непосредственно за управление манипулятором. Разумеется, мы должны будем детально описать и задокументировать обоснованность такого разделения с точки зрения безопасности для пациента и способов самого изолирования (рис. 5).

Например, мы можем разработать такую архитектуру нашего ПО, что часть, отвечающая за управление перемещениями манипулятора, будет выполняться в отдельном адресном пространстве или даже на отдельном процессоре. Таким образом, сбои и отказы в ПО других компонентов не будут влиять на способность контролировать перемещения скальпеля.

3.4. Требования к документации

При создании медицинского ПО стандарт требует иметь как минимум следующие документы:

1. Файл управления рисками (Risk Management File) – совокупность записей и других документов, создаваемых в процессе управления рисками (разделы 4.2, 7).

2. Классификация безопасности ПО (Software Safety Classification) – разделяет программные системы и программные элементы в соответствии с процессами, которые будут применяться для разработки и технической поддержки (раздел 4.3.c).

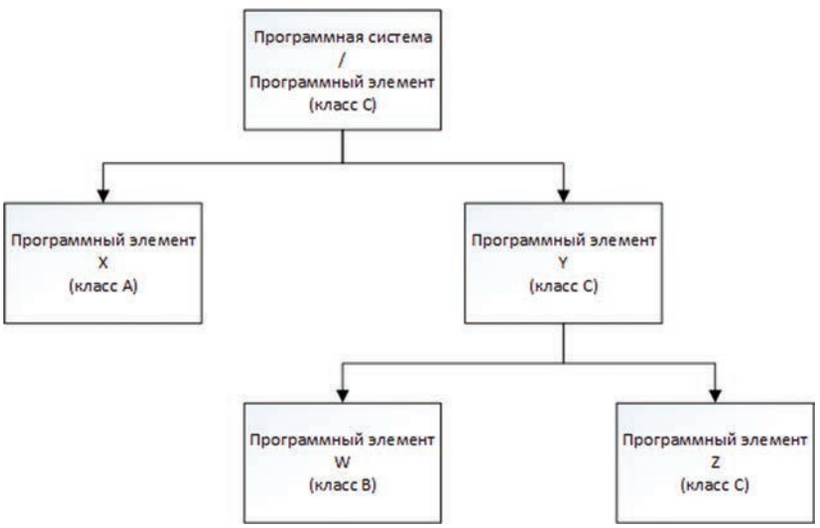


Рис. 5. Наследование класса медицинского ПО

3. План разработки ПО (Software Development Plan) – содержит план разработки, описывающий весь процесс разработки ПО соответствующего класса программной системы (раздел 5.1.1).

4. Требования к ПО (Software System Requirements) – раздел 5.2, включая меры по управлению рисками (раздел 5.2.3).

5. Архитектура ПО (Software Architectural Design) – разделы 5.3, 5.4.

6. План тестирования ПО (Software Test Plan) – разделы 5.5, 5.6, 5.7, особенно замечания 1 и 2 к разделу 5.7.1.

7. Соответствие проводимого тестирования требованиям к ПО (Traceability Overview [of test procedures to software requirements]) – раздел 5.7.4.

8. Отчёт по проведённому тестированию ПО (Software Test Report) – раздел 5.7.5.

9. Отчёт по остаточным аномалиям (Residual Anomalies) – раздел 5.8.

10. Документирование выпущенной версии ПО (Configuration Management) – разделы 5.8.4, 5.8.5, 8.

4. Выводы

В данной статье были описаны основные термины и требования, с которыми придётся столкнуться разработчикам медицинского ПО. Мы рассмотрели различия между классами ПО и причину их появления, а также дали ответы на вопросы: почему так важно знать класс ПО и каким образом можно уменьшить трудозатраты при разработке.

Это лишь вершина айсберга и далеко не весь IEC-62304: объём статьи, разумеется, не позволяет рассказать о всех аспектах подобной разработки и не заменит собой изучение самих стандартов. Но мы надеемся, что рассмотренный материал позволит читателям лучше понять причины появления стандартов, осознать их важность, а также послужит стартовой точкой при их изучении.

5. Список литературы

1. IEC-62304: Процессы жизненного цикла программного обеспечения – требования к процессу разработки медицинского ПО (ГОСТ Р МЭК 62304-2013).

2. ISO-14971: Требования для уменьшения рисков при разработке медицинского ПО (ГОСТ ИСО 14971-2011).

3. ISO-13485: Требования к системе управления качеством при разработке медицинского ПО (ГОСТ Р ИСО 13485-2004).

Сергей Кирюхин, Алексей Ханыгин, Ринат Валеев, ЗАО «РТСофт»

Некоторые подходы и технологии разработки современных ИУС с использованием отечественной инструментальной платформы PLATINUM–RT

Данная статья завершает материал, опубликованный в предыдущем номере нашего журнала под названием «Отечественная инструментальная платформа для разработки информационно-управляющих систем PLATINUM-RT» и описывает основные технологии разработки информационно-управляющих систем с использованием инструментальной платформы PLATINUM-RT.

Для успешного выполнения проекта по разработке приложений в первую очередь необходимо тщательно проработать производственную модель предприятия (модель производственной деятельности предприятия) с отражением её административно-производственной структуры.

Далее подробно описаны основные этапы реализации проекта, которые целесообразно выполнять последовательно с целью минимизации рисков.

Разработка производственной модели предприятия

Как уже было сказано выше, первый этап реализации проекта – разработка производственной модели предприятия. В данном случае под моделью понимается логическое структурирование производственных подразделений предприятия в рамках разрабатываемого приложения. Необходимо определить и задокументировать перечень подразделений, которые будут включены в приложение. Это необходимо, так как каждый объект приложения будет в дальнейшем связан только с одним конкретным подразделением. Аналогично, как и объекты, «алармы» также связаны с конкретным подразделением.

Производственная модель предприятия строится в виде иерархической структуры, и в качестве примера можно привести следующие уровни: предприятие/головной офис – филиал/производственная площадка – цех – производственная линия – оборудование/установка/агрегат. Количество уровней и степень детализации определяется конкретными требованиями при разработке приложения. Готовая модель предприятия позволит реализовать разработанные правила именования, позволит создавать объекты (шаблоны, контейнеры), соответствующие реальному производству, производить их репликацию в данной структуре предприятия. На данном этапе предоставляется возможность более детализировано определить спецификацию шаблонов и производственных структур.

Идентификация устройств и формирование функциональных требований

Вторым этапом является идентификация устройств нижнего уровня (так называемые полевые устройства), которые будут использоваться в приложении. К ним относятся вентили, смесители, разрыхлители, насосы, PID-контроллеры и т. п. Некоторые устройства могут быть достаточно сложными и включать более простые, например насос включает в себя мотор как один из элементов. На данном этапе целесообразно выделить базовые и более высокоуровневые (составные, сложные) устройства. Необходимо выявить все взаимосвязи между данными устройствами, которые определяются их участием в технологических схемах. После определения базовых устройств следующим действием будет их группирование по типам, например вентили или насосы. Определение перечня базовых устройств, обладающих схожими функциями, даст возможность сформировать/инициализировать/создать им в дальнейшем соответствующий «объект» в терминах/понятиях среды PLATINUM-RT. Экземпляр объекта в дальнейшем будет

сформирован/инициализирован по соответствующему шаблону. Количество типов устройств определяет и количество шаблонов объектов, которые необходимо будет создать в среде разработки для данного приложения. Соответственно для «сложных» объектов необходимо будет создать в среде разработки «контейнеры».

Следующий шаг данного этапа – формирование функциональных требований к определённым ранее устройствам.

Для каждого из устройств для формирования функциональных требований необходимо определиться по следующим вопросам:

– количество каналов/точек ввода/вывода;
– обработка данных – какие скрипты должны быть связаны с устройством;
– хранение исторических данных и условия – какие данные должны быть сохранены в архиве;
– наличие алармов и событий – какие условия для алармов, какие события должны быть включены в «логи» (регистрационные журналы);
– политика безопасности – какие пользователи должны иметь доступ к устройству, типы доступа для пользователей;
– графические элементы – какие графические элементы должны соответствовать данному устройству.

Разработка правил формирование имен

Третьим этапом является разработка правил формирование имён шаблонов, экземпляров шаблонов и атрибутов объектов.

Правила формирования имён должны соответствовать требованиям корпоративных документов, регламентирующих данный аспект, и ограничениям, определяемым платформой PLATINUM-RT.

В платформе формирование имён для пользовательских переменных (тегов HMI-интерфейса) отлично от того, как формируются имена тегов экземпляров объекта.

В данной платформе формирование имён должно соответствовать следующему правилу:

– для пользовательских тегов – <objectname>\<attributename>;
– для тегов экземпляров – <objectname> . <attributename>.

Планирование объектов, шаблонов и экземпляров

Как указывалось выше, создание систем в рамках платформы PLATINUM-RT базируется на объектно-ориентированном подходе. В инструментальной платформе PLATINUM-RT используется широко распространённый механизм создания объектов с помощью шаблонов. На четвёртом этапе при создании приложения следует определить и создать дочерние шаблоны для устройств определённого типа, чтобы обеспечить возможность использования данных шаблонов для создания в дальнейшем экземпляров на их основе.

Для каждого шаблона должен быть разработан набор атрибутов и значения по умолчанию, в том числе и с использованием определяемых пользователем атрибутов. Данные атрибутов будут использоваться для последующего конфигурирования функций ввода, вывода, аварийной сигнализации и ведения журнала, не встроенных в исходные объекты.

При создании экземпляр наследует атрибуты шаблона. Конфигурация многих атрибутов экземпляра, унаследованных от родительского шаблона, доступна для изменения при условии, что они не заблокированы в родительском шаблоне.

Создание экземпляров возможно только после создания соответствующих шаблонов объекта. В результате создания экземпляров получаются отдельные объекты на основе шаблона, обладающие всеми характеристиками и атрибутами данного шаблона. После создания экземпляра объекта можно произвести его развеётывание.

Разработка пользовательских объектов

На следующем этапе целесообразно провести работу по формированию пользовательских объектов, обеспечивающих дополнительную функциональность для приложений. К пользовательским объектам относятся производственные атрибуты, скрипты, атрибуты, определяемые пользователем, и атрибуты расширения. Производственные атрибуты могут быть аналоговыми или цифровыми (дискретными).

Пользовательские атрибуты дают возможность расширить логику обработки. Они позволяют:

– добавлять новые атрибуты объекту;
– конфигурировать их как тип «данные»;
– определять категории атрибута;
– определять первоначальное значение атрибута и фиксировать его;
– определять новый атрибут как массив;
– определять условия алармов и архивации атрибута;
– устанавливать режим доступа (политику безопасности).

Платформа PLATINUM-RT поддерживает реализацию скриптов двух типов: простой и сложный.

В рамках простого скрипта можно осуществлять назначения (присвоения), сравнения, простые математические функции и т. д.

Сложные скрипты дают возможность выполнять логические операции, используя управляющие структуры на основе результатов выбора направления по условию типа «IF-THEN-ELSE».

Разработка модели развёртывания

Заключительным этапом является разработка модели развёртывания системы. В данной среде разработки нет необходимости в модели развёртывания копировать физическую среду предприятия. Запуск модели развёртывания осуществляется на компьютерах, на которых установлен специальная служба развёртывания платформы. Далее необходимо развернуть платформу на этих компьютерах, которая будет идентифицировать компьютер как элемент среды исполнения, содержать соответствующие базовые объекты и исполнять логику приложения, содержащуюся в объектах. Платформа будет представлять специальные сервисы, осуществлять мониторинг, собирать статистику о состоянии компьютера и запускать или останавливать «движки» (модули исполнения). Возможно на одной платформе и, соответственно, одном компьютере установить несколько «движков». Использование механизмов «движков» даёт возможность управлять обменом данными, как по скорости, так и по периодичности, что аналогично управлению ПЛК. «Движок» может осуществлять управление (хостинг) одним или несколькими цехами (производственными зонами) и всеми соответствующими объектами, давая возможность взаимодействия между ними.

Во время процесса развёртывания происходит инсталляция необходимого программного обеспечения на определённый компьютер так, что на нём объекты могут быть «живыми» и функциональными. До тех пор пока вы не развернули конфигурационное окружение среды разработки в окружение «runtime», изменения, которые произведены в среде разработки, не появятся в среде исполнения.

Применение платформы PLATINUM-RT при создании информационно-управляющих систем даёт целый ряд важных преимуществ на всех этапах жизненного цикла ИУС. Проектирование и разработка системы на базе платформы PLATINUM-RT позволит оптимизировать процесс разработки за счёт оптимизации работы трудовых ресурсов, сокращения сроков разработки и отладки системы.

На этапе внедрения инструментария платформы PLATINUM-RT снижаются затраты на конфигурирование и развёртывание системы.

Существенное сокращение затрат достигается на этапе эксплуатации системы за счёт уменьшения стоимости технического сопровождения и, при необходимости, её модификации.

Одно из основных преимуществ использования платформы PLATINUM-RT – возможность разработки ИУС практически для любых отраслей промышленности. Поставляемые библиотеки шаблонов и библиотеки графических элементов, типовых для определённой отрасли промышленности, сокращает время на разработку систем автоматизации, стандартизирует и унифицирует подходы к автоматизации.

Платформа PLATINUM-RT предоставляет широкий набор протоколов сбора и передачи данных. Важным преимуществом является наличие протоколов отечественных стандартов и производителей оборудования, что не ограничивает в выборе полевых устройств или интеграции уже существующих распределённых систем управления (РСУ) в единую платформу.

Новости рынка

Что «Интернет вещей» сулит энергетикам

Переход к «Интернету вещей» (IoT) получает всё большую поддержку со стороны энергодобывающих и энергораспределительных компаний. Экономический потенциал его огромен и уже сегодня превышает 2 трлн долл., а к 2020 году может достичь 7 трлн. «Интернет вещей» затронет каждую отрасль, включая нефтегазовую, что означает новый уровень ситуационной осведомлённости в реальном времени, которая сейчас нужна, как никогда раньше.

Египетская компания Petrobel применяет IoT на буровых установках в Средиземном море для управления нефтедобычей и ремонтными работами из расположенного на берегу центра. Достигнутая в результате экономия оценивается в 125 тыс. долл. на одну буровую в месяц.

Основные пользователи IoT в розничной продаже – заправочные станции. С помощью IoT они передают данные об остатках топлива и принимают платежи с мобильных телефонов (услуга «плати на ходу» и платежи в рассрочку по купонам). Система может использоваться и для уведомления страхователей о пройденном километраже.

В системах обогрева домов жидким топливом IoT пока нет, но он косвенно влияет на потребление нефтепродуктов, экономя электроэнергию и повышая эффективность домашних энергосистем. Применение IoT поможет на 20% сократить затраты на содержание жилья.

Вместе с тем необходимо совершенствовать защиту всех IoT-приложений. «Интернет вещей» обеспечивает более совершенный контроль и информационную безопасность, расширяя функционал и возможности систем SCADA по устранению последствий проникновения. При этом требуется установка систем информационной безопасности, с тем чтобы защита старых систем не привела к созданию новых уязвимостей.

Источник: http://thenetwork.cisco.com/

Леонид Орлов, Константин Сергеев ЗАО «РТСофт»

Стандарт МЭК 61850: наука, практика, лирика

В данной статье рассматривается текущее состояние разработки стандарта «МЭК 61850. Сети и системы связи на подстанциях», даётся критический анализ выводов из прошлых публикаций о МЭК 61850 и в заключение – краткая справка о наиболее интересных проектах по АСУТП и РЗА с применением стандарта МЭК 61850, выполненных специалистами ЗАО «РТСофт» за последние 5 лет.

Стандарту посвящаю стих!
Надежду нам вселяя,
Он в жизнь релейную проник:
Мы – в ожиданьи рая.

Но здесь поспешность не нужна,
Она ведёт к конфузу,
Осмысленность во всём важна:
И в выборках, и в «гузах»...

Чтоб суть стандартную понять
(А польза – несомненна!),
Релейщик каждый должен знать:
Готовить надо смену...

Взирая на стандартный ряд
И на его проблемы,
Сознаюсь: я безмерно рад,
Что вечной будет тема.

Г. С. Нудельман. Стандарт вечности

Релейная защита и автоматизация электрических сетей (РЗА) – это очень интересная сфера деятельности, и в этой области работают интересные и творческие люди. Одним из ярких представителей профессии релейщика является Года Семенович Нудельман, автор более 100 изобретений и патентов в области РЗА, кандидат технических наук, доктор электротехники, действительный член АЭН РФ, ныне занимающий пост председателя совета директоров ОАО «ВНИИР». Года Семенович известен не только как эксперт в области РЗА, но и как поэт. Основной темой и эпиграфом для этой статьи послужило его новое стихотворение.

Специалисты-энергетики уже догадались, что речь в нём идёт о международном стандарте «МЭК 61850. Сети и системы связи на подстанциях». В настоящее время стандарт МЭК 61850 получил широкое применение в энергетической отрасли многих стран мира, в том числе и Российской Федерации. За прошедшие годы в мире и в России был накоплен значительный опыт применения стандарта МЭК 61850, разработки устройств и систем на его базе, реализовано множество проектов. В то же время и по сей день этот стандарт вызывает множество вопросов и обсуждений. Компания «РТСофт» в 2008 г. создала центр компетенции по стандарту МЭК 61850,

а с 2009 г. реализовала первые пилотные проекты с использованием коммуникационного протокола МЭК 61850-8-1. В России активные обсуждения стандарта начались в 2008 г. и различные эксперты и специалисты высказывали полярные мнения – от безудержного оптимизма до полного неприятия. В 2009 г. наши специалисты выпустили аналитическую статью, в которой дали свою оценку преимуществ и недостатков этой новой технологии. В дальнейшем мы также старались в своей работе придерживаться взвешенного подхода к различным инновационным технологиям, сопоставляя преимущества и затраты, выгоды и риски.

В сегодняшней статье мы попытаемся оценить текущее состояние разработки стандарта и критически проанализировать выводы прошлых публикаций о МЭК 61850. В заключение дадим краткую справку о наиболее интересных проектах по АСУТП и РЗА с применением стандарта МЭК 61850, выполненных специалистами «РТСофт» за последние 5 лет.

Информационным поводом для создания стихотворения-эпиграфа послужило недавнее сообщение в блоге Карлхайнца Шварца (один из разработчиков стандарта) о том, что ряд стандарта МЭК 61850 растёт в общей сложности до 45 частей. За пояснениями мы обратились к одному из ведущих российских интернет-ресурсов, посвящённых стандарту МЭК 61850 и инновационным технологиям, – электронному журналу «Цифровая подстанция» – ЦПС (http://digitalsubstation.ru). В одной из недавних статей, размещённых на этом сайте, описывается текущее состояние разработки стандарта МЭК 61850. Приведём эту информацию в разделе ниже.

Обзор текущего состояния разработки стандарта МЭК 61850

Более 10 лет назад в состав разрабатываемого стандарта МЭК 61850 входило небольшое количество документов. Сегодня же их количество увеличилось в несколько раз и составляет 45. Они относятся к различным категориям: это и стандарты, и технические отчёты, и технические требования. Из общего числа 21 документ утверждён и издан Международной Электротехнической Комиссией, 24 других документа находятся на стадии разработки.

Все, кто более или менее знаком со стандартом, точно знают главы:

- 1 (Введение и обзор);
- 2 (Словарь терминов);
- 3 (Общие требования);
- 4 (Управление проектами и системами);
- 5 (Требования к информационному обмену между функциями и моделями устройств);
- 6 (Язык описания конфигурации информационного обмена между устройствами на подстанциях);
- 7-1 (Базовая структура информационного обмена — Принципы и модели);
- 7-2 (Базовая структура информационного обмена — Абстрактные коммуникационные модели и сервисы);
- 7-3 (Базовая структура информационного обмена — Общие классы данных);
- 7-4 (Базовая структура информационного обмена — Совместимые логические узлы и классы данных);
- 8-1 (Назначение на конкретный коммуникационный протокол — Назначение на MMS и ИСО/МЭК 8802-3);
- 9-2 (Назначение на конкретный коммуникационный протокол — Передача мгновенных значений в соответствии с ИСО/МЭК 8802-3);
- 10 (Проверки соответствия).

Это хорошо знакомый всем «джентльменский набор». Но этот набор не досчитывает более 30 документов.

Во-первых, стоит сказать о логическом продолжении глав 7-X: 7-410, 7-410 (дополнение 1), 7-420, 7-500, 7-510, 7-520. Все эти главы определяют новые классы данных МЭК 61850: логические узлы, объекты и типы данных для гидроэлектростанций и малой генерации. Также эти документы описывают порядок моделирования данных, правила моделирования – применительно ко всем энергообъектам.

Во-вторых, теперь есть и глава 8-2, которая определяет назначение абстрактных сервисов и моделей, определённых в 7-2, **на веб-сервисы**. Скоро станут доступны для аренды облачные SCADA-системы и подстанция может «закрутиться» в браузере.

Глава с индексом 9 теперь не в гордом одиночестве — её дополнит глава 9-3. Она опишет **долгожданный профиль для протокола синхронизации времени PTP**. Ведь больше всего об этом протоколе точной синхронизации времени говорят в привязке к шине процесса. Логичная состыковка.

Глава 10 также теперь не будет одна. Документ 10-210 опишет требования к испытаниям на функциональную совместимость для устройств с поддержкой МЭК 61850 (с реализацией моделей функций и оборудования гидроэлектростанций). Глава 10-3 определит порядок функционального тестирования комплексов РЗА с использованием МЭК 61850 для проверки реализации функций с использованием стандартных узлов и данных информационной модели стандарта.

Значительно расширяются модели данных стандарта МЭК 61850 — от энергообъектов до электромобилей.

Теперь о новых документах — с новыми индексами 80 и 90:

– 80-1 рассматривает вопросы интеграции с комплексами, функционирующими по условиям протоколов МЭК 60870-5-101/104;
– 80-3 – технический отчёт, который рассмотрит требования к реализации функциональности стандарта на основе веб-сервисов;
– 80-4 – определит назначение моделей стандарта МЭК 62056 на модели стандарта МЭК 61850;
– 80-5 – назначение Modbus на МЭК 61850.

Глав с индексом 90 больше:

– 90-1 – этот уже опубликованный отчёт рассматривает вопросы обмена данными между устройствами, установленными на различных энергообъектах;
– 90-2 – рассмотрит вопросы обмена данными между энергообъектами и центрами управления;
– 90-3 – уделит внимание вопросам использования стандарта МЭК 61850 в комплексах мониторинга оборудования, появятся новые логические узлы;
– 90-4 – уже опубликованный отчёт рассматривает вопросы реализации инфраструктуры сети Ethernet в комплексах, функционирующих по условиям стандарта МЭК 61850;
– 90-410 – рассмотрит вопросы построения сетевой инфраструктуры на гидроэлектростанциях;
– 90-5 – уже выпущен и определяет порядок передачи данных о синхронизированных векторных измерениях посредством сервисов стандарта;
– 90-6 – определит сценарии использования МЭК 61850 в комплексах автоматизации распределительных сетей;
– 90-7 – новые модели для фотовольтаических установок;
– 90-8 – новые модели для электромобилей (!!!);
– 90-9 – новые модели данных для накопителей энергии;
– 90-10 – новые модели данных для идентификации режимов;
– 90-11 – порядок использования стандарта МЭК 61850 для моделирования свободно-программируемой логики;
– 90-12 – руководящие указания по построению коммуникационной инфраструктуры для организации связи между объектами;
– 90-14 – новые модели данных для моделирования данных оборудования гибких передач переменного тока FACTS;
– 90-15 – интеграция объектов малой генерации по условиям МЭК 61850;
– 90-16 – управление системами на основе стандарта;
– 90-17 – передача данных о качестве электроэнергии с использованием МЭК 61850.

Нельзя не согласиться с мнением ЦПС, что стандарт пришёл в нашу жизнь всерьёз и надолго, и наконец-то становится понятен «скрытый смысл» стихотворения-эпиграфа.

Анализ преимуществ и недостатков стандарта МЭК 61850 сегодня

В статье [1], опубликованной в 2009 г., приводился список преимуществ и недостатков стандарта МЭК 61850, с точки зрения специалистов ЗАО «РТСофт». Произведём их переоценку (при необходимости) с учётом накопленного многолетнего опыта применения стандарта и приведённого выше состояния его разработки.

Преимущества стандарта МЭК 61850 и предложения по их использованию

– Горизонтальный обмен между низовыми устройствами (GOOSE). Здесь наша позиция практически не претерпела никаких изменений, в наших проектах по-прежнему эта технология используется для оперативных блокировок разъединителей. Кроме того, в ряде проектов сигналы GOOSE использовались для обмена информацией для нужд функций автоматики (УРОВ, АПВ...). Передача сигнала GOOSE на отключение выключателя от срабатывания РЗА не применяется. Более того, попытки их использования в данном качестве другими интеграторами, привели к аварийным ситуациям на энергообъектах, что привело, по сути, к запрету такого их применения.

Чем вызвана данная ситуация? Едва ли несовершенством самого стандарта, скорее наложением нескольких факторов: неисправностей оборудования ЛВС, ошибками при наладке, организационными недоработками в организации строительства объекта и сдачи/приёмки работ.

Планируется ли более широкое применение GOOSE? Несомненно. В 2013 г. была утверждена «Единая техническая политика ОАО «Россети», в которой рекомендуется «применение цифровых УСО с оптическим интерфейсом и протоколом МЭК 61850-8-1, максимально приближенных к объекту управления, для управления коммутационными аппаратами

(за исключением выключателей) и получения дискретной информации от присоединения и других методов оптимизации кабельных проводок для улучшения электромагнитной обстановки на ПС» [4]. Но повсеместно использовать GOOSE для передачи ответственных сигналов РЗА релейщики пока опасаются. Данное решение пока проходит апробацию в ходе пилотных проектов по цифровым подстанциям с действием защит на сигнал.

– Упрощение интеграции устройств МП РЗА. Здесь наше видение полностью оправдалось. Действительно, передача сигналов и осциллограмм от устройств РЗА по протоколу МЭК 61850-8-1 намного ускорилась и упростилась по сравнению с протоколом МЭК 60870-5-103. Но по-прежнему встречаются объекты, на которых приходится совмещать применение обоих протоколов и производить конвертацию сигналов протокола МЭК 60870-5-103 в MMS, что в общем случае противоречит стандарту МЭК 61850. Тем не менее для удовлетворения нужд Заказчика, в ПТК АСУТП производства ЗАО «РТСофт» имеется и такая встроенная возможность, не требующая никаких специальных познаний стандартов.

– Содержательные имена тэгов. Ситуация коренным образом не изменилась, но помимо использования узла GGIO для сигналов другого назначения (имеющих соответствующие предопределённые логические узлы), обнаружилась и другая крайность. Выяснилось, что многие разработчики устройств также считают, что стандарт описывает не все необходимые для устройств атрибуты логических узлов, в результате в моделях их устройств появляются никому не известные логические узлы и атрибуты. Да, в большинстве случаев это не противоречит стандарту, но зачастую приводит к неполной совместимости устройств и ПТК различных производителей.

– Самоописание. Практический опыт действительно показывает удобство и необходимость использования этого свойства устройств с поддержкой МЭК 61850. К сожалению, по сей день невозможно получить полный набор конфигурационных данных, необходимых для полной настройки ИЭУ в заводских условиях. Практически во всех проектах приходится вносить изменения в конфигурации устройств уже находясь «в поле», и именно здесь неоценимую помощью оказывают функции Online-импорта моделей устройств.

Недостатки стандарта МЭК 61850 и предложения по их компенсации

– Недостаточный уровень стандартизации в части функциональности. Как видно из приведённого в начале статьи обзора, и по истечении 5 лет с момента написания [1], в стандарте по-прежнему не регламентированы или недостаточно проработаны многие важные вопросы. Помимо уже упомянутых ранее вопросов выбора протокола синхронизации времени, очень важны вопросы организации локальной сети, в которой работают устройства с поддержкой МЭК 61850. В частности, вопросы по резервированию сети, вопросы по архитектуре сети – сегментированию, настройке разных VLAN для разных видов трафика (SV, MMS, GOOSE – ОБР, GOOSE – РЗА и др.). При построении больших систем, особенно при использовании протокола МЭК 61850-9-2, неизбежно возникают вопросы с производительностью и устойчивостью ЛВС, которые в большинстве случаев можно решить грамотной настройкой сетевого оборудования. Но, к сожалению, стандарт не указывает, как именно нужно это делать, в результате разные интеграторы применяют разные подходы, что может приводить к проблемам при расширении системы устройствами сторонних производителей.

– Недостаточный уровень стандартизации в части информационного обмена. Проблема всё по-прежнему актуальна. Практически каждая попытка интеграции сторонних ИЭУ в ПТК АСУТП выявляет неполное соответствие сторонних устройств стандарту, либо неполную совместимость реализации протокола МЭК 61850 в ПТК АСУТП и в интегрируемых ИЭУ. Добровольная сертификация на соответствие требованиям МЭК 61850 позволила бы улучшить ситуацию, но в нынешних экономических условиях большинство производителей от неё отказываются. Таким образом, проблема функциональной совместимости решается путём совместных испытаний, проводимых несколькими производителями по обоюдному согласию, либо в рамках аттестационных испытаний.

Помимо уже имевшихся ранее проблем, стоит упомянуть и выход в свет второй редакции стандарта МЭК 61850, которая, как это ни прискорбно, обратно не совместима с первой редакцией стандарта! Это означает, что если на объекте уже установлены устройства с поддержкой МЭК 61850-8-1 ред.1, на объект **нельзя** установить дополнительно, пусть даже точно такие же, устройства того же производителя, но уже с поддержкой МЭК 61850-8-2 ред.2. На практике этой означает, что и старые, и новые устройства нужно привести (перепрошить) к одной и той же редакции, что в ряде случаев может быть просто невозможно.

Между тем разработчики не сидят на месте и активно работают над следующей редакцией стандарта,

которую решили назвать редакцией «2.1». Будет ли она совместима со второй редакцией – время покажет, мы обязательно вернёмся в будущем к этой теме.

– Отсутствие полноценных инструментальных средств. На сегодняшний день существуют программные продукты для инжиниринга по МЭК 61850, независимые от производителей оборудования, но в большинстве случаев фирменное ПО для конфигурирования устройств с ними несовместимо и требует доработки или дополнительной работы по интеграции [2].

– Повышенные требования к вычислительным ресурсам и производительности сети. По большому счёту, проблема производительности ИЭУ и SCADA-систем на сегодняшний день решена. На рынке представлено достаточное количество процессоров различных производителей, позволяющих обрабатывать трафик MMS от большого количество серверов МЭК 61850-8. В ряде случаев, для особо крупных энергообъектов, производители используют каскадированные решения, распределяя серверы МЭК 61850-8 по несколько клиентам – коммуникационным серверам (станционным контроллерам).

Сегодня вопрос производительности ИЭУ и технологической ЛВС выходит на первый план при построении полностью цифровых подстанций с шиной процесса.

– Увеличение стоимости реализации проектов. Здесь мы оказались на 100% правы. Действительно, проекты АСУТП подстанций с применением стандарта МЭК 61850 имеют повышенную стоимость по сравнению с проектами, основанными на устаревших протоколах серии МЭК 60870-5-10x, Modbus и др., и обещанного идеологами стандарта сокращения затрат по сей день, увы, не наблюдается. Такое положение дел приводит к тому, что энергокомпании, не имеющие достаточных финансовых средств, вынуждены использовать устаревшие протоколы обмена данными. С другой стороны, по прошествии достаточно большого промежутка времени, в течение которого в РФ стал внедряться стандарт МЭК 61850, подходы к автоматизации в Западной Европе практически не изменились. Там по-прежнему практически не используется этот современный стандарт, предпочтение отдаётся упомянутым устаревшим. И уж здесь причина такого технологического отставания кроется явно не в недостатке финансирования, а в рачительном подходе к инвестициям. То есть многие западные компании действительно не видят никакой финансовой выгоды в применении стандарта МЭК 61850, как в части технологий цифровых подстанций, так и в части протоколов обмена данными MMS, GOOSE.

Таким образом, большинство наших предположений оказались верными. То же можно сказать об основном выводе нашей статьи 2009 г.: подход «МЭК 61850 любой ценой» следует признать неоправданным.

Сегодня МЭК 61850 применяется в качестве основного протокола при создании АСУТП подстанций высокого и сверхвысокого напряжения (220 кВ и выше), в первую очередь на объектах ОАО «ФСК ЕЭС». В распределительных сетевых компаниях, на ПС 110кВ он применяется примерно в 50 % случаев, на ПС 35кВ – в 20–25 % проектов, а на подстанциях среднего напряжения – крайне редко, в основном из-за сравнительно высокой стоимости устройств РЗА СН с поддержкой данного протокола.

Практический опыт реализации проектов АСУТП и РЗА компанией ЗАО «РТСофт» за 2009–2014 гг.

Рассмотрим наиболее интересные проекты АСУТП и РЗА, реализованные нашими специалистами за последние годы. Как видно ниже, в проектах были использованы различные принципы инжиниринга по стандарту МЭК 61850 [2], подсистемы РЗА различных производителей и различные контроллеры присоединений.

1. Первый проект с РЗА Siemens + ПТК АСУТП SMART-SPRECON – ПС «Широкая», 2009 г.

Характеристики данного проекта:
– инжиниринг: «снизу вверх»;
– уровни напряжения: 220/110/35/6 кВ;
– устройства РЗА: Siemens;
– контроллеры присоединений: 6MD664;
– количество устройств SIEMENS: 95;
– SCADA-система: SPRECON-V460;
– протокол связи: МЭК 61850;
– сетевые коммутаторы: Ruggedcom.

Особенность данного проекта – первый проект по совместному использованию РЗА SIEMENS и ПТК АСУТП SMART-SPRECON с интеграцией по МЭК 61850.

2. Первый проект с РЗА ЭКРА, с поддержкой МЭК 61850 и инжинирингом по методу «сверху-вниз» – ПС «Борская», 2012 г.

Характеристики данного проекта:
– инжиниринг: «сверху вниз»;
– уровни напряжения: 220/110/35/10 кВ;
– Устройства РЗА: ЭКРА;
– Контроллеры присоединений: SPRECON-E-C;
– Количество устройств ЭКРА: 101;
– SCADA-система: SPRECON-V460;

– протокол связи: МЭК 61850;
– сетевые коммутаторы: Ruggedcom.

Новизна этого проекта заключалась в том, что это был первый крупный проект, где использовались терминалы РЗА ООО «НПП Экра» с поддержкой МЭК 61850-8-1.

3. Первый проект с использованием технологии упрощённого инжиниринга – ПС «Амур», 2013 г.

Характеристики данного проекта:
– инжиниринг: «упрощённый»;
– уровни напряжения: 220/110/10 кВ;
– устройства РЗА: ЭКРА;
– контроллеры присоединений: SPRECON-E-C;
– количество устройств ЭКРА: 64;
– SCADA-система: SPRECON-V460;
– протокол связи: МЭК 61850;
– сетевые коммутаторы: Ruggedcom.

Этот проект интересен тем, что в нём впервые применена технология упрощённого инжиниринга, благодаря которой сводятся к минимуму работы по конфигурированию обмена данными по МЭК 61850 между ИЭУ и SCADA-системой. В данном случае происходит автоматическая генерация моделей данных контроллеров присоединений и обеспечивается поддержка интеграции устройств сторонних производителей на уровне готовых конфигурационных файлов (.cid/.icd), благодаря чему существенно снижается трудоёмкость и стоимость реализации проекта. При этом полностью отпадает потребность в изучении стандарта МЭК 61850 инженерным персоналом Заказчика, что весьма актуально в нынешних экономических условиях.

В целом за 5 лет компания «РТСофт» реализовала более 50 проектов по АСУТП подстанций высокого напряжения, в том числе более 20 комплексных проектов по созданию систем РЗА и АСУТП. Стандарт МЭК 61850 оказался весьма полезен для реализации этих проектов, и теперь уже не только наши эксперты-разработчики, но и инженеры, проектировщики и наладчики по достоинству оценили все его преимущества и научились грамотно справляться с имеющимися недостатками.

Также мы получили практическую возможность сравнить эффективность вариантов интеграции МП РЗА по протоколам МЭК 61850 и МЭК 60870-5-103 на объектах электроснабжения Олимпиады «Сочи-2014». ПТК АСУТП производства «РТСофт» был установлен на 4 ПС 110–220кВ, при этом на одном из объектов были установлены устройства РЗА с поддержкой МЭК 61850, а на других трёх подстанциях, реализованных на более раннем этапе строительства – устройства того же производителя, но с поддержкой МЭК 60870-5-103 и устаревшей прошивкой. На подстанции с МЭК 61850 интеграция была выполнена быстро и без затруднений, а на других трёх ПС возникли некоторые трудности с выгрузкой осциллограмм, которые удалось оперативно решить благодаря оперативной доработке ПТК АСУТП без перепрошивки терминалов РЗА. Компания «РТСофт» оказалась единственным производителем АСУТП, который обеспечил полноценную интеграцию устройств РЗА по обоим протоколам в рамках проекта «Сочи-2014».

Заключение

Таким образом, стандарт МЭК 61850 по-прежнему актуален. За 10 лет его разработки он нашёл широкое применение, существенно изменился и всё еще находится в стадии развития, и пока далёк от совершенства.

Сегодня мы не знаем, действительно ли тема МЭК 61850 будет вечной, как утверждается в стихотворном эпиграфе, но мы уже видим, что она объединила как минимум три поколения релейщиков и «АСУшников» и помогла им найти общий язык.

И закончить эту статью также хотелось бы стихотворными цитатами:

– «Покуда есть на свете IEC, от всех цепей избавят нас гуси!» (оратор, 2007 г.);

– «Увы, наладчикам добавилось проблем... Но для беседы больше общих тем!» (руководитель проекта, 2009 г.);

– «Теперь защиты и АСУТП заговорят на общем языке...» (из протоколов испытаний, 2009–2012 г.);

– «Общенье это крепче медных уз... Друзья мои, прекрасен наш союз!» (заключительный тост).

Литература

1. Журнал «Электрические станции» №11/09. Орлов Л. Л., Егоров Д. В., ЗАО «РТСофт». МЭК 61850 – новый стандарт для построения систем автоматизации в энергетике.

2. Журнал «Релейная защита и автоматизация» №4/13. Орлов Л. Л., Сергеев К. А., ЗАО «РТСофт». Обзор требований единой технической политики ОАО «Российские сети» и возможных технических решений по автоматизации распределительных сетей.

3. Интернет-сайт «Цифровая подстанция» – digitalsubstation.ru. http://digitalsubstation.ru/blog/2015/02/17/standart-mehk-61850-ot-ehnergoobektov-do-ehlektromobilejj/

4. Положение о единой технической политике в электросетевом комплексе. Утверждено Советом директоров ОАО «Россети» (протокол № 138 от 23.10.2013).

Дженс Зербст (Jens Zerbst), Лиро Ринта Жуппи (Liro Rinta Jouppi),
Джованна Дондосола (Giovanna Dondossola), Кристоф Пойриер (Christophe Poirier),
Паскаль Ситбон (Pascal Sitbon), Деннис Хольстайн (Dennis Holstein),
Джон Макдональд John (McDonald), Роберт Иванс (Robert Evans)

Кибербезопасность в энергетике. Состояние вопроса

В настоящее время процессы производства, передачи и распределения электроэнергии всё больше зависят от информационных систем, включая и сети передачи данных. В результате технического прогресса появились реальные угрозы для безопасности и надёжности снабжения электроэнергией потребителей, причиной которых является возможность использования уязвимостей в информационных системах и архитектуре их взаимодействия. Этот документ оценивает текущий статус кибербезопасности, включая обсуждение современных рисков и угроз для инфраструктуры энергетических компаний. Также статья содержит ссылки на рекомендации, составленные на основе лучшего практического опыта реализации защиты, руководствуясь принципами использования современных стандартов.

1. Введение

До широкого применения современных технологий информатизации, энергетикам не нужно было сильно беспокоиться об угрозах из сети Интернет. Они полагались главным образом на закрытость своих систем и на мероприятия по их физической защите. В то время системы управления были связаны скорее с физическим устройством контроля и исполнения, чем между собой по телекоммуникационным протоколам.

В настоящее время операции производства, передачи и распределения электроэнергии всё больше зависят от цифровых систем промышленной автоматизации, в том числе и от смежных информационных систем и сетей связи, например:

– С помощью цифровых систем энергокомпании централизованно осуществляют контроль и управление. Ранее эти функции выполнялись локально и децентрализованно. В ситуации, когда сокращение операционных расходов возможно главным образом за счёт внедрения новых решений и использования передового опыта – эволюция и внедрение таких систем становится необратимым процессом.
– Растущее использование возобновляемых источников энергии усложняет управление сетями настолько, что делает невозможной их эксплуатацию без систем автоматизированного управления.
– Технологии Smart grids ведут к появлению многочисленных новых услуг, путём вовлечения потребителей и сервисов, основанных на распределённой автоматизации, что кардинально меняет архитектуру систем управления и принципы доступа к ним и их использования [1].

«Эта эволюция порождает новые риски и угрозы процессу энергоснабжения, основанные на использовании уязвимостей архитектуры цифровых систем и (или) коммуникаций между ними. Сложившаяся ситуация порождает необходимость создания новых требований к безопасности для цифровых систем управления в энергетике и смежной с ними инфраструктуры. Требования безопасности должны быть обоснованы оценкой соответствующих рисков и общими архитектурными решениями» [2].

«Под киберзащищённостью обычно понимаются безопасность и действия, которые могут использоваться для защиты cyber-домена как в гражданской, так и в военной области от угроз, направленных на него или могущих нанести вред его взаимозависимым сетям и информационной инфраструктуре. Мероприятия по

киберзащите направлены на сохранение доступности и целостности сетей, инфраструктуры и конфиденциальности содержащейся в них информации» [3].

Кибербезопасность – это в первую очередь люди, процессы и технологии, действующие совместно, «чтобы охватить весь спектр возможностей снижения угроз, уменьшения уязвимостей; международной кооперации – с целью выработки политики реагирования на инциденты; повышения отказоустойчивости и сокращения времени восстановления компьютерных сетей и данных после кибератак, в том числе и при участии правоохранительных органов, и. т. д.» [4].

Статья с разных сторон раскрывает тематику кибербезопасности применительно к энергетике. Она не претендует на исчерпывающее изложение темы или детальное рассмотрение частных вопросов. Также даётся краткое описание состава и статуса прошлых и текущих работ в этой быстро развивающейся области в рамках СИГРЭ.

2. Риски для цифровых систем

2.1. Смена технологий

Энергокомпании привыкли к долгому сроку службы технической инфраструктуры. Для проприетарных систем это было нормой; они были спроектированы и построены специально для решения определённого круга задач. За последние десять лет технологического развития природа и характер бизнеса изменились. Современное оборудование проектируется и выпускается на принципах создания версий, готовых для применения «с полки» (Commercial Off the Shelf) – стандартизованное «железо» и программное обеспечение, предназначенное для решения различных задач. В целом промышленность перешла от разработки специализированного программного и аппаратного обеспечения к универсальным операционным системам и стандартным решениям, которые используются для достижения многих целей. В этом же направлении идёт развитие человеко-машинных интерфейсов (HMI), программируемых логических контроллеров (PLCs), а также другого оборудования защиты и автоматики. Сегодня информационные системы с одинаковой операционной системой (и уязвимостями!) могут использоваться и в офисе, и в центре диспетчерского управления в составе оперативных информационных комплексов (SCADA-системы), или на подстанциях в системах релейной защиты и автоматики.

То же утверждение верно и для сетей передачи данных. Ранее в качестве каналов передачи данных для телеуправления и элементов АСУ ТП использовались медные «последовательные линии» и тип соединения «точка–точка». Сегодня передача данных всё чаще осуществляется с использованием современных «маршрутизируемых» коммуникационных протоколов (например, IP), которые дают новые возможности для связи, одновременно с новыми уязвимостями и слабыми местами. Возврат к использованию старых «последовательных» протоколов уже невозможен, они не обеспечат пропускную способность, необходимую для работы современных приложений, таких, например, как система мониторинга переходных режимов (WAMS) и тех возможностей, к которым мы привыкли в IP-протоколах.

2.2. Увеличение связности

В немецкой газете [5] [6], был описан пример из реальной жизни, демонстрирующий увеличение количества связей между офисными/бизнес-сетями и технологической сетью системы контроля критической инфраструктуры. Статья описывает выполнение теста на проникновение (pentest) в энергетическую компанию, которая находится в Германии и снабжает около 40 000 жителей местного региона электричеством и водой. Согласно статье, в короткий срок эксперт по безопасности смог получить доступ к системе контроля критической инфраструктуры путём проникновения через офисную сеть с использованием комбинированного метода атаки: социального инжиниринга плюс уязвимостей программного обеспечения.

Этот факт, конечно, не может демонстрировать уровень безопасности и защищённости инфраструктуры всех компаний, он только подчёркивает то обстоятельство, что полная изоляция систем управления от бизнес-систем – миф [7]. И этот миф давно уже мешает энергетическим компаниям занимать правильную позицию по внедрению решений, обеспечивающих нужный уровень информационной безопасности.

В качестве иллюстрации того, как связи между системами используется в реальных атаках, можно рассмотреть направление атак вирусом Stuxnet [8] на примере упрощённой IT-архитектуры завода (см. рис.). Представленный рисунок выполнен на основе публично доступной упрощённой информации о способах распространения вредоносной программы Stuxnet [9].

Для выполнения заражения и атаки Stuxnet использовал следующие методы проникновения [10]:

1. Заражение по сети компьютеров с программным обеспечением WinCC через заданный «жёстко» пароль сервера базы данных.

2. Распространение компонентов вируса через общие сетевые ресурсы.

3. Заражение Windows Server с использованием уязвимости MS08-067.

4. Связи peer-to-peer и обновления [1].

5. Вероятно также, что для распространения использовалось Zero-Day-уязвимость MS10-061 сервиса очереди печати.

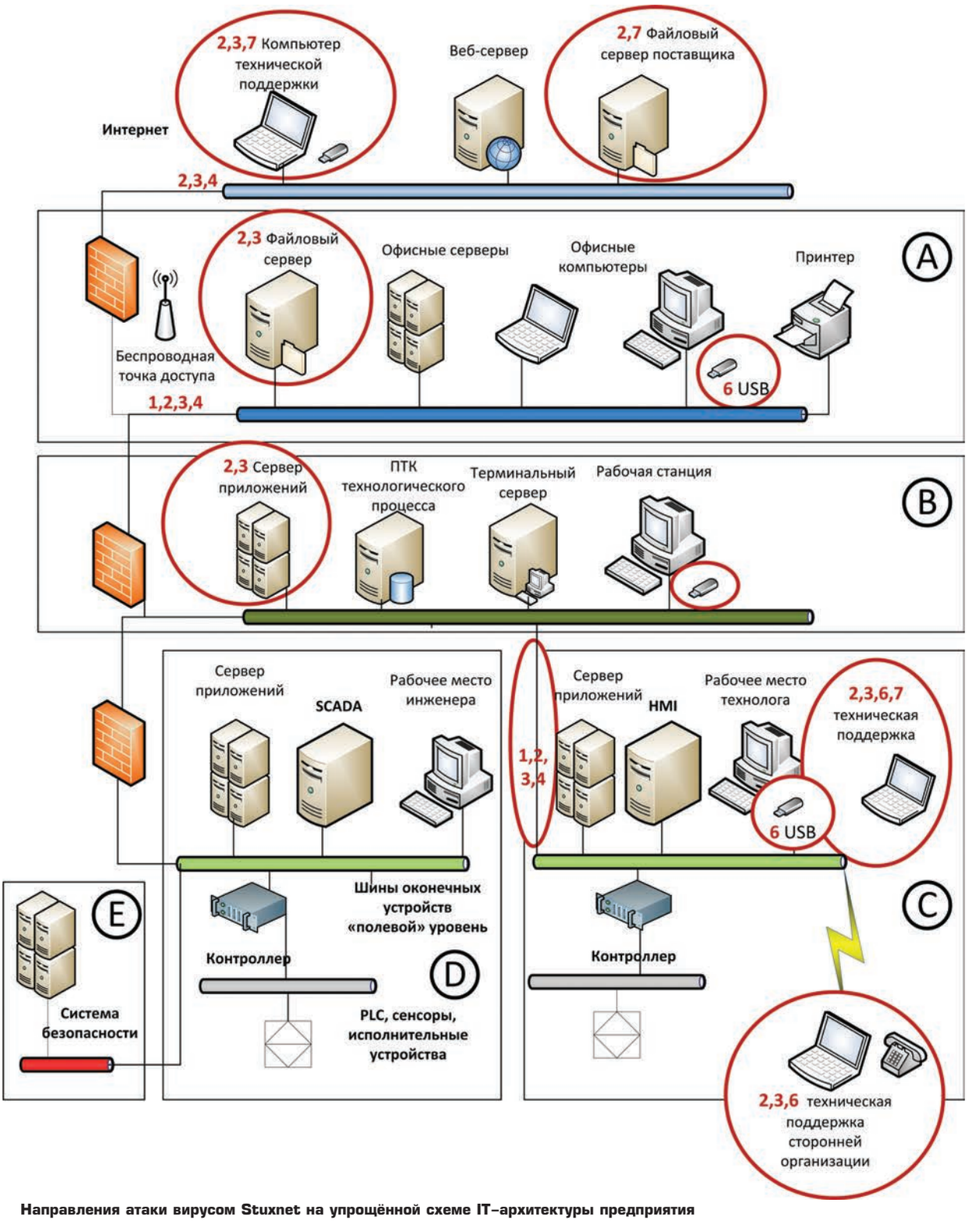
6. Распространение через flash- накопители: уязвимость CVE-2010-2568 или AutoRunInf.

7. Заражение Siemens S7-файлов проекта, с использованием файлов MCP или временных (TMP) файлов.

Перечислим на примере того же рисунка перечень комплексных мер защиты (без претензии на полноту списка):

I. Физическое разделение систем (сетей), так называемый air gap или использование специализированных устройств, «дата-диодов», гарантирующих односторонние коммуникации (см. например, между зоной E и D).

II. Логическое разделение систем с сохранением минимальной функциональной связи, основанной



Направления атаки вирусом Stuxnet на упрощённой схеме IT–архитектуры предприятия

на требованиях приложений, например межсетевой экран, снабжённый средствами глубокой инспекции пакетов (см. между зонами D и B).

III. Ограничения подключения и доступа к публичным ресурсам в Интернете (см. например, зоны B, C и D не имеют доступа к Интернету).

IV. Деление на зоны компьютерных сетей, обоснованное требованиями к необходимому уровню защиты каждой из зон (выделение зон A, B, C, D и E).

V. Отдельная зона для управления установкой исправлений и обновлений (зона A, B, C, D и E).

VI. Организационные или технические ограничения на использование съёмных носителей, например на использование USB- или компакт-дисков (см. например, инженерные станции в зоне D могут не иметь USB-разъёмов, по сравнению с рабочей станцией в зоне B).

VII. Ограничения на подключение сервисных рабочих станций к определённым сегментам сети (см. например, доступ к зоне D разрешён только через терминальный сервер в зоне B, по сравнению с зоной C, где допускается прямое подключение с целью технического обслуживания).

VIII. Ограничение на дистанционное обслуживание третьей стороной (см. например, ограниченный внешний доступ к зоне D).

Торговые и информационные бизнес-системы уже сегодня соединены с элементами критической инфраструктуры.

Тенденцию к интеграции и увеличению числа связей между решениями и системами в энергетике уже не остановить. Олицетворением этого тренда является всё более широкое использование удалённого доступа и взаимодействия посредством открытых коммуникаций и стандартных моделей данных, как в IEC 61850 [11]. С ростом уровня интеграции и взаимодействия всё большее число энергокомпаний будет подвержено риску кибератак со значительными потенциальными последствиями.

Новые рыночные требования кардинальным образом увеличивают потребность в межсистемных связях для электронного обмена данными и интеграции, например:

– Поддержка и обслуживания в режиме 24/7 в сочетании с необходимостью снижения её стоимости нуждается в удалённых службах и сервисах, которые должны быть доступны по всему миру, и предъявляет повышенные требования к высокой пропускной способности каналов для обмена файлами обновлений и конфигураций, размер и темп появления которых постоянно растёт.
– Энергетическая отрасль развивается в направлении гибкого управления потреблением электроэнергии (demand response) – технологии, которая позволяет в автоматизированном режиме в реальном времени организовать взаимодействие производителей возобновляемой энергии и клиентов для координации спроса и выравнивания пиков потребления. Управление двунаправленными потоками электрической энергии, в случае распределённой генерации, также нуждается в новых способах обмена данными. Всё это значительно увеличивает количество участников рынка и необходимых коммуникаций.
– Энергетическая система должна включать в себя всё больше генерации от возобновляемых источников энергии, которые по своей природе менее контролируемы и предсказуемы, чем традиционные способы получения электроэнергии. Эта потребность должна компенсироваться более высокой степенью интеграции.
– Умный учёт (Smart Metering) значительно увеличивает требования к коммуникациям по сравнению со вчерашним днем, одновременно добавляя новый уровень контроля за объектами потребления. Одновременно с ростом требований к взаимодействию систем повышается и критичность к наличию постоянного и надёжного их соединения. Внезапно оказалось, что надёжность всей энергетической системы очень зависит от надёжности телекоммуникаций. Без выполнения этого условия появляется риск возникновения крупных системных аварий (black-outs) [12].

В то время как системы становятся всё более сложными и уязвимыми для атак с разных направлений, мы не должны забывать о наличии унаследованных систем. В статье, опубликованной в октябре 2013 г. в [13], исследователи сообщают об обнаруженных уязвимостях в устройствах, обеспечивающих каналы связи (serial) между серверами и подстанциями. Риски взлома последовательных каналов связи обычно игнорируются, специалисты по безопасности энергетических систем обычно фокусируются на защите IP-коммуникаций. Считается, что каналы связи, работающие на последовательных протоколах, не могут порождать векторы атаки (см. [8]). Исследователи утверждают, что вызвать нарушения в энергосистеме через взлом устройств последовательной связи может быть даже проще, чем атаковать через IP-сети, так как не требуется преодолевать защиту брандмауэров. Бреши в безопасности могут также появиться в результате добавления в существующие системы, использующие serial-протоколы, устройств с сетевыми интерфейсами на основе IP, поддерживающих функции дистанционного обслуживания [14].

2.3. Возрастание угроз

Согласно недавнему докладу ICS-CERT [15], энергетический сектор выделяется как одна из целей для кибератак в промышленном секторе. Тенденцию увеличе-

ния этой угрозы подтверждает и один из поставщиков антивирусного программного обеспечения в отчёте, опубликованном в начале 2014 года: «энергетический сектор стал одним из основных направлений для целенаправленных атак и теперь входит в пятерку наиболее атакуемых сегментов в мире» [16].

Сообщается также об увеличении угроз на техническом уровне. Количество сообщений об уязвимостях в SCADA-системах выросло на 600 % по сравнению с 2010 годом, а число раскрытых уязвимостей удвоилось в промежутке между 2011 и 2012 годами [17]. Эти цифры иллюстрирует рост интереса со стороны злоумышленников, хотя частично такой рост объясняется тем, что раскрытие инцидентов стало обязательным для некоторых операторов. Эти уязвимости затрагивают широкий спектр устройств различных производителей, а их число превышает количество уязвимостей в Java- или Flash-технологиях – важный факт, поскольку именно Java и Flash часто рассматриваются как слабо защищённое программное обеспечение [17].

Чтобы представить более дифференцированную картину сегодняшнего пейзажа угроз для IT-инфраструктуры в электроэнергетике, можно разделить все атаки на целевые и нецелевые [18].

Примеры и признаки целевых атак:

– Хорошо финансируются государственными институтами, например Stuxnet, вероятно, нанёс значительный ущерб иранской ядерной программе [10], а хакерская группа Dragonfly угрожала саботажем западным энергетическим компаниям [19].
– Хакеры с политическими или экологическими требованиями (хактивисты), такие как Anonymous, направляли свои атаки против компаний ядерной энергетики EDF, GE и ENEL во втором квартале 2011 г. после трагедии на Фукусиме [20]. Или атака вирусом Shamoon 2, в результате которой были заражены около 30 000 компьютеров нефтяной компании в Саудовской Аравии в 2012 году [21].
– Особое беспокойство должны вызывать недовольные сотрудники или обслуживающий персонал сторонних организаций, которые имеют права доступа и знают тонкости эксплуатации систем и способы хранения конфиденциальных данных [22].

Примеры нецелевых атак:

– Частные лица просто пытаются найти возможности и технологии взлома SCADA-систем, имеющих интерфейсы в Интернете, с помощью известных уязвимостей, найденных с использованием поисковой системы Shodan [23].
– Заражение компьютерными вирусами, например атомная электростанция в США, штат Огайо, была заражена компьютерным червём Slammer во время технического обслуживания [24].

Несмотря на то, что большинство подобных атак не требуют сложных инструментов и значительных затрат, в целом нападения имеют тенденцию становиться всё более изощрёнными в плане привлечения ресурсов и усложнения тактики.

Можно сделать вывод, что по мере развития «умных сетей», одним из элементов которых является интеллектуальная измерительная инфраструктура (Advanced Metering Infrastructure), одновременно будет возрастать сложность и количество угроз. Эта ситуация усугубляется тем, что измерительное оборудование имеет подключение к публичной сети Интернет, что не даёт возможности застраховать от угроз внутренние сети компаний путём изоляции и использования только частных интрасетей.

В мире быстро развивающихся угроз предприятия электроэнергетики должны уделять значительное внимание поддержанию в актуальном состоянии осведомлённости и должным образом готовиться к защите своей конфиденциальной информации и информационных систем.

3. Помощь, доступная энергокомпаниям

3.1. Развитие стандартов

Растущее осознание рисков киберугроз подтолкнуло энергетиков к изучению стандартов информационной безопасности, применяемых в настоящее время для цифровых систем [25]. Недавно комитет по стандартизации начал анализ стандартов в области безопасности и телекоммуникаций применительно к вариантам применения в интеллектуальных энергосистемах.

Национальный институт стандартов и технологий США (NIST) представил всеобъемлющее руководство по анализу уровня рисков, требований и мер по обеспечению безопасности для основных логических сетевых интерфейсов [26]. В 2013 году 15-ая рабочая группа 57-го комитета Международной электротехнической комиссии (WG15 IEC TC 57) опубликовала библиографический список по системам защиты от кибератак [27]. Европейский комитет по стандартизации, Европейский Комитет по Электротехническим Стандартам и Европейский институт стандартизации в области связи (CEN/CENELEC/ETSI), в формате координационной группы, приступили к изучению подобных стандартов, применительно к области диспетчерского контроля «умных сетей» [28].

В вопросе поддержки, оказываемой энергетическим компаниям для решения задачи достижения всеобъемлющей безопасности управления, заслуживают внимания три (различающихся) каркаса основ защиты:

– Комитет ISA99, происхождение которого берёт начало в промышленности с непрерывным производством, весьма активно развивает процессы и спецификации, ориентированные на применение во всём объёме в разных отраслях индустрии, которые также могут быть использованы для энергетической отрасли. Их передовые проекты используются в качестве входных данных для МЭК (TC65) и перерабатываются в стандарты МЭК или технические доклады (серии МЭК 62443) за исключением МЭК 62443-2-4, который составлен на основе документов WIB (Ассоциация по автоматизации технологических процессов, Нидерланды) [29].
– Технический доклад ISO/IEC 27019 дополняет набор элементов управления, содержащийся в стандарте ISO/IEC 27002, предоставляя дополнительные указания для осуществления контроля, в соответствии с дополнительными требованиями энергетического сектора промышленности.
– Недавно предложенный NIST [30] базис построения системы защиты от кибератак ставит своей целью помочь операторам критических инфраструктур улучшить уровень киберзащиты и заслуживает особого внимания энергокомпаний.

Помимо этих трёх общих инициатив активность в отношении разработки и внедрения технических средств обеспечения безопасности для стандартных коммуникационных протоколов, таких как МЭК 61351, проявляют и поставщики систем управления, под эгидой IEC TC57 WG15. Кроме того, в области ядерной энергетики реализуются собственные инициативы – как на национальном уровне, например «Международный журнал по ядерной технике и технологиям» (NEI) 08-09 в США [31], так и на международном уровне (документы МАГАТЭ [32] и стандарты МЭК [33]).

3.2. Управление и организационные инициативы

Освоение и развитие активно-адаптивных интеллектуальных сетей побудило ЕС и США к созданию комплексных планов внедрения. И там, и там предусматривается разработка отраслевых перспективных планов («дорожные карты») с целью достижения кибербезопасности энергоснабжения.

Союз по иностранным делам и политике безопасности Евросоюза изложил своё видение и действия, необходимые для обеспечения открытого и безопасного киберпространства для государств-членов [34]. Эта концепция формулирует пять стратегических приоритетов:

1. Достижение устойчивости систем к внешним возмущениям в виртуальном пространстве.

2. Радикальное снижение уровня киберпреступности.

3. Создание политики защиты киберпространства и возможностей, связанных с общей доктриной безопасности и обороны (Common Security and Defense Policy – CSDP).

4. Разработка промышленных и технологических средств и приёмов обеспечения кибербезопасности.

5. Установление гармоничной и последовательной политики в области использования международного киберпространства Евросоюза и поощрения европейских ценностей.

Процесс реализация этой стратегии начался ближе к концу 2013 года и ускорился в 2014 году. Параллельно с этим Совет ЕС обсуждает возможность укрепления и расширения состава полномочий для Европейского агентства по сетевой и информационной безопасности (ENISA), образованного в 2004 году. Наряду с другими учреждениями ENISA играет ключевую роль в реализации и развёртывании стратегии ЕС. Вот, например, полномочия, запрашиваемые ENISA [33]:

– Содействие в создании для стран-участниц устойчивого киберпространства, обладающего способностью к восстановлению нормального функционирования, в частности путём выполнения экспертиз безопасности и устойчивости систем промышленного управления, транспортной и энергетической инфраструктуры.
– Разработка, в сотрудничестве с соответствующими национальными компетентными органами, заинтересованными сторонами, международными и европейскими органами по стандартизации, совместно с Объединённым исследовательским центром Комиссии Европейских сообществ, технических руководств и рекомендаций, адаптирующих стандарты и передовую практику сетевой информационной безопасности (NIS) для использования в государственном и частном секторе.
– Выявление новых тенденций и потребностей с учётом эволюции моделей киберпреступности и кибербезопасности, с целью разработки адекватных инструментов и технологий экспертизы.

Для облегчения и поддержки процесса создания общеевропейской интеллектуальной энергосистемы сформирована рабочая группа Еврокомиссии. Конечной целью этой программы является определение и подготовка набора нормативных рекомендаций для гарантированного и последовательного развития общеевропейской интеллектуальной сети с новыми сервисами и услугами и достижение преимуществ всеми участниками процесса [35]. Ключевым результатом работ экспертной группы №2 (EG2) будет выявление

соответствующих сценариев для выработки нормативов и рекомендаций для защиты данных. Цель состоит в создании инфраструктуры защиты, обеспечивающей конфиденциальность и доступность данных. Европейское агентство по сетевой и информационной безопасности (ENISA), в рамках программы работ экспертной группы (EG2), недавно опубликовало список мер безопасности для интеллектуальных сетей [36]. Этот список используется в качестве основы для координационной группы Европейского Комитета по электротехническим стандартам и Европейского института стандартизации в области связи для сопоставления со стандартами информационной безопасности и выявления незакрытых требований. Европейский проект развития безопасности энергетических систем (European project Security of Energy Systems – SoES) сделал шаг вперёд к заполнению пробелов, выявленных вышеупомянутыми группами экспертов [37].

Начиная с 2005 года, Министерство энергетики США в сотрудничестве с другими учреждениями США и Канады содействует разработке «дорожной карты» по повышению кибербезопасности для систем управления в энергетическом секторе. В 2011 году «дорожная карта» была обновлена [38], с учётом меняющегося ландшафта технологий Smart Grid, с опорой на новые приоритеты, с целью улучшения раскрытия уязвимостей, устранения всё более инновационных угроз, с выделением культуры безопасности, которая выходит за рамки простого соответствия требованиям. Цель США – к 2020 году реализовать устойчивые системы энергоснабжения, которые спроектированы, установлены и эксплуатируются таким образом, что поддержание важнейших функций не будет затронуто даже во время киберинцидентов.

3.3. Роль СИГРЭ

Международный Совет по большим электрическим системам высокого напряжения (СИГРЭ) продемонстрировал свою приверженность поддержке энергокомпаний в части решении вопросов обеспечения кибербезопасности и берёт на себя обязательства продолжить эту деятельность и в будущем. В этом разделе резюмируется деятельность рабочих групп СИГРЭ, связанных с этой темой.

Совместная рабочая группа СИГРЭ (СРГ) комитетов D2/B3/C2-01 «Безопасность информационных систем и корпоративных сетей в электроэнергетических системах». В период между 2003 и 2006 годами были проведены следующие виды работ. СРГ подготовила технические рекомендации [39], целью которых было повышение осведомлённости в вопросах информационной и кибербезопасности в электроэнергетических системах и выработка рекомендаций по решению задач обеспечения безопасности, сосредоточив внимание на моделировании в этой области, методологии оценки рисков и создании каркаса безопасности.

Рабочая группа СИГРЭ D2.22 «Подходы к обеспечению информационной безопасности для компаний электроэнергетики». Работа была проведена между 2006 и 2009 годами, в развитие результатов РГ D2.22. Исследование посвящалось углублённому рассмотрению трёх вопросов: как управлять информационной безопасностью; общей модели оценки рисков и методов предотвращения угроз, нападений и исправления уязвимостей; технологии безопасности для SCADA-систем управления сетями в реальном времени [40].

Рабочая группа СИГРЭ D2.31 «Принципы построения архитектуры безопасности для информационных систем в электроэнергетике». Рабочая группа начала работу в 2010 году. Завершение планировалось в 2014 году. Деятельность Рабочей группы структурирована по трём направлениям:

- Обсуждение методологий «глубокой обороны» и «поэтапного приближения к безопасности» в качестве базовых и надёжных подходов к организации защиты в электроэнергетике. Рабочая группа подвела итоги своей работы в документах [41] [1] [3].
- Моделирование кибератак с целью оценки безопасности интеллектуальных сетей как основного метода для дальнейшего развития архитектуры. Рабочая группа подвела итоги своей работы в документах [3], [42], [43].
- Обсуждение рисков использования удалённых услуг и передачи информации от партнёров/к партнёрам, а также передового опыта в части правил передачи информации для технического обслуживания внешним партнёрам и третьи лицам [44].

D2.38 СИГРЭ «Основы управления реагированием на риски, порождаемые киберугрозами, для объектов критической инфраструктуры». После завершения работы группы в 2015 году техническая брошюра будет описывать основной набор инструментов для электроэнергетических компаний, который можно использовать для автоматизации ответа на угрозы из информационного пространства. Выбор конкретных компонентов из этого набора будет основываться на данных, полученных в ходе глобального опроса энергокомпаний, заинтересованных в получении комплекта инструментов для автоматизированного ответа на угрозы.

B5-D2.46 СИГРЭ «Приложения и способы управления мерами по обеспечению кибербезопасности для систем защит и управления». Работа над технической брошюрой этой группы близится к

завершению и фокусируется на решении вопросов кибербезопасности с точки зрения систем защит и управления, включая обсуждение угроз, связанных с темой информации, стандартов, практических решений и тематических исследований.

Рабочая группа WG D2.01 исследовательского комитета D2 в 2013 году провела глобальное обследование [45] для определения приоритетных проблем операционных и бизнес-систем в энергокомпаниях. Эти результаты будут использоваться для формирования новых рабочих групп в качестве предпочтительной темы в 2014 году. В ходе опроса с высоким приоритетом была определена тема «Риски и кибербезопасность для развивающегося бизнеса и практики эксплуатации предприятий электроэнергетики», обусловленная бизнес-потребностями использования дистанционного управления и мобильных устройств. Эта информация помогла определить стратегию формирования новой рабочей группы, которой поручено развитие этой темы, после завершения своих задач группой WGD2.31. Таким образом, в планах исследовательского комитета D2 продолжать поддерживать энергокомпании будущими исследованиями по вопросам кибербезопасности.

3.4. Руководящие принципы для снижения риска, основанные на практике

Не существует одного простого действия, которое позволило бы устранить все угрозы кибербезопасности. Как можно видеть из всего вышесказанного, обеспечение безопасности это непрерывный процесс, который необходимо пересматривать на регулярной основе. Ниже приведены некоторые практические рекомендации, которые можно использовать для повышения безопасности систем (взято из [46]).

Организационные методы:

- Создать строгий процесс управления текущими рисками, включая определение критически важных активов.
- Установить эффективные процессы управления.
- Регулярно пересматривать организационные политики и процедуры, включая проведение самостоятельного аудита уровня информационной и физической безопасности.
- Регулярно создавать резервные копии (выполнять архивацию) систем и иметь планы аварийного восстановления.
- Чётко определить требования к кибербезопасности для внутренних целей и с любыми сторонними организациями.
- Обеспечить мониторинг функций, процессов и систем.
- Организовать процесс управления инцидентами.

Инженерные методы/коммуникационные сети:

- Определить сетевую топологию SCADA-ситемы и всех связанных присоединений.
- Свести к минимуму количество коммуникаций, при одновременном повышении надёжности каналов и оборудования связи.
- Не полагаться на ложное чувство безопасности, возникающее при использовании проприетарных протоколов. Закрытость корпоративных протоколов не делает их абсолютно безопасными.
- Придерживаться принципа использования эшелонированной защиты.

Методы работы с людьми:

- Чётко определить роли, сферы ответственности, полномочия и функциональные обязанности для менеджеров, системных администраторов и пользователей в процессе обеспечения информационной безопасности.
- Разработать соответственные инструкции для персонала и регулярно проводить его обучение.

Другая практическая информация может быть найдена в следующих документах (не исчерпывающий перечень):

- Документы совместной рабочей группы СИГРЭ, комитеты D2/B3/C2-01: «Управление информационной безопасностью в электрических системах».
- Технический доклад ISO/IEC №27019.
- Стандарт NIST SP 800-82: «Руководство по безопасности систем управления в промышленности (ICS)».
- Документы VDI/VDE 2182.
- VGB R175z «Информационная безопасность для электрических станций».
- CPNI: «Рекомендуемые стандарты безопасности – для АСУ ТП и SCADA-систем».

4. Заключение и перспективы

Процесс взаимопроникновения эксплуатационных и информационных технологий всеобъемлющ. Для электроэнергетики ещё большую значимость и критичность приобретают коммуникационная инфраструктура и информационные потоки. В то же время эта отрасль становится всё более привлекательной мишенью, как для злонамеренных субъектов, так и для иностранных государственных учреждений. Таким образом, в энергетике принципиальное значение теперь имеет то, в какой мере принимаются во внимание угрозы и риски кибербезопасности по всем организациям, повышение осведомлённости в этих вопросах на уровне управления и производства, включая поставщиков, партнёров и иных третьих лиц.

Источник: Status of Cybersecurity, Electra. № 276

Перевод и адаптация текста – П. Литвинов, ЗАО «РТСофт»

5. Список источников

1. J.-T. Zerbst, S. Zimmermann, D.K. Holstein, and C. Poirier, "Towards an adapted classification methodology for graded security approaches in EPU architectures" CIGRE Symposium, Lisbon, 2013

2. J.-T. Zerbst, L. Pietre-Cambacedes, G. Dondossola, J. McDonald, M. Ekstedt, "Cyber-attack modeling and security graded approach: key elements when designing security architecture for Electric Power Utilities (EPUs)," 44th CIGRE Session, Paris, 2012

3. European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace“, Brussel, 2013

4. Cyberspace policy review: Assuring a Trusted and Resilient Information and Communications Infrastructure http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

5. Christiane Grefe,“Blackout”, Die Zeit 16/2014 – http://www.zeit.de/2014/16/blackout-energiehacker-stadtwerk-ettlingen

6. Felix Lindner, ”Licht aus!”, c't magazin 09/2014 – http://heise.de/-2165153

7. L. Pietre-Cambacedes , M. Tritschler and G. Ericsson, "Cyber security myths on power control systems: 21 misconceptions and false beliefs," IEEE Transactions on Power Delivery, Vol. 26, Issue 1, pp. 161–172, January 2011.

8. R. Langer, “Robust Control System Networks – How to achieve reliable control after Stuxnet”, Momentum Press, New York, 2012

9. J.-T. Zerbst, L. Pietre-Cambacedes, Å. Torkilseng and O. Breton, "Graded approach to cyber security for EPUs: Clarifying the security levels and zones concepts," CIGRE D2 Colloquium, Buenos Aires 2011

10. Nicolas Falliere, Liam O Murchu, Eric Chien, “W32.Stuxnet Dossier”, 2011 – http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

11. ABB white paper: “Security in the Smart Grids”, 2009 - http://www02.abb.com/db/db0003/db002698.nsf/0/832c29e54746dd0fc12576400024ef16/$file/paper_Security+in+the+Smart+Grid+%28Sept+09%29_docnum.pdf

12. Jacobs, Mike. "10 Years After Record Blackout, Is U.S. Any Better Prepared? (Op-Ed)." LiveScience. TechMedia Network, 14 Aug. 2013. Web. 17 Apr. 2014. http://www.livescience.com/38905-is-nation-better-prepared-to-prevent-blackouts.html

13. Kim Zetter, “Researchers Uncover Holes That Open Power Stations to Hacking”, wired.com, 2013 - http://www.wired.com/2013/10/ics/ [14] G. Dondossola, F. Garrone, J. Szanto “Cyber Risks in Energy Grid ICT Infrastructures” in Critical Infrastructure Protection and Resilience in the ICT Sector, Paul Theron and S. Bologna Ed., IGI Global, 2013

14. G. Dondossola, F. Garrone, J. Szanto “Cyber Risks in Energy Grid ICT Infrastructures” in Critical Infrastructure Protection and Resilience in the ICT Sector, Paul Theron and S. Bologna Ed., IGI Global, 2013

15. ICS-CERT Monitor “Incident Response Activity – October, November, December 2013”, 2013 – http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf

16. C. Wueest, Symantec, “Targeted Attacks Against the Energy Sector”, 2014

17. Stefan Frei, “ Vulnerability Threat Trends: A DECADE IN REVIEW, TRANSITION ON THE WAY”, NSS Labs, Inc., 2013

18. J. Zerbst, M. Schaefer, I. Rinta-Jouppi, "Zone principles as Cyber Security architecture element for Smart Grids", Innovative Smart Grid Technologies Conference Europe (ISGT Europe), 2010 IEEE PES

19. Symantec Security Response: Dragonfly: Western Energy Companies Under Sabotage Threat - http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear

20. François Page, McAfee Labs, ”Hacktivism Cyberspace has become the new medium for political voices”, 2012

21. Heather MacKenzie, „Shamoon Malware and SCADA Security“, 2012 – http://www.isssource.com/shamoon-malware-and-scadasecurity/

22. Marshall Abrams, Joe Weiss “Malicious Control System Cyber Security Attack Case Study Maroochy Water Services, Australia”, 2008 – http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

23. Ryan Naraine, ” Shodan search exposes insecure SCADA systems”, 2010 – http://www.zdnet.com/blog/security/shodan-searchexposes-insecure-scada-systems/7611

24. Kevin Poulsen, ”Slammer worm crashed Ohio nuke plant net”, 2003 http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/

25. L. Pi`etre-Cambacéd`es, T. Kropp, J. Weiss, R. Pellizzoni “Cybersecurity standards for the electric power industry – a survival kit”, Paper D2-217, CIGRE Paris Session 2008, France

26. The NIST Smart Grid Interoperability Panel Cyber Security Working Group, “Introduction to NISTIR 7628 – Guidelines for Smart Grid Cyber Security”, September 2010. http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

27. F. Cleveland, “List of Cybersecurity for Smart Grid Standards and Guidelines”, May 2013. http://iectc57.ucaiug.org/wg15public/Public%20Documents/List%20of%20Smart%20Grid%20Standards%20with%20Cybersecurity.pdf

28. Smart Grid Coordination Group Set of Standards Working Group “First set of standards” version 2.0, November 2012. http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/xpert_group1_first_set_of_standards.pdf

29. см. “Working-party on Instrument Behaviour” (WIB) web site at www.wib.nl

30. NIST Cybersecurity Framework http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

31. Nuclear Energy Institute, NEI 08–09 Cyber Security Plan for Nuclear Power Reactors (rev. 6), April 2010

32. IAEA Nuclear Security Series No. 17, Reference Manual, Computer Security aAt Nuclear Facilities, 2011

33. L. Pietre-Cambacedes, T. Quinn, L. Hardin "Cyber Security of Nuclear Instrumentation and Control Systems – Overview of the IEC Standardization Activities" IFAC conference on Manufacturing, Management and Control (MIM 2013), Invited session on Cybersecurity of Control and Safety systems, St. Petersburg, Russia, June 2013

34. European-Commission, "Cybersecurity strategy of the European Union: An open, safe and secure cyberspace," European Commission, Joint Communication JOIN (2013) 1 final, 7 February 2013

35. European Network and Information Security Agency (ENISA), “Smart Grid Security, Recommendations for Europe and Member States – Annex 5 Smart Grid Security Related Initiatives”, 2012-03-31

36. European Network and Information Security Agency (ENISA), “Smart Grid Security, Recommendations for Europe and Member States”, 2012-07-01

37. SoES Project, “Internation Standards and Policies – Map and Analysis”, Security of Energy Systems Project, Deliverable D2, 2014. http://www.soes-project.eu

38. ECSWG, "Roadmap to Achieve Energy Delivery Systems Cybersecurity," US Department of Energy September 2011

39. Cigré JWG D2/B3/C2-1 Technical Brochure TB 317 on “Security for Information Systems and Intranets in Electric Power Systems”, 2007

40. Technical Brochure 419 of the WG D2.22 "Information Security for Electric Power Utilities (EPUs) — CIGRE Developments on Frameworks, Risk Assessment, and Technology", 2010

41. J.-T. Zerbst, L. Pietre-Cambacedes, Å. Torkilseng and O. Breton, "Graded approach to cyber security for EPUs: Clarifying the security levels and zones concepts," 2011 CIGRE D2 Colloquium, Buenos Aires, Argentina, October 2011

42. G. Dondossola, L. Pi`etre-Cambacéd`es, J. McDonald, M. Ekstedt, A. Torkilseng “Modelling of cyber-attacks for assessing smart grid security”, D2 Colloquium 2011, Buenos Aires, 2011

43. M. Ekstedt, M. Korman, R. Terruggia, G. Dondossola, “Application of a cyber-security assessment framework to smart grid ICT architectures” SCD2 Colloquium 2013, India

44. P. Sitbon, C. Poirier, J.-T. Zerbst, D.K. Holstein, M. Scherer, R. Evans, Marc Tritschler, “Security in remote services used by EPUs”, 45th CIGRE Session, Paris, 2014

45. WG D2.01 Report, Electra No 274, “Strategic Priorities for Information Systems Issues”, June 2014

46. US Department of Energy, “21 Steps to Improve Cyber Security of SCADA Networks”, 2002

Давид Гил (David Gil), Асиер Лано (Asier Llano), Фернандо Кастро (Fernando Castro), Хосе Антонио Морено (Jose Antonio Moreno), Соня Мартинес (Sonia Martinez), Txetxu Арсуага (Txetxu Arzuaga), ZIV CG Automation, Испания

Применение телекоммуникационных технологий PLC при подключении объектов распределённой генерации к электрическим сетям

Объекты распределённой генерации (Distributed Energy Resources, DER – распределённые энергетические ресурсы) в настоящее время развернуты вдоль сетей среднего напряжения (СН) и низкого напряжения (НН) распределительных электрических сетей и являются неотъемлемым компонентом «умной» сети. Для подключения DER в электрическую сеть требуется обеспечение информационного обмена систем автоматизации управления в распределительных электросетевых компаниях с этими установками в режиме «всегда на связи». Наиболее привлекательными для обеспечения такой коммуникационной инфраструктуры являются технологии PLC (Power Line Communication).

В статье приводятся основные требования к интеграции распределённых энергетических ресурсов в распределительные электрические сети, особое внимание уделено интеграции в сеть низкого напряжения (НН). Описаны основные характеристики сети НН, используемой в качестве телекоммуникационного средства обмена информацией. Анализируются различные технологии PLC (Power Line Communication), которые можно использовать в качестве технологической основы для этой цели, например Powerline Intelligent Metering Evolution (PRIME). Как резюме в статье рассматривается вопрос об особенностях функционирования новых технологий PLC совместно с унаследованными приложениями, такими как Advanced Metering Infrastructure (AMI), используемыми в системах учёта электроэнергии (ЭЭ), при их реализации поверх сети связи PLC.

Ключевые слова: интеграция объектов распределительной генерации, сети низкого напряжения, аварийное отключение, телекоммуникационные технологии PLC, PRIME, борьба с созданием изолированных участков сети после аварии.

Новые вызовы при интеграции объектов распределительной генерации – автопроизводители

Автопроизводители, являясь особым субъектом в энергетическом секторе, представляют собой новый вид потребителей энергии – энергопредприятия, которые не только потребляют электроэнергию, но и вырабатывают её и поставляют на рынок. Подобные компании, как правило, частные, и во многих странах электроэнергетические и коммунальные электросетевые компании обязаны по закону приобретать электроэнергию (ЭЭ), выдаваемую в сеть энергопредприятиями. Тем не менее качество параллельной работы с сетью при подаче электроэнергии, подаваемой в электрическую сеть от собственных вырабатываемых энергоресурсов энергопредприятия, не гарантируется. По этой причине электроэнергетические и коммунальные сетевые компании должны быть обеспечены информационным обменом с энергопредприятиями при интеграции объектов DER в свои сети:

- Основные технологические параметры должны контролироваться в режиме реального времени, например напряжение, ток, активная и реактивная мощности.
- Энергетические или коммунальные компании должны предоставлять средства для отключения энергопредприятия от сети, если текущее состояние сети этого требует.

– Энергетические или коммунальные компании должны предотвратить случайное или несанкционированное повторное подключение к сети энергопредприятий, если условия подключения к электрической сети не выполняются.

Во многих странах объекты распределённой генерации устанавливаются вдоль сети НН, что усложняет процесс управления интеграцией этих объектов в сеть, поскольку энергетическим и/или коммунальным сетевым компаниям требуется собирать информацию от всех источников генерации, подключенных к сети СН или НН.

Многие объекты распределённой генерации, которые подключены к сети СН, располагают устройствами телемеханики контролируемого пункта с каналами связи по линиям электропередачи или по радио, что позволяет им осуществлять обмен информацией с энергетическими или коммунальными компаниям. Для низковольтных установок требуется новое поколение интеллектуальных электронных устройств в целях обеспечения определённого уровня дистанционного управления данным типом оборудования. Коммутационный аппарат, подключающий инвертор DER-оборудования к сети, должен быть как минимум под телеуправлением. Для энергетических или коммунальных компаний требуется также получение отдельных параметров электрического режима, таких как напряжение, активная и реактивная мощности. По причине наличия инвестирования в энергетические и коммунальные компании, они создают передовую инфраструктуру системы измерений, которая может стать третьей стороной телекоммуникационных услуг как альтернативы для интеграции с DER. Поэтому следует проанализировать возможность применения PLC-технологий для обеспечения телеуправления оборудованием распределённой генерации.

В случае использования телекоммуникационной технологии PLC архитектура системы представлена на рис. 1. Она включает новые функции, которые будут выполняться на распределительной подстанции, где происходит управление всеми объектами распределённой генерации, подключенными к её фидерам (аналогичным образом концентратор данных управляет всеми смарт-счётчиками, обслуживаемыми низковольтными фидерами). Также небольшие RTU-устройства (дистанционный передатчик) с PLC-технологией должны быть установлены в каждом устройстве распределённой генерации НН в качестве информационного датчика – источника данных генерации для энергопредприятий.

В статье основной упор будет сделан на оценке возможностей расширения инфраструктуры PLC, уже развёрнутой для приложений смарт-измерений ЭЭ, с целью обеспечения информационного обмена с объектами распределённой генерации в сети НН. Анализ проводится на основе использования технологии Powerline Intelligent Metering Evolution (PRIME) [1].

Сети НН как средство телекоммуникаций

Существует несколько документов, моделирующих сети НН как телекоммуникационный канал. В данном разделе будут обобщаться некоторые из основных исследований, которые изложены в разных работах [9, 3, 4, 11 и 7]. При моделировании сети НН как телекоммуникационного канала необходимо учитывать следующие основные аспекты:

– Шум. Какие внешние факторы могут мешать принимаемому сигналу.
– Импульсные характеристики канала. Как телекоммуникационный сигнал изменяется при распространении по сети НН.
– Импеданс канала. Как увеличить мощность PLC-сигнала, вводимого в сеть.

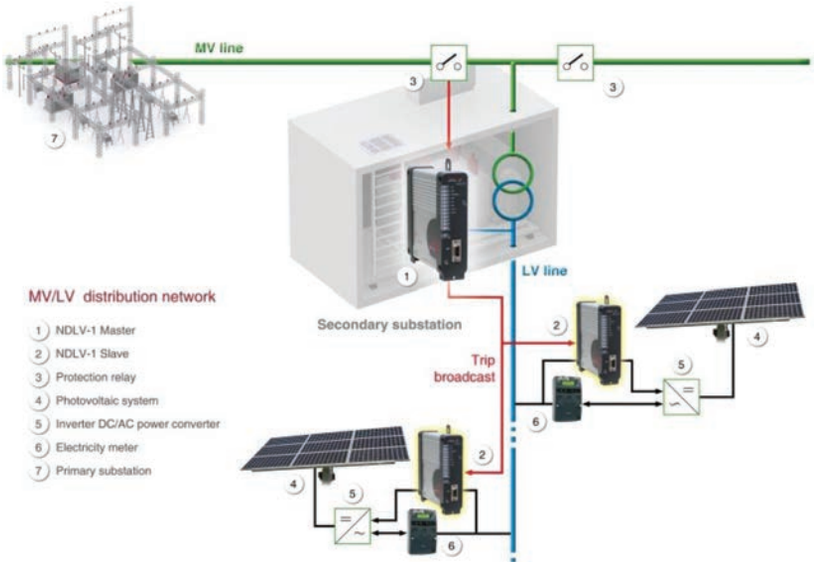


Рис. 1. Архитектура системы

Шум в сети НН

Есть несколько способов классифицировать причины нарушения сигнала, которые могут возникнуть в сети [8], тем не менее для PLC предпочтительны параметры классификации, которые сформулированы в [3], – частота и временной интервал, периодичность или его синхронизация с сетью. На основе

таких параметров классификация шума может выглядеть следующим образом:

– фоновый шум/помехи,
– импульсный шум,
– синхронный шум (в сети),
– узкополосный шум.

Фоновый шум/помехи

Фоновый шум является широкополосным и имеет статичный характер. Его удельная мощность достаточно низкая по сравнению с другими нарушениями, но его изучение интересно тем, что оно всегда имеет предмет исследования. Как правило, фоновый шум можно найти в сети НН [9, 4, 12]. Данные материалы указывают на потерю уровня сигнала до 35 дБ/декаду со значениями –90 дБ (Вт/Гц) на частоте 9 кГц и –125 дБ (Вт/Гц) на частоте 95 кГц. Эти цифры меняются в зависимости от времени, и их значения зависят от потребления электроэнергии. Показания стабильны в часы пик. С другой стороны, в часы пиковых нагрузок коэффициент шума может быть в пределах от 15 дБ и даже выше 20 дБ.

Хотя шум по своей природе может отличаться от одной сети НН к другой (это зависит от различных типов нагрузок – двигатели, освещение и пр.), на основании статистических данных фоновый шум может быть рассчитан по следующей формуле [4]:

$$N(f) = 10^{K-3.95\times10^{-5}f} \quad [\frac{W}{Hz}]$$

где К – переменная нормального распределения с усредненной μ = –σσ8,64. Стандартное отклонение σ величины К составляет 0,5 (измеряется при входном импедансе 50 Ом). Если перевести функцию распределения мощности в формулу напряжения, применима следующая формула:

$$N(f) = \sqrt{50} \times 10^{\frac{K}{2}-1,975\times10^{-5}\times f} \quad [\frac{V_{RMS}}{Hz}]$$

Данная формула для вычисления шума удобнее, поскольку многие устройства связи (несколько сотен) совместно используют коммуникационную среду сети НН, чьи устройства имеют высокий входной импеданс, чтобы минимизировать его эффект для разделяемой среды передачи данных.

Основываясь на результатах [10], в городской сети мощность шума может составлять около 73 дБ VRMS, а за городом значения шума могут достигать 48 дБ VRMS.

Импульсный шум

Импульсный шум характеризуется короткой продолжительностью по сравнению с длительностью процессов, происходящих в телекоммуникационных системах. Его природа связана с преходящими эффектами, которые возникают, например, при включении компьютера или телевизора.

В некоторых статьях [3] продолжительность импульсного шума ограничена 100 мкс. Другие ссылки [11] определяют различные ограничения по продолжительности (между 1 мкс и 48 мс), хотя некоторые авторы рассматривают последний отрезок в качестве пульсирующего шума.

Амплитуда, длительность и частота импульсных шумов очень разнообразна. Можно считать, что чем выше продолжительность, тем меньше амплитуда, и наоборот.

Импульсные шумы можно классифицировать по периодичности:

– Апериодический импульсный шум. Этот тип шумов может достигать очень больших значений амплитуды, таких как 2 кВ. Они могут быть вызваны включением разъединителя.
– Синхронный периодически возникающий импульсный шум в сети. Этот тип шумов может быть вызван некоторыми инверторами AC–DC/DC–AC. Он является периодическим (та же частота, как и частота сети или одной из её гармоник) импульсным сигналом.
– Асинхронный периодически возникающий импульсный шум в сети. В этом случае период шума не имеет ничего общего с частотой сети. Это может быть вызвано различными коммутационными состояниями электрических машин (повторяющиеся помехи).

Узкополосный шум

Узкополосный шум влияет только на небольшую часть полосы пропускания канала связи PLC. Этот шум может быть вызван резонансными эффектами сопротивления линии НН, которые концентрируют бóльшую часть мощности шума в определённых частотах. Также данный тип шума могут вызвать частотные селективные устройства, подключённые к сети, например импульсные источники питания. Кроме того, ещё одним источником возникновения узкополосного шума в линиях НН может стать радиовещание (AM).

Импульсная характеристика канала

Частотную характеристику канала трудно спрогнозировать в низковольтных ЛЭП. Это зависит от точки измерения, от топологии сети, а также от распределения нагрузки. Некоторые данные [3] показывают, что затухание может достигать значений и в 100 дБ/км. Тем не менее в некоторых промышленных низковольтных ЛЭП длиной 750 м можно видеть ослабление всего в 20 дБ. В этом случае не так чётко можно увидеть экспоненциальную зависимость между затуханием и расстоянием. Также можно найти пределы затухания начиная от 40 дБ до 100 дБ. Групповая задержка в полосе CENELEC A незаметна [2] для узкополосных коммуникаций, где длительность передачи символа намного выше.

Для цифровых схем модуляции фазы, со временем могут иметь достаточную значимость фазовые вариации. Некоторые данные [3] показывают, что такие вариации должны быть ниже, чем ±10 ° [3], будучи, возможно, когерентными демодуляциями.

Функциональные характеристики PRIME для сетей НН

PRIME – это система связи, специально разработанная для преодоления проблем использования PLC в сети НН. Это узкополосная OFDM-система (Orthogonal Frequency-Division Multiplexing – мультиплексирование с ортогональным частотным разделением каналов), которая поддерживается организацией PRIME-Alliance. Система PRIME была стандартизирована ITUT G.9901 [5] и G.9904 [6], кроме того она была стандартизирована по IEEE как часть стандарта IEEE P1901.

Система PRIME состоит из трёх уровней связи, как представлено на рис. 2:

– Уровень конвергенции (совмещения) CL отвечает за размещение единицы данных протокола на уровне MAC.
– Уровень MAC отвечает за предоставление механизма, позволяющего создать сеть PRIME. Он также контролирует доступ всех узлов к общему каналу Powerline.
– Уровень PHY отвечает за прямую связь между узлами сети.

Обычно PHY-уровень отвечает за преодоление помех, с которыми можно столкнуться в сети (шум и импульсная характеристика канала). В нашем случае PRIME PHY-уровень на основе OFDM имеет 97 вспомогательных частот в CENELEC A-Band (от 41,992 кГц до 88,867 кГц). Хотя есть шесть различных схем модуляции, доступных для всех простых вспомогательных частот, в данной области используются только сверхточные режимы кодирования (DBPSK, DQPSK, D8PSK). Из-за особенностей MAC частота ошибок 10^{-3} считается отличным показателем для обеспечения того, что значение будет правильно согласовано с уровнем приложений связи. Даже худшие значения величины 10^{-2} могут быть достаточными, чтобы поддерживать связь. В качестве эталона на рис. 3 показано поведение PRIME-системы в селективном частотном канале. Наблюдается снижение чувствительности приёмника менее 2 дБ из-за данного вида помех.

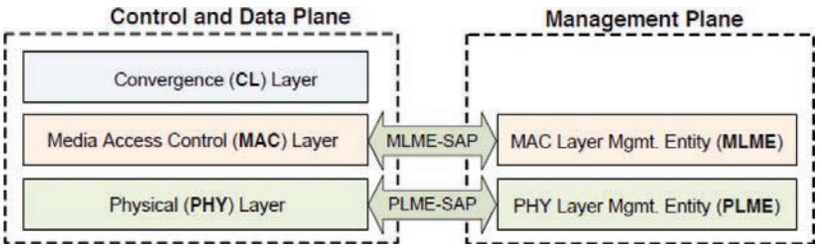


Рис. 2. Уровни связи системы PRIME

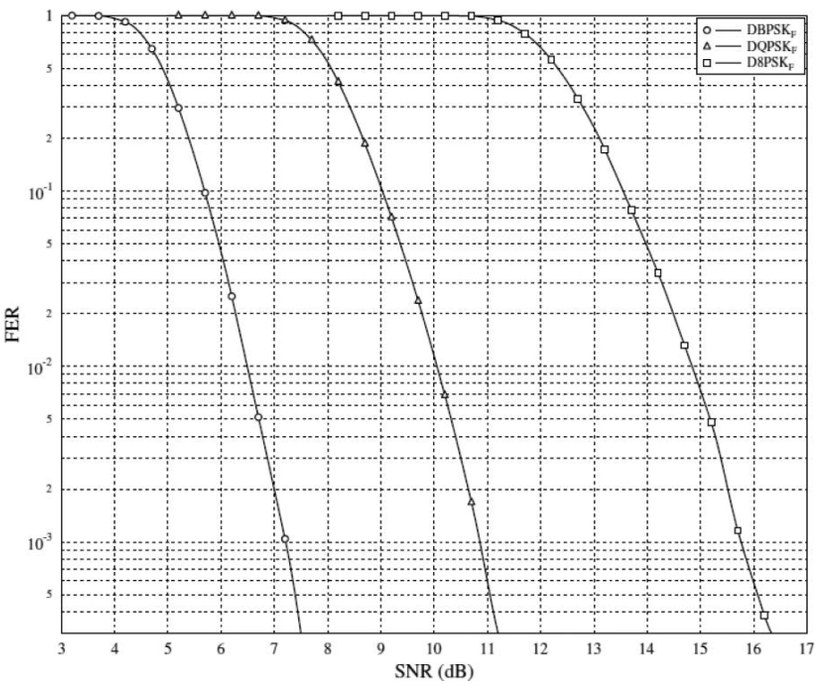


Рис. 3. Поведение PRIME–системы при нарушениях

Также очень хорошие реакции PRIME наблюдаются при наличии импульсных шумов. Для длительности импульса менее 500 мкс амплитуда колебания шума 20 дБ (в сравнении с пиком импульсного шума на фоне шумов) в системе PRIME составила только 7,5 дБ.

Выводом по данному разделу является то, что надёжные схемы модуляции для PRIME-системы подходят также для приложений телемеханики. Возникает следующий вопрос: каковы имеющиеся возможности для использования PRIME в сети с уже развёрнутой системой интеллектуального учёта электроэнергии (Smart Metering)?

Передача сигналов телеуправления по сети НН в PRIME–системе

В соответствии со спецификацией PRIME [1], время передачи делится на MAC-кадры. Базовый узел и узел оказания услуг могут получить доступ к каналу в период поочередного использования канала связи (Shared Contention Period, SCP) или запросить период без контроли-

руемого доступа (Contention-Free Period, CFP). Что касается последнего, базовый узел отвечает за предоставление доступа к CFP. На рис. 4 показана структура MAC-кадра.

Длина MAC-кадра составляет 276 символов OFDM (каждый символ длится 2,24 мс), что составляет 618,24 мс. Максимальная длина для SCP возникает только тогда, когда нет выделенного доступа к каналу (CFP), что служит основой для приложений смарт-измерений. Следует обратить внимание на то, что по крайней мере один слот сигнала (4 символа) всегда присутствует (один генерируется базовым узлом). Если сервисные узлы должны преобразовываться в коммутаторы, то длина SCP уменьшается на 4 символа.

Сервисные узлы, реализующие приложения телемеханики, могут либо подключиться к каналу (как и любой другой PRIME-узел), либо потребовать CFP. В первом случае приложения телеуправления будут конкурировать за доступ к каналу измерительной смарт-системы. Тем не менее они могут конкурировать путем назначения более высокого уровня приоритета MAC, чем тот, который связан с применением смарт-измерений. Во втором случае приложения телемеханики сокращают время, доступное для приложений смарт-измерений, которые могут повлиять на производительность системы и, что ещё хуже, на стабильность сети, потому что весь трафик контроля отвечает за поддержание топологии сети связи во время SCP.

Приложения телемеханики, использующие CFP

Возможность иметь CFP для приложений телемеханики весьма привлекательна, но следует отметить, что могут возникать неявные постоянные задержки из-за используемого свойства временного уплотнения. В худшем случае для этой задержки длина MAC-кадра будет 618,24 мс (команда телеуправления должна направляться по базовым узлам при запуске MAC-кадра).

Другой аспект связан с нижней длиной посылки для SCP. Стабильность сети PRIME зависит от правильного обмена контрольной информацией между узлами обслуживания и базовым узлом. Данная контрольная информация обменивается внутри SCP, и ему присваивается высокий приоритет MAC (уровень приоритета 1). Если выполнение этой связи ухудшается из-за сокращения длины SCP, стабильность сети связи будет значительно снижена.

Некоторые расчёты авторов показывают, что снижение SCP до 230 символов будет влиять на стабильность сети в незначительной степени. Это означает, что SCP для приложений телеуправления будет возможно (с продолжительностью до 30 символов – обратите внимание, что в самой надёжной модуляции, DBPSKF, каждый символ содержит 48 бит). Единственный недостаток этого варианта – временное уплотнение, что означает в худшем случае задержку MAC-кадра.

Приложения телемеханики, конкурирующие с приложениями смарт–измерений

При данном раскладе устройства телемеханики конкурируют со смарт-счётчиками для доступа к каналу в течение передачи SCP. В связи с характером данных телемеханики им требуется назначать более высокий приоритет, чем у смарт-счётчиков, но более низкий приоритет, чем у PRIME-данных управления сетью, из-за его влияния на стабильность сети связи.

Имея в виду степень важности данных, которые передаются, можно предположить, что текущее использование канала, организованное узлами смарт-измерений, может означать, что одновременно пытаются получить доступ к каналу максимум 3-4 устройства (скорее, 2-3). Моделирование, выполненное авторами, показывает, что нагрузка системы телемеханики может также конкурировать с нагрузкой смарт-измерений. Только одно условие, как было сказано выше, назначает более высокий приоритет. В этом случае полученные задержки для 95 % нагрузки телемеханики будут меньше, чем 30 мс из-за алгоритмов доступа канала CSMA/CA.

Передача трафика телеуправления по сети НН (FSK)

Другая возможность состоит в применении подхода *similar-to-a-teleprotection (аналогично телезащите)*, что позволит энергетическим и коммунальным компаниям управлять состоянием коммутационных аппаратов в сети. Для этого может быть использована хорошо зарекомендовавшая себя схема модуляции – частотная манипуляция Frequency Shift Keying, (FSK). В этой схеме модуляции данные передаются с помощью сдвига частоты непрерывной величины в двоичной форме (к одной или другой) из двух дискретных частот. Этап приёма основан на согласованных фильтрах. Выход из согласованных фильтров будет сравниваться для принятия решения, если была получена первая частота, вторая, или ни одна из них. На рис. 5 схематически изображён такой ресивер.

В предыдущих разделах были описаны серьёзные проблемы с шумом сигнала РКС в сети НН. FSK-

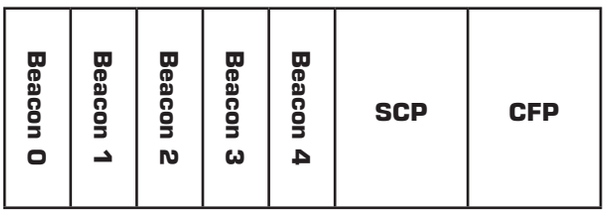


Рис. 4. Спецификация структуры кадров в PRIME

модуляция устойчива к шуму и позволит получать полезные данные в таких каналах связи. Также это даёт возможность работать с группой современных систем учёта ЭЭ.

Рис. 5. Схема фильтрации при использовании FSK

FSK-модем можно использовать для отправки и получения данных от энергопредприятий. Очевидно, что это решение не будет быстрее, но в некоторых случаях развеётывание может обеспечить хорошее средство борьбы с шумом. Возможно, самое интересное приложение связанно с использованием FSK-модема как устройства защиты оборудования ВН. В этом случае энергетические и коммунальные компании могут получить уровень надёжности связи выше 10^{-3} (при SNR 6 дБ), а безопасность передачи лучше, чем 10^{-6} при SNR 6 дБ. Это вполне допустимо, когда энергетическим и муниципальным компаниям нужно только передавать телесигнал ON/OFF энергопредприятиям для управления состоянием выключателя на устройства DER.

Используя данный подход, можно контролировать линию ВН и определять, существует ли ошибка передачи в линии связи, а также отслеживать момент потери связи с распределительной ПС (выход согласованных фильтров будет равен нулю в обоих случаях). FSK-модем может также отправить команду на выключатель или активировать сигнал для дальнейшего принятия решения. Это необходимо, чтобы избежать ответвлений в сетях НН.

Выводы

В статье показаны возможности использования технологии связи по линиям НН для интеграции комплексов DER в электрические сети. Некоторые возможности уже доступны для энергетических и коммунальных компаний. Рассмотрены несколько вариантов передачи информации, например с использованием существующих систем AMI на основе PRIME (либо в конкуренции с трафиком измерений или временем резервирования канала для этого приложения) или с использованием подхода *similar-to-a-teleprotection (аналогично телезащите)* для отправки команд включения-выключения коммутационных аппаратов оборудования энергопредприятий.

Литература

1. PRIME Alliance. PRIME Alliance home page. URL: http://www.prime-alliance.org (visitado 24-06-2013).

2. Nuria González-Prelcic y col. «A Channel Model for the Galician Low Voltage Mains Network».Power Line Communications and Its Applications (ISPLC), 2001 IEEE International Symposium on. 2001, pages 365–370.

3. O. G. Hooijen. «A Channel Model for the Low-Voltage Power- Line Channel; Measurement and Simulation Results».Power Line Communications and Its Applications, 1997.ISPLC 1997.IEEE International Symposium on. 1997.

4. O. G. Hooijen. «A channel model for the residential power circuit used as a digital communications medium». Electromagnetic Compatibility, IEEE Transactions on 40.4 (1998), pages 331–336. ISSN: 0018-9375. DOI: 10.1109/15.736218.

5. ITU-T. G.9901 Narrowband othogonal frequency division multiplexing power line communication transceivers – Power spectral density specification. Norm. 2012.

6. ITU-T. G.9904 Narrowband othogonal frequency division multiplexing power line communication transceivers for PRIME networks. Norm. 2012.

7. Wenqing Liu, M. Sigle y K. Dostert. «Channel phase distortion and its influence on PLC systems».Power Line Communications and Its Applications (ISPLC), 2012 16th IEEE International Symposium on.2012, pages 268–273. DOI: 10.1109/ISPLC.2012.6201341.

8. L. M. Millanta y M. M. Forti.«A classification of the powerline voltage disturbances for an exhaustive description and measurement».Electromagnetic Compatibility, 1989, IEEE 1989 National Symposium on. 1989, pages 332–336. DOI:10.1109/NSEMC.1989.37202.

9. J. B. O'Neal Jr. «The Residential Power Circuit as a Communication Medium». En: Consumer Electronics, IEEE Transactions on CE-32.3 (1986), pages 567–577. ISSN: 0098-3063. DOI: 10.1109/TCE.1986.290080.

10. A. A. Smith. «Power Line Noise Survey».En: Electromagnetic Compatibility, IEEE Transactions on EMC-14.1 (1972), pages 31–32. ISSN: 0018-9375. DOI: 10.1109/TEMC.1972.303202.

11. M. Tlich y col. «Novel approach for PLC impulsive noise modelling». En: Power Line Communications and Its Applications, 2009. ISPLC 2009.IEEE International Symposium on. 2009, pages 20–25. DOI: 10.1109/ISPLC.2009.4913397.

12. R. M. Vines y col. «Noise on Residential Power Distribution Circuits». Electromagnetic Compatibility, IEEE Transactions on EMC-26.4 (1984); pages 161–168. ISSN: 0018-9375. DOI: 10.1109/TEMC.1984.304217.

Источник: Powerline communications for connecting distributed energy resources

Перевод и адаптация текста - М. Задонская, А. Вериго, ЗАО «РТСофт»