ISSN 18817-0455

www.controlengineering.ru

CONTROL ENGINEERING Россия

№ 2 (68)

Открывает мир управления, автоматики и оборудования

апрель 2017

ИНТЕЛЛЕКТУАЛЬНЫЕ НЕФТЯНЫЕ МЕСТОРОЖДЕНИЯ

РОБОТЫ БУДУЩЕГО И БИОМЕХАТРОНИКА

КИБЕРПРОСТРАНСТВО: ПРАВИЛА БЕЗОПАСНОСТИ

oni разумная автоматика

Приглашаем посетить наш стенд на выставке «Нефтегаз 2017»: 17 – 20 апреля, Москва, Экспоцентр, павильон 2, зал 3, стенд № 23F65

Реклама

Основа системы

- электродвигатели
- преобразователи частоты
- программируемые контроллеры
- логические реле
- панели операторов
- программное обеспечение
- комплексные отраслевые решения

www.oni-system.com

тел. (495) 502-79-81, info@oni-system.com

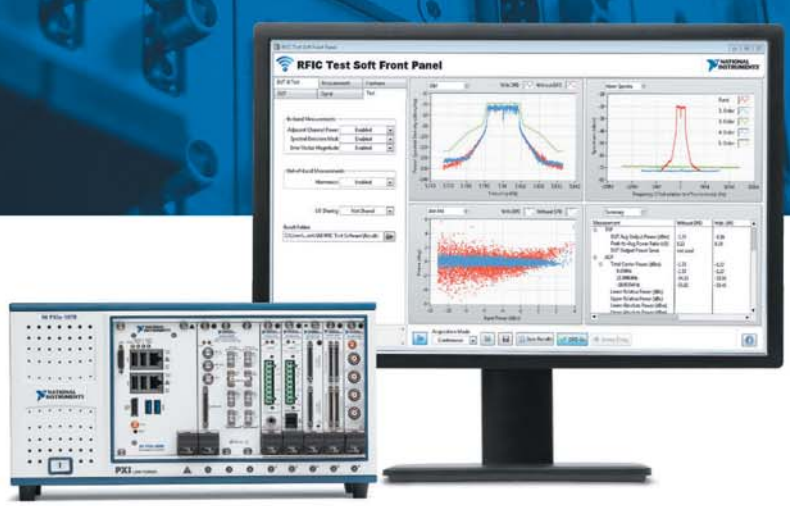
УМНЫЕ УСТРОЙСТВА ТРЕБУЮТ

УМНЫЕ

СИСТЕМЫ ТЕСТИРОВАНИЯ

Традиционный подход к автоматизированным системам тестирования не оправдывает себя. Для тестирования умных устройств необходимо использовать передовые системы, такие как платформы PXI и программное обеспечения LabVIEW и TestStand. Более 35 000 компаний по всему миру используют данный подход, который позволяет существенно снизить стоимость тестирования.

Будьте готовы к вызовам будущего:
ni.com/smarter-test



NATIONAL INSTRUMENTS™

NI PXI, LabVIEW, and TestStand

Реклама

©2017 National Instruments. All rights reserved. LabVIEW, National Instruments, NI, ni.com, and NI TestStand are trademarks of National Instruments. Other product and company names listed are trademarks or trade names of their respective companies. 25198

INNOPROM

10—13 Июля 2017

ГЛАВНАЯ ЭКСПОРТНАЯ ПЛОЩАДКА РОССИИ

г. Екатеринбург, МВЦ «Екатеринбург-ЭКСПО»

ТЕМА:

УМНОЕ ПРОИЗВОДСТВО

ГЛОБАЛЬНЫЙ ПОДХОД

СТРАНА-ПАРТНЕР: **ЯПОНИЯ**

ОСНОВНЫЕ ТЕМАТИЧЕСКИЕ ТРЕКИ В 2017 ГОДУ:

- «Металлообработка»
- «Автоматизация промышленности. Робототехника»
- «Промышленный интернет»
- «Технологии для энергетики. Энергоэффективность»
- «Машиностроение и производство компонентов»

ОРГАНИЗАТОРЫ:

МИНПРОМТОРГ РОССИИ

ПРАВИТЕЛЬСТВО СВЕРДЛОВСКОЙ ОБЛАСТИ

FORMIKA

ГОРЯЧАЯ ЛИНИЯ ПО ВОПРОСАМ УЧАСТИЯ:

8 800 700 82 31

www.innoprom.com

#ИННОПРОМ2017

Реклама

Чтобы быть современным человеком, мало быть в курсе последних политических, культурных и научных новостей, мало пользоваться всевозможными электронными устройствами и быть активным участником социальных сетей, мало быть одетым по последнему слову моды — нужно еще использовать современную лексику. Например, очень несовременно звучат слова «календарный план» или «график работ». Любой прогрессивный сотрудник знает, что вместо этих архаичных документов нужно составлять и класть начальнику на стол «дорожную карту», причем разрабатывать ее нужно не на «совещании», «собрании» или, упаси боже, «планерке», а исключительно на «стратегической сессии». Если по ходу конференции вы задумали проводить обсуждение какого-либо вопроса, то называйте это не «круглым столом», а непременно «панельной дискуссией» или просто «панелью». «Продвинутые юзеры» вас поймут, а на мнение отставших от жизни «аутсайдеров» и внимания обращать не стоит. «Передовой опыт» давно заменен «лучшими практиками», а новая продукция предприятия на самом деле не должна называться ни «новой», ни «модернизированной», ни даже «высокотехнологичной», а непременно «инновационной». И помните, что «благоприятные условия» на самом деле являются «окном возможностей», в случае открытия которого можно очень своевременно реализовать «вытягивающий проект».

Овладение этой лексикой является хоть и обязательной, но самой простой, первой ступенью в карьере современного человека. Гораздо сложнее вторая ступень, которая состоит в освоении определенного набора специальных терминов, требующих минимального технического понимания. К таким сверхпопулярным сегодня терминам относятся: «3D-принтеры», «дополненная реальность», «когнитивные технологии», «большие данные», «электронное правительство», «кибербезопасность» и т. д. Произносятся они часто, но, похоже, далеко не всегда правильно понимаются даже самими авторами текстов. Тематические статьи настоящего номера помогут читателям разобраться в термине «кибербезопасность» и больше узнать об этой теме. Здесь же я позволю себе несколько не очень строгих и не очень научных рассуждений на эту тему.

Во-первых, что такое кибербезопасность? Кого и от чего она защищает? То, что это очень запутанные вопросы, я понял (не удивляйтесь) на премьере спектакля Большого драматического театра (г. Санкт-Петербург) «Губернатор». Спектакль поставлен по одноименному рассказу Леонида Андреева, в котором главный герой — губернатор провинциального города — сначала руководит расстрелом демонстрации, а потом на протяжении всего произведения обреченно ждет возмездия со стороны террористов. И оно приходит — губернатора все же убивают. При чем здесь кибербезопасность? Напомню, что слово «губернатор» пришло в латынь из греческого, где оно звучит как *kybernetes*, т. е. «рулевой», «управляющий». Таким образом, слова «губернатор» и «кибернетика» исторически однокоренные. Означает ли это, что защита особо важных государственных персон, к которым, безусловно, относятся губернаторы, также является проблемой кибербезопасности? Одинаковы ли принципы защиты киберфизических систем и губернаторов? Все ли здесь сводится только к игре однокоренных слов?

Другой интересный и непростой вопрос: а когда проблема кибербезопасности стала актуальной? Общепринятое мнение — в XXI веке, с появлением Интернета и особенно «Интернета вещей». Однако многие знают средневековую легенду о глиняном человеке — големе, — созданном пражским раввином Лёвом. Предлагаю взглянуть на нее глазами специалиста по кибербезопасности.

Гениальный изобретатель, намного опередивший свое время, раввин Лёв, создал антропоморфную киберфизическую систему — глиняного человека. Главным ноу-хау изобретения являлся программный код, т. е. пергамент с каббалистической надписью. С помощью него голем наделялся искусственным интеллектом, позволявшим ему действовать автономно, выполняя команды своего хозяина. Загрузка программного кода осуществлялась достаточно примитивно — пергаментный свиток просто вкладывался в рот голема. Инструкция по безопасному использованию голема содержала жесткое требование: в шаббат голему работать, естественно, запрещалось. Поэтому вечером каждой пятницы раввин Лёв вынимал заветный пергамент изо рта своего помощника до утра воскресенья. Но однажды он это сделать забыл, что привело к сбою в работе голема, и из помощника человека он превратился в реальную угрозу — начал громить и крушить все вокруг (в те архаичные времена люди еще не придумали систем защиты киберфизических систем от некорректных или несанкционированных воздействий). С большим трудом раввину Лёву удалось выключить «заглючившего» голема. По легенде он запер обездвиженного глиняного великана на чердаке Староновой синагоги. Сегодня гостям Праги гиды обязательно показывают наглухо закрытое чердачное окно, расположенное на тыльной стене Староновой синагоги, и несколько скоб-ступенек, спускающихся от окна, но обрывающихся на довольно большой высоте от земли. Говорят, что это раввин Лёв убрал нижние ступени, чтобы никто не мог залезть на чердак и опять оживить голема. Достаточно примитивное средство защиты от киберугрозы.

Как видите, в очередной раз приходится убедиться в глубокой наивности мысли о том, что мы в XXI веке сталкиваемся с чем-то невиданным и являемся смелыми первопроходцами на пути новых технологий и изобретений. Думаю, если более внимательно изучить исторические документы, то мы найдем в прошлом аналоги и 3D-принтеров, и дополненной реальности, и даже электронного правительства. Поэтому давайте с бóльшим уважением относиться к нашим предшественникам и не считать их «аутсайдерами» или «лузерами» только потому, что у них не было мобильного Интернета.

Главный редактор
Владимир Никифоров

CONTROL ENGINEERING Россия

№ 2 (68) '2017

Главный редактор
Владимир Никифоров | vladimir.nikiforov@fsmedia.ru

Выпускающий редактор
Алина Жилина
alina.zhilina@fsmedia.ru

Новостной редактор
Наталья Новикова

Технические консультанты
Алексей Платунов
Сергей Колюбин
Игорь Гуров
Александр Микеров

Отдел рекламы
Ольга Зайцева | olga.zaytseva@fsmedia.ru
Татьяна Ильиных | tatyana.ilinyh@fsmedia.ru
Ирина Миленина | irina@fsmedia.ru

Дизайн
Игорь Домрачев

Верстка
Дмитрий Никаноров

Отдел подписки
Наталья Виноградова | podpiska@fsmedia.ru

Директор
Екатерина Косарева | Ekaterina.Kosareva@fsmedia.ru

Заместитель директора
Павел Правосудов | pavel@fsmedia.ru

Санкт-Петербург
190121, Санкт-Петербург, Садовая ул., 122
Тел.|факс +7 (812) 438-1538

Москва
105120, Москва,
Нижняя Сыромятническая, д. 10, стр. 4, оф. 218
Тел.|факс: +7 (495) 987-3720

www.controlengrussia.com
www.controleng.ru

Издатель
ООО «Электроникс Паблишинг»
197101, Санкт-Петербург,
Петроградская набережная, д. 34, лит. Б
Тел.|факс +7 (812) 438-1538

Журнал «Control Engineering Россия» зарегистрирован Федеральной службой по надзору в сфере связи и массовых коммуникаций. Свидетельство от 24.05.2013 г. ПИ №СС 77-54248

Учредитель ООО «Электроникс Паблишинг»

Журнал печатается по лицензии издательства CFT Media.

Control Engineering Россия является торговой маркой CFE Media LLC. Все права защищены.

Подписано в печать 31.03.17
Тираж 7000 экз.
Свободная цена

Отпечатано в типографии ООО «МЕДИАКОЛОР»
105187, г. Москва, ул. Вольная, 28

Редакция не несет ответственности за информацию, приведенную в рекламных материалах.
Полное или частичное воспроизведение материалов допускается с разрешения ООО «Электроникс Паблишинг».

8 НОВОСТИ

РЫНОК

16 SCHNEIDER ELECTRIC & SKOLKOVO: ЗАПУСК ЦЕНТРА НИОКР В ОБЛАСТИ ПО

18 В ТРЕНДЕ — ПОЛЕЗНАЯ ИНФОРМАЦИЯ

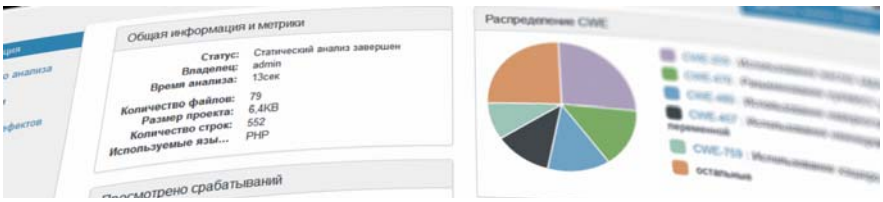
Крис Дартнелл и Марк де Гиран, эксперты компании Schneider Electric, ответили на широкий круг вопросов — от российской специфики развития «Интернета вещей» до ключевых трендов в мире автоматизации.

КИБЕРБЕЗОПАСНОСТЬ

22 КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

В ближайшем будущем рост числа кибератак заставит пользователей систем автоматизации более взвешенно и комплексно подходить к вопросам защиты своих активов от этой категории рисков.

26 APPCHECKER — ИНСТРУМЕНТ СТАТИЧЕСКОГО АНАЛИЗА



30 ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ SCADA В ЭПОХУ «ИНТЕРНЕТА ВЕЩЕЙ»

Системы SCADA изначально не были предназначены для выполнения требований кибербезопасности, поэтому сегодня предприятиям нужно как-то приспосабливаться к новой реальности.

34 CISCO FIREPOWER 2100 — МЕЖСЕТЕВОЙ ЭКРАН СЛЕДУЮЩЕГО ПОКОЛЕНИЯ ДЛЯ ИНТЕРНЕТ-ГРАНИЦЫ

36 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ

Компания Cisco провела опрос специалистов в сфере информационной безопасности, представляющих более 200 российских организаций. Его результаты приведены в данной инфографике.

38 ПРАВИЛЬНО ВЫБРАННАЯ ТЕХНОЛОГИЯ ШИФРОВАНИЯ — КЛЮЧ К БЕЗОПАСНОСТИ

СОДЕРЖАНИЕ

41 **КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ: ЧТО ТАКОЕ DLP-СИСТЕМА И ЗАЧЕМ ОНА НУЖНА БИЗНЕСУ**

АППАРАТНЫЕ СРЕДСТВА

44 **НА ШАГ ВПЕРЕДИ: НОВЫЕ РАЗРАБОТКИ КОМПАНИИ HARTING**

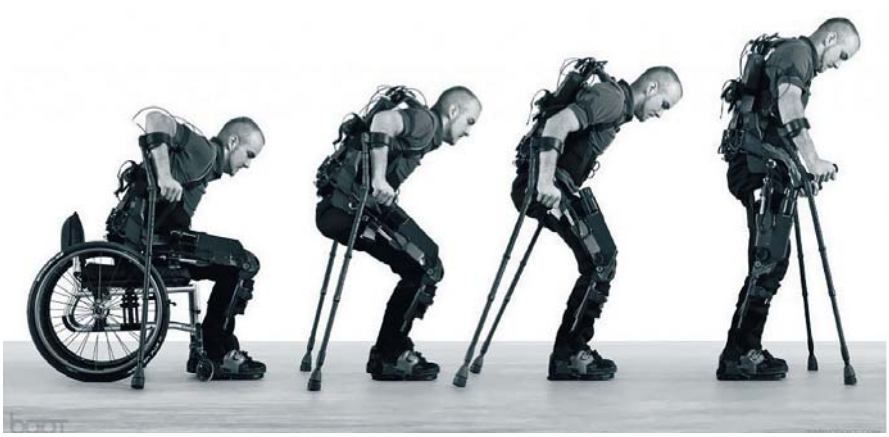
Накануне HANNOVER MESSE компания HARTING Technology Group ознакомила журналистов со своими новыми разработками, которые будут представлены на этой выставке.

47 **ИНТЕРФЕЙСЫ СРЕДСТВ ИНДИКАЦИИ**

50 **СОВРЕМЕННЫЕ МЕТОДЫ КОНТРОЛЯ И ЗАЩИТЫ ЦЕПЕЙ ПИТАНИЯ ОТ ТОКОВ ПЕРЕГРУЗКИ В СИСТЕМАХ АВТОМАТИКИ**

РОБОТОТЕХНИКА

54 **БИОМЕХАТРОНИКА: ШАГИ НАВСТРЕЧУ ЭНЕРГОЭФФЕКТИВНЫМ РОБОТАМ**



58 **РОЛЬ ЭЛЕКТРОННО-КОМПОНЕНТНОЙ БАЗЫ В РОБОТОТЕХНИКЕ**

62 **ИНТЕГРИРОВАННЫЙ СЕРВОПРИВОД ЕМСА**

БЕСПРОВОДНЫЕ ТЕХНОЛОГИИ

66 **ЗАЧЕМ НУЖЕН WI-FI В ТОРГОВОМ ЦЕНТРЕ**

CONTROL ENGINEERING Россия

№ 2 (68) '2017

Chief editor
Vladimir Nikiforov | vladimir.nikiforov@fsmedia.ru

Publishing editor
Alina Zhilina
alina.zhilina@fsmedia.ru

News editor
Natalia Novikova | natalia.novikova@fsmedia.ru

Technical consultors
Aleksey Platunov
Sergey Kolyubin
Igor Gurov
Alexander Mikerov

Advertising Department
Olga Zaytseva | olga.zaytseva@fsmedia.ru
Tatyana Ilinykh | tatyana.ilinyh@fsmedia.ru
Irina Milenina | irina@fsmedia.ru

Design
Igor Domrachev

Page-proofs
Dmitry Nikanorov

Subscription Department
Natalia Vinogradova | podpiska@fsmedia.ru

CEO
Ekaterina Kosareva | ekaterina.kosareva@fsmedia.ru

Deputy Director
Pavel Pravosudov | pavel@fsmedia.ru

Saint Petersburg
190121, St. Petersburg,
Sadovaya str., b.122
t/f: +7 (812) 438-1538

Moscow
105120, Moscow,
Nizhnaya Siromyatnicheskaya str., 10,
b.4, of. 218
t/f: +7 (495) 987-3720

www.controlengineering.ru
www.controleng.ru

Publisher
LLC Electronics Publishing
197101, St. Petersburg,
Petrogradskaya nab., b.34B
t/f: +7 (812) 438-1538

Control Engineering Russia Magazine is registrated by Federal Service on Surveillance in the Sphere of communication media. License # CC 77-54248 from 24.05.2013

Full or part rewriting is allowed after LLC Electronics Publishing permission.

Journal is published by license from CFT Media.

Control Engineering Russia is a trademark of CFE Media LLC.
All rights reserved

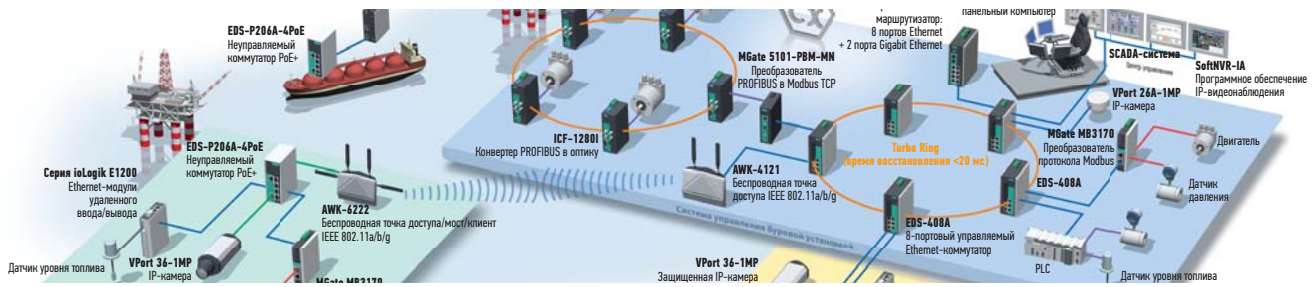
СОДЕРЖАНИЕ

АВТОМАТИЗАЦИЯ НЕФТЕГАЗОВОЙ ОТРАСЛИ

70 **ТРИ ВАЖНЫХ ВОПРОСА НА ПУТИ СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНОГО НЕФТЯНОГО МЕСТОРОЖДЕНИЯ**

Существует возможность повысить эффективность разработки нефтяных месторождений, используя уже существующие сети на устье скважины, — благодаря интеллектуальным системам.

74 **ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ НА НЕФТЯНЫХ МЕСТОРОЖДЕНИЯХ: ПРИМЕРЫ**



80 **СИСТЕМА ДИСПЕТЧЕРИЗАЦИИ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ ТПП «РИТЭК-УРАЛОЙЛ»**

ОТРАСЛЕВЫЕ РЕШЕНИЯ

84 **НПФ «КРУГ»: ОПЫТ АВТОМАТИЗАЦИИ НЕФТЕПАРКОВ И СКЛАДОВ ГСМ**

88 **ATLAS MES — ИННОВАЦИОННАЯ СИСТЕМА ДЛЯ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ**

ИННОВАЦИИ

92 **НОВЫЙ ТРЕНД В БИЗНЕСЕ: «УМНЫЕ КОНТРАКТЫ»**

Smart contracts, или «умные контракты», — актуальная тема в мире бизнеса, которую активно обсуждают последние несколько лет не только в России, но и в мире. Почему этот инструмент появился только сейчас и чем он интересен для энергетики?

94 **«ИНТЕРНЕТ ВЕЩЕЙ» В РОССИЙСКОМ ДОМЕ**

ПРИМЕНЕНИЯ И ПРОЕКТЫ

96 **PID-EXPERT — АВТОМАТИЗАЦИЯ АВТОМАТИЗАЦИИ**

В данной статье речь пойдет об успешном опыте повышения эффективности работы системы автоматического управления на Заводе по стабилизации конденсата им. В. С. Черномырдина (Сургутский ЗСК).

РЕТРОСПЕКТИВА

100 **ВОЙНА ТОКОВ И ПОБЕДА ПЕРЕМЕННОГО ТОКА**

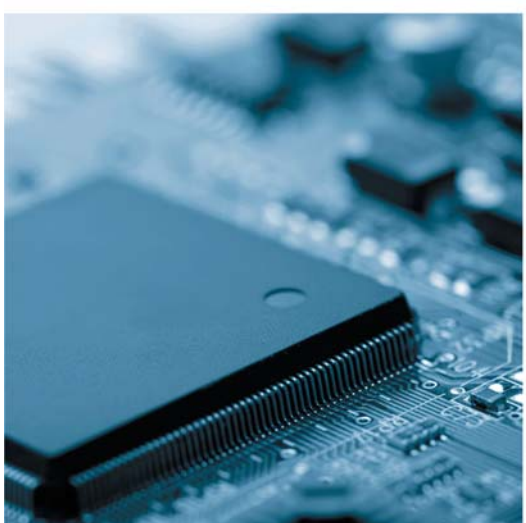
АВИ СОЛЮШНС
точность решает всё

Новое имя – прежние ценности

ВЫСОКОТЕХНОЛОГИЧНЫЕ КОМПОНЕНТЫ И РЕШЕНИЯ ДЛЯ СЛОЖНЫХ ТЕХНИЧЕСКИХ ЗАДАЧ

Источники питания

Электроприводы



Электронные компоненты

Датчики

(812) 702–10–01
sales@avi–solutions.com
www.avi–solutions.com

на рынке
с 1998 года

Реклама

РЕШЕНИЕ POLYCOM REALPRESENCE CENTRO СТАЛО ДОСТУПНО В РОССИИ

Компания Polycom, Inc. объявила о начале продаж системы Polycom RealPresence Centro в России. Это первое в отрасли решение, которое помещает человека в центр совместной работы. Система может успешно применяться в организациях, которые заняты в таких сферах, как реклама, архитектура и промышленный дизайн, финансы, государственное управление, здравоохранение, образование, юриспруденция, промышленное производство, розничная торговля и разработка программных и аппаратных ИТ-решений. В частности, с помощью RealPresence Centro бизнес-тренеры могут удаленно проводить корпоративные тренинги, а руководители проектов — демонстрировать на экранах системы контент, необходимый для общей работы команды.

Решение RealPresence Centro основано на принципиально новой парадигме проведения групповой конференц-связи, когда участники в буквальном смысле помещаются в центр группового взаимодействия. Тем самым обеспечивается органичное вовлечение пользователей в обсуждение и, как следствие, высокая результативность встреч. При создании RealPresence Centro учитывалось присущее людям инстинктивное стремление собираться в круг во время общения. Исследования показали, что физически объединенная в круг команда работает слаженнее и продуктивнее. Решение RealPresence Centro впервые воспроизводит этот опыт так, чтобы все участники видео-конференц-связи чувствовали эффект «погружения» независимо от того, находятся ли они в одной комнате или на другом конце земного шара. Более того, система предвидит потребности пользователей, демонстрируя на экране именно тех людей и те информационные блоки, которые необходимы в конкретный момент времени. Четыре превосходных сенсорных экрана и интуитивно понятный интерфейс RealPresence Centro позволяют подключаться к совещаниям одним касанием и устанавливать решение по принципу Plug and Play.

www.polycom.com.ru

СЕМИНАР «РОБОТИЗАЦИЯ: 1-Й УРОВЕНЬ» В МОСКВЕ

12 апреля 2017 года в Москве пройдет семинар «Роботизация: 1-й уровень». Семинар будет интересен для инженерных организаций, специализирующихся на промышленной автоматизации, которые хотели бы использовать промышленные роботы в своих проектах.

Участники семинара познакомятся с базовыми технологиями интеграции промышленных роботов Kawasaki в современные производственные процессы. Для этого специалисты продемонстрируют, насколько легко начать внедрение робота, и развеют миф о том, что роботы — это сложно.

Участники семинара узнают:

- Как управлять роботом Kawasaki (каждый сможет попробовать управлять роботом).
- Как робот взаимодействует с простейшим дополнительным оборудованием, таким как захваты.
- Основы эффективной и безопасной эксплуатации роботов, требования к их сервисному обслуживанию.

В рамках семинара также состоится круглый стол «Поиск направлений для взаимовыгодного делового сотрудничества».

Ведущие семинара:

- Эиитиро Миядзоэ, глава московского представительства «Кавасаки Хэви Индастриз».
- Игорь Рыженков, директор ООО «Робовизард».
- Роман Тимофеев, менеджер по работе с ключевыми клиентами ООО «Робовизард».
- Алиса Конюховская, вице-президент Национальной ассоциации участников рынка робототехники.

Для участия необходимо пройти регистрацию на сайте: /www.robowizard.ru/blog/seminar-r1l-april-2017

НА САЙТЕ НПФ «КРУГ» ОБНОВЛЕН РАЗДЕЛ «УЧЕТ ЭНЕРГОРЕСУРСОВ»

На сайте НПФ «КРУГ» значительно обновлен раздел технических решений «Учет энергоресурсов».

Откорректированы описания типовых технических решений:

- Интегрированная автоматизированная система комплексного учета энергоресурсов (ИАСКУЭ).
- Автоматизированная система комплексного учета теплоресурсов.
- Автоматизированные системы учета электроэнергии (АИИС ТУЭ/АИИС КУЭ).
- Автоматизированная система диспетчерского контроля и учета энергопотребления электросетевой компании (АСДКУЭ).
- Автоматизированная система коммерческого учета природного газа.
- Автоматизированная система коммерческого учета сжиженного углеводородного газа.
- Системы измерений количества и показателей качества нефти (СИКН).

На сайте доступен для скачивания буклет в формате pdf «Учет энергоресурсов. Технические решения и референс-лист. Системы диспетчеризации и учета ресурсов».

www.krug2000.ru

ФОРУМ-ВЫСТАВКА «ПЕРЕДОВЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ. ПТА — САНКТ-ПЕТЕРБУРГ 2017»

6–8 июня 2017 года для специалистов в области автоматизации раскроет двери юбилейный X специализированный форум-выставка «Передовые Технологии Автоматизации. ПТА — Санкт-Петербург 2017». Место проведения: Санкт-Петербург, конференц-центр «Конгресс»,. Шпалерная ул., 56. Организатор: ООО «ЭКСПОТРОНИКА».

Программа форума посвящена развитию технологий автоматизации зданий и технологических процессов с приходом четвертой промышленной революции и поделена на следующие тематические секции:

- Автоматизация в эпоху «Индустрии 4.0».
- Диспетчерское управление инфраструктурными объектами.
- Практика автоматизации инженерных систем зданий.
- Промышленная автоматизация в проектах и решениях.
- Интеллектуальные системы безопасности.

Слушателей также ждут круглые столы на тему «Интеллектуальное здание будущего», «Импортозамещение в автоматизации: миф или реальность?» и семинары компаний. Одновременно в выставочной зоне форума представят свое оборудование и решения ведущие производители, дистрибьюторы и системные интеграторы в сфере автоматизации.

Форум проходит при поддержке Международного общества автоматизации (ISA), Санкт-Петербургского регионального отделения Союза машиностроителей России, Ассоциации инженеров по вентиляции, отоплению, кондиционированию воздуха, теплоснабжению и строительной теплофизике и других структур.

В 2016 году посетителями мероприятия стали более двухсот руководителей и технических специалистов промышленных предприятий, строительных, управляющих, транспортных и энергетических компаний из России, Белоруссии и Казахстана, включая «Норильский никель», «Ростерминалуголь», «Казахтелеком», «Казатомпром», «Силовые машины», «ГТ-Энерго», «Ростелеком», «ТГК-1», «Газпром нефть».

Подать заявку на участие и получить пригласительный билет можно на сайте www.pta-expo.ru/spb/

MITSUBISHI ELECTRIC СМЕЩАЕТ АКЦЕНТЫ НА РЫНКЕ ПРОМЫШЛЕННОЙ АВТОМАТИКИ В СТОРОНУ E-F@CTORY И КОМПЛЕКСНЫХ РЕШЕНИЙ

Развитие «умных производств» на базе концепции e-F@ctory — краеугольный камень японской стратегии Super Smart Society, или «Общества 5.0», а также акцент на комплексные решения, создаваемые совместно с партнерами, — станут приоритетами компании Mitsubishi Electric в области промышленной автоматизации на 2018 финансовый год. Об этом объявлено 22 марта 2017 года на ежегодной партнерской конференции в Сочи.

Развитие e-F@ctory подразумевает сочетание решений для автоматизации производственных процессов и информационных технологий, возможность практического использования результатов обработки больших массивов данных. За счет интеграции различных сетей связи и промышленного оборудования эта концепция позволяет повысить продуктивность предприятий, предоставить их руководству более наглядный доступ к информации, обеспечить оперативный контроль над процессами и сократить издержки.

В наступающем финансовом году департамент промышленной автоматизации ООО «Мицубиси Электрик (РУС)» расширит работу с флагманскими линейками оборудования: программно-логическими контроллерами, панелями оператора, SCADA-системами, преобразователями частоты, низковольтными комплектными устройствами и промышленными роботами.

www.MitsubishiElectric.ru.

Реклама

SCHNEIDER ELECTRIC СОЗДАСТ В ТАТАРСТАНЕ ЦЕНТР НИОКР ДЛЯ АДАПТАЦИИ И РАЗРАБОТКИ ИННОВАЦИОННЫХ РЕШЕНИЙ ДЛЯ ПРОМЫШЛЕННОСТИ

В 2017 году в высокотехнологичном городе Иннополисе в Республике Татарстан откроется центр НИОКР компании Schneider Electric. Соглашение о намерениях между АО «Шнейдер Электрик» и Особой экономической зоной «Иннополис» было подписано в присутствии Президента Республики Татарстан Рустама Минниханова и заместителя главного исполнительного директора Schneider Electric Эммануэля Бабо.

Новый центр НИОКР будет действовать преимущественно по направлению адаптации и разработки информационно-управляющих систем и специализированного программного обеспечения для нужд нефтегазового комплекса и других отраслей промышленности. Разработки центра позволят клиентам компании повысить операционную эффективность и безопасность производств с помощью локальных решений, учитывающих особенности российских условий эксплуатации. Ведущие нефтяные компании Татарстана проявили интерес к совместной работе. Многие из них долгие годы осуществляют взаимодействие с компанией Schneider Electric.

Во всем мире и в России с большой скоростью развиваются технологии промышленного Интернета, ужесточаются требования к кибербезопасности промышленности, в том числе в области автоматизированных систем управления технологическими процессами (АСУ ТП) и систем противоаварийной защиты. В связи с актуальностью этого направления было принято решение о разработках в сфере кибербезопасности промышленных объектов на базе нового центра НИОКР Schneider Electric в Татарстане. Компания уже ведет переговоры о совместной работе с «Лабораторией Касперского», которая в 2016 году открыла в Иннополисе центр компетенций.

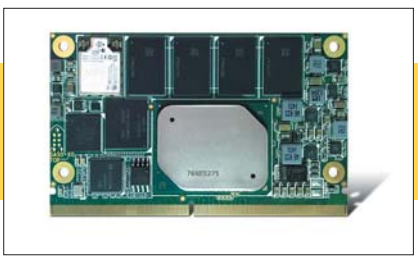
Еще одно перспективное направление исследовательского центра в области решений для нефтегазовой промышленности — создание специализированных линеек контрольно-измерительных приборов, например устройств и систем для измерения извлекаемых углеводородов, в том числе высоковязкой и трудноизвлекаемой нефти.

Планируется, что в центре НИОКР на первом этапе будут работать 10 инженеров Schneider Electric с возможностью в будущем расширять количество рабочих мест. Инвестиции в проект предварительно оцениваются в €1 млн за первые 5 лет. Центр НИОКР войдет в состав международной сети исследовательских центров компании и будет вести разработки не только для России, но и для зарубежных стран.

На встрече делегации Schneider Electric с Президентом Татарстана Рустамом Минниханом также было подписано соглашение с университетом Иннополис о научном и образовательном сотрудничестве.

www.schneider-electric.com/ru

НОВЫЕ SMARC 2.0 МОДУЛИ КОМПАНИИ CONGATEC С ПОДДЕРЖКОЙ USB-C



Компания congatec представила новые модули SMARC 2.0, поддерживающие мощные возможности подключения через USB-C. Проектировщики систем теперь могут использовать возможности USB-C для стандартных периферийных устройств от USB 3.1 до USB 1.0, а также совершенно новый вариант, предназначенный для подключения дисплеев или даже организации питания в системе или к периферийным устройствам, что минимизирует проблемы подключения благодаря применению одного кабеля. Кроме того, текущая пропускная способность в части передачи данных до 5 Гбит/с, в соответствии со спецификацией USB 3.1, служит своеобразным турбоускорителем для приложений, интенсивно использующих данные. Типичными приложениями для конструкций на базе спецификации SMARC 2.0, выполненных на основе процессоров Intel Atom, Celeron или Pentium (кодовое название Apollo Lake), являются карманные компьютеры и другие мобильные устройства, автомобильное встроенное оборудование, а также стационарные встроенные системы «Интернета вещей» (IoT) с низким энергопотреблением и высокими требованиями в части производительности.

Именно такое, уже полностью готовое к применению решение, вобравшее передовой опыт компании congatec по разработке устройств на базе последних возможностей USB-C, представлено в ее новых модулях SMARC 2.0. Устройства оснащены новейшими процессорами Intel Atom, Celeron и Pentium и подходящей платой-носителем с одним полнофункциональным встроенным гнездом USB-C, предназначенным для демонстрации новых возможностей по организации электропитания и интеграции дисплея.

www.congatec.com

ПРОФЕССИОНАЛЬНЫЙ 3D-ПРИНТЕР 3NTPROF ОТ ГК «ТРИНИТИ»

3D-принтер 3ntProf, разработка системного интегратора «Тринити», — оптимальное решение для 3D-печати для небольших рабочих групп инженеров, дизайнеров, архитекторов, а также учебных заведений всех инженерных специальностей.

Профессиональный 3D-принтер — это периферийное устройство, использующее метод послойного создания физического объекта по цифровой 3D-модели. Применение высокоэффективной 32-битной электроники позволяет избежать провала производительности на печати сложной геометрии. А высокоточные шаговые двигатели: (0,9 °/шаг), увеличивают точность воспроизведения в два раза по сравнению с принтерами конкурентов.

Одно из немаловажных преимуществ принтера 3ntProf — отсутствие консольных закреплений, что обеспечивает повышенную прочность конструктива и, следовательно, точность печати. Также, помимо базовой комплектации, пользователь может установить модуль сетевой печати для удаленного управления и обзора записи процесса через камеру.

В следующих версиях продукта планируется разработка системы автоматической смены инструментов: печатные головы с различными материалами, пишущие инструменты, мелкая механическая обработка, лазер-гравер.

www.trinitygroup.ru

УНИВЕРСАЛЬНАЯ ИНТЕЛЛЕКТУАЛЬНАЯ КОНВЕЙЕРНАЯ СИСТЕМА SUPERTRAK ОТ B&R

Компания B&R устроит показ конвейерной технологии на выставке interpack, которая пройдет 4–10 мая в Дюссельдорфе (Германия).

В этом году на стенде B&R (стенд E62, зал № 6) будет продемонстрирована SuperTrak — универсальная интеллектуальная конвейерная система, способная внести ключевой вклад в «Индустрию 4.0». Революция в интеллектуальном производстве обещает компаниям, занятым выпуском товаров повседневного спроса, небывалую эффективность оборудования (OEE) и низкую совокупную стоимость владения (TCO).

SuperTrak — это новое поколение технологии надежного, дружественного конвейера, построенного на базе линейного двигателя с длинным статором. В отличие от аналогичных систем, доступных до сих пор, она обеспечивает подлинную надежность промышленного уровня и простоту обслуживания. Независимые управляемые каретки позволяют изготавливать продукцию в значительных масштабах с высокой степенью индивидуализации, а также минимизировать время, затрачиваемое на переналадку или переоборудование.

Компания B&R также продемонстрирует, как наладить органичную связь открытых стандартов, таких как POWERLINK, OMAC PackML и OPC UA — «кровеносной системы» решений промышленного IoT. Бесшовное взаимодействие от датчика к облаку и между линиями от разных производителей и производственно-технологических коммуникаций приведет к резкому повышению эффективности работы.

www.br-automation.com

СОТРУДНИЧЕСТВО HONEYWELL И SEEQ В ОБЛАСТИ IIOT ДЛЯ РЕАЛИЗАЦИИ ПРОГРАММЫ HONEYWELL CONNECTED PLANT

Корпорация Seeq стала новым участником программы Connected Plant компании Honeywell, в рамках которой возможности промышленного «Интернета вещей» (IIoT) применяются для повышения безопасности, эффективности и надежности операций как на отдельном объекте, так и на нескольких предприятиях. Недавно Honeywell объявила о заключении аналогичных соглашений с компаниями Flowserve, Aereon и рядом других лидеров отрасли. Клиентам, использующим технологии Honeywell UOP, предлагается пакет услуг Connected Performance Services, который предоставляет доступ к экспертным знаниям о технологических процессах UOP в облачной платформе Connected Plant.

Многие аналитики отрасли признали Seeq лидирующей инновационной компанией на рынке средств углубленного анализа производственных процессов. Особенностью решений компании в сфере извлечения ценной информации из технологических данных является их ориентированность на инженеров в отличие от многих других предложений, предназначенных для специалистов по обработке данных.

www.honeywell.ru

Honeywell
TDK
SICK
VISHAY
BOURNS
TE connectivity
Panasonic
JAMICON
MASTECH
MITSUBISHI ELECTRIC
UNI-T
muRata
SOLOMON

Осциллограф регистратор DL850E

YOKOGAWA
Сделано в Японии

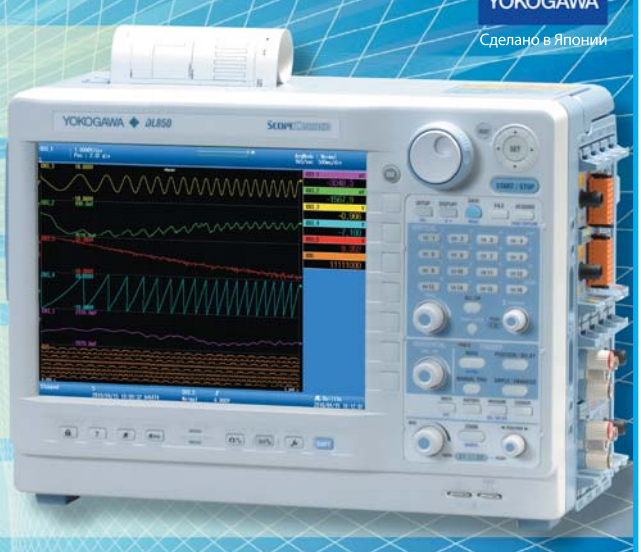
19 сменных модулей для измерения напряжения, тока, датчиков и шины CAN/LIN

Регистрация продолжительностью до 200 суток на встроенный жесткий диск

16 каналов с расширением до 128

Функция двойного захвата с одновременной регистрацией событий при низкой и высокой частоте выборки

Синхронизация и регистрация в режиме вычисления энергопотребления



www.platan.ru
ПЛАТАН

Офисы в Москве: м. Молодежная, ул. Ивана Франко, 40, стр. 2, (495) 97 000 99, info@platan.ru;
м. Электрозаводская, ул. Б. Семеновская , 40, стр. 26, БЦ Агат, (495) 744 70 70, platan@platan.ru
Офис в Санкт-Петербурге: ул. Зверинская, 44, (812) 232 88 36, baltika@platan.spb.ru

Реклама

НПФ «КРУГ» РАЗРАБОТАНА АСУ ТП ГАЗОТУРБИННЫХ УСТАНОВОК ТЭЦ «МАЯК-ЭНЕРГИЯ»

В НПФ «КРУГ» разработана и поставлена заказчику автоматизированная система управления технологическим процессом газотурбинных установок ТЭЦ ООО «Маяк-Энергия». Разработка велась в рамках проекта по строительству ГТУ ТЭЦ бумажной фабрики «Маяк».

Пензенская бумажная фабрика «Маяк» основана в 1850 году и специализируется на производстве и реализации обойных бумаг, картонов для плоских слоев гофрокартона, бумаги, составляющей основу внутреннего слоя бумажно-слоистого пластика.

ГТУ ТЭЦ «Маяк-Энергия» состоит из трех энергоблоков. В состав каждого энергоблока входят:

- газотурбинная установка с номинальной мощностью 7,494 МВт;
- котел-утилизатор с производительностью сухого насыщенного пара 20 т/ч;
- дожимная компрессорная установка мощностью 470 кВт и производительностью 3150 нм^3/ч;
- общестанционное оборудование: блок отключающей арматуры, установка нейтрализации стоков, компрессор сжатого воздуха, вспомогательное оборудование;
- электротехническое оборудование: ГРУ 10 кВ, ГРУ 6 кВ, РУСН 0,4 кВ.

В комплекте поставки имеются шкафы управления котлами-утилизаторами (2 шт.), шкафы управления общестанционным оборудованием (7 шт.), серверный шкаф, шкаф питания, пульты аварийного останова (2 шт.), два АРМ операторов, АРМ инженера, веб-сервер, архивная станция.

АСУ ТП ГТУ ТЭЦ обеспечивает координированное управление оборудованием во всех предполагаемых режимах выработки и отпуска электроэнергии и пара потребителям (пуски, режимы работы на заданных параметрах, переходные режимы, остановы).

НПФ «КРУГ» разработаны техническое задание на АСУ ТП и проектно-сметная документация, выполнена поставка комплекса технических средств и программного обеспечения.

Внедрение АСУ ТП ГТУ ТЭЦ планируется осуществить в два этапа:

- первый этап — автоматизация двух энергоблоков, общестанционного оборудования и электротехнического оборудования;
- второй этап — автоматизация третьего энергоблока.

www.krug2000.ru

МОДУЛЬ НОСИТЕЛЯ МЕЗОНИНОВ DIC551 ОТ FASTWEL — ЗОЛОТОЙ КЛЮЧИК В МИР COMPACTPCI SERIAL

Компания Fastwel выпустила модуль носителя мезонинов DIC551. Новинка позволит разработчикам электронно-вычислительного оборудования легко и быстро создавать собственные модули уровня CompactPCI Serial.

Новинка изготовлена по мезонинной технологии с использованием платы-носителя DIC551 и набора мезонинов MIC100x, которые и определяют функциональные возможности модуля.

Плата-носитель мезонинов DIC551 выполнена в стандарте CompactPCI Serial 3U. В основе платы-носителя — ПЛИС со встроенным приемопередатчиком PCIe x1.

Системным интерфейсом сопряжения с другими модулями системы CompactPCI Serial для DIC551 является PCIe x1. На носитель можно установить две мезонинные платы, обеспечив возможность тыльного или лицевого вывода сигналов с мезонина.

Мезонин представляет собой функционально завершенную плату, имеющую аналоговый или цифровой ввод/вывод. Исполнение мезонина не зависит от используемой системной шины компьютера, общение мезонина с платой-носителем происходит с помощью «простых» последовательных и параллельных каналов связи (SPI, SPORT, UART и др.). Связь «простых» каналов связи и интеграцию в систему стандарта CompactPCI Serial осуществляет плата-носитель.

Проектировщик системы может либо выбрать стандартные мезонины от Fastwel, либо относительно легко и быстро разработать собственный мезонин. При этом производство платы-носителя DIC551 и разработку драйверов носителя для набора операционных систем специалисты Fastwel берут на себя.

www.prosoft.ru

СЕРВИС CLOUD API ОТ CONGATEC ДЛЯ ШЛЮЗОВ IOT И ПОГРАНИЧНЫХ IOT-СЕРВЕРОВ

Новый сервис Cloud AP от компании congatec взаимодействует с локальными интеллектуальными датчиками, обрабатывает и преобразует полученные от них данные, а также выполняет автоматизированные действия на основе механизма локальных правил, снижая трафик до облака IoT и обеспечивая быстрые действия в самой локальной сети. Безопасный двунаправленный обмен данными с любыми подходящими облаками достигается за счет использования упрощенного сетевого протокола MQTT с обеспечением безопасности транспортного уровня TLS. Такие функции делают новый сервис Cloud API подходящей отправной точкой для OEM-производителей, которым необходим доступ к интеллектуальным сенсорным сетям через шлюзы IoT и пограничные IoT-серверы. Типичные области применения данного решения: от промышленного производства и индустриального оборудования до «умных» городов, «умных» объектов, «умных домов», интеллектуальных энергетических сетей, оборудования медицинского «Интернета вещей», в транспортном секторе и для цифровых рекламно-информационных систем.

www.congatec.com

«АПСС-СИБИРЬ 2017» ОБНОВЛЯЕТ ФОРМАТ ДЕЛОВОЙ ПРОГРАММЫ

24 мая в Новосибирске пройдет VII Специализированная конференция «АПСС-Сибирь 2017» (Автоматизация: Проекты. Системы. Средства), в рамках которой будут представлены передовые аппаратные и программные продукты ведущих мировых производителей. Экспозиция и деловая часть мероприятия сформированы в соответствии с ожиданиями и с учетом потребностей предприятий и системных интеграторов Сибирского региона. Участниками конференции станут руководители и ключевые специалисты компаний и организаций, занятых в инфраструктурных, градостроительных, транспортных проектах, а также в сфере производства, энергетики и других отраслях промышленности Сибири.

В этом году мероприятие пройдет под девизом «Будущее начинается сегодня».

В конференц-зоне будут работать три секции, максимально полно отражающие актуальный круг тем в самых востребованных и перспективных направлениях:

- «Промышленная автоматизация: на пути к Industry 4.0».
- «Импортозамещение: от контроллера до облака».
- «Smart City. Технологии и новые возможности».

Свое участие в качестве докладчиков уже подтвердили ведущие разработчики и производители оборудования и программного обеспечения для встраиваемых систем и автоматизации технологических процессов.

Узнать подробнее о мероприятии и зарегистрироваться можно на сайте: www.pta-expo.ru/siberia/.

НОВЫЕ AC/DC-ПРЕОБРАЗОВАТЕЛИ ОТ RECOM МОЩНОСТЬЮ 1 И 2 ВТ ДЛЯ ПРИЛОЖЕНИЙ «УМНЫЙ ДОМ» И «УМНЫЙ ОФИС»

В системах «умного дома» и офиса зачастую используется множество малопотребляющих постоянно включенных проводных узлов, оснащенных датчиками. Для удовлетворения новых требований рынка компания RECOM дополнила серии RAC новыми преобразователями с сертификацией для применений внутри помещений EN60335.

Серии RAC01-G (1 Вт) и RAC02-G (2 Вт) были специально разработаны для систем автоматизации внутри зданий. Модули действуют в широком диапазоне входных напряжений 100–240 В AC и предназначены для использования по всему миру. Стандартные уровни выходных напряжений 5 и 12 В подходят для питания реле, шлюзов и узлов в системах автоматизации. Типичное потребление без нагрузки составляет 180 мВт, диапазон рабочих температур –25…+80 °C. Модули защищены от короткого замыкания, перегрузок по току и размещены в миниатюрном корпусе размером 33,7×22,2×19 мм. Все устройства сертифицированы по стандартам EN60950, EN62368 и имеют трехлетнюю гарантию. Сертификация по стандарту EN55022 класса A (RAC-GA) и класса B (RAC-GB) достигается без применения дополнительных компонентов. Серия RACxx-GA также сертифицирована по стандарту EN60335 для жилых помещений.

www.recom-power.com

В ВЫСТАВКЕ РЗА-2017 ПРИМУТ УЧАСТИЕ ПРЕДСТАВИТЕЛИ ШЕСТНАДЦАТИ ГОСУДАРСТВ

В Международной конференции и выставке «Релейная защита и автоматика энергосистем 2017» планируют принять участие профессионалы по релейной защите и автоматике из 16 государств. В общей сложности на мероприятие заявлено свыше 160 докладов, из которых более четверти — доклады иностранных участников. Об этом на организационном совещании в Министерстве энергетики РФ заявил председатель программного комитета конференции, заместитель директора по управлению режимами ЕЭС АО «СО ЕЭС» Андрей Жуков.

- Время проведения: 25 по 28 апреля 2017 года.
- Место проведения: Санкт-Петербург, КВЦ «Экспофорум».

Мероприятие объединило два традиционных события, имеющих многолетний успешный опыт в сфере РЗА: Международную конференцию «Современные направления развития систем релейной защиты и автоматики энергосистем» и Международную выставку и научно-практическую конференцию «Релейная защита и автоматика энергосистем». В объединенном формате конференция и выставка будут проводиться один раз в три года.

Отличительной чертой выставки в этом году станет экспозиция старых реле и устройств РЗА. Экспонаты, среди которых есть старейшее из электрических реле защиты, применявшихся в энергосистеме Санкт-Петербурга, расскажут участникам о том, как развивалась отечественная релейная техника на протяжении нескольких десятилетий. Таким образом, на выставке специалисты смогут как ознакомиться с новейшими моделями релейных устройств и систем противоаварийной автоматики энергосистем, так и прикоснуться к истории их развития.

Международная конференция и выставка «Релейная защита и автоматика энергосистем 2017» — крупнейшее профессиональное событие в сфере РЗА. Мероприятие пройдет при поддержке Министерства энергетики Российской Федерации и Исследовательского комитета B5 «Релейная защита и автоматика» Международного совета по большим электрическим системам высокого напряжения (CIGRE). Организаторами Международной конференции и выставки «Релейная защита и автоматика энергосистем 2017» стали АО «Системный оператор Единой энергетической системы» (АО «СО ЕЭС»), ПАО «Федеральная Сетевая Компания Единой энергетической системы» (ПАО «ФСК ЕЭС»), ПАО «Федеральная гидрогенерирующая компания «РусГидро» (ПАО «РусГидро»), Российский национальный комитет СИГРЭ (Ассоциация «РНК СИГРЭ») и ОАО «Выставочный павильон «Электрификация».

Подробнее о мероприятии можно узнать на сайте: http://rza-expo.ru/ru/

КОМПАНИЯ ABB ПРИОБРЕТАЕТ B&R

Компания ABB объявила о приобретении компании B&R (Bernecker + Rainer Industrie-Elektronik GmbH) — крупнейшего независимого поставщика, ориентированного на программные решения на базе продуктов и ПО для автоматизации оборудования и производственных процессов во всем мире. B&R, основанная в 1979 году Эрвином Бернекером и Йозефом Райнером, со штаб-квартирой в Эггельсберге (Австрия), насчитывает более 3000 человек, в том числе около 1000 специалистов по НИОКР и прикладных инженеров. Компания работает в 70 странах, обеспечивая продажи более чем на $600 млн (2015–16 гг.) в сегменте рынка машин и оборудования для автоматизации объемом $20 млрд. Слияние компаний создаст комплексное предложение для клиентов, объединив инновационные продукты B&R, ПО и решения для современной автоматизации предприятий с лучшими разработками ABB в области робототехники, автоматизации процессов, оцифровки и электрификации.

B&R – инновационная компания в сфере автоматизации со штаб-квартирой в Австрии и офисами по всему миру. Как мировой лидер в области промышленной автоматизации, данная компания сочетает самые передовые технологии и инжиниринг, чтобы предоставить заказчикам практически во всех отраслях промышленности комплексные решения для автоматизации производства, устройств позиционирования, HMI и интегрированной технологии безопасности. Используя промышленные коммуникационные стандарты fieldbus, такие как POWERLINK и openSAFETY, а также мощную среду разработки программного обеспечения Automation Studio, B&R предопределяет будущее автоматизации.

С этим приобретением компания ABB расширит разработки по промышленной автоматизации, интегрируя инновационные продукты B&R в программируемые логические контроллеры, промышленные ПК и сервомеханизмы, а также в ПО и системы. ABB предоставит своим клиентам уникальное комплексное портфолио по автоматизации с открытой архитектурой. Компания B&R имеет быстрорастущую клиентскую базу по всему миру, насчитывающую более 4000 производителей оборудования, выдающиеся достижения в области программного обеспечения и решений для автоматизации, а также непревзойденную экспертизу в приложениях для клиентов в сегменте автоматизации оборудования и производства.

Обе компании имеют взаимодополняющие портфели. ABB — ведущий поставщик решений для сетей, промышленности, транспорта и инфраструктуры. B&R является ведущим поставщиком решений по автоматизации оборудования для таких отраслей, как производство пластмассы, упаковки, продуктов питания и напитков. Совместное стремление к открытой архитектуре расширяет спектр предложений для заказчиков и предоставляет больше возможностей, упрощая подключение к цифровым технологиям.

Инновации лежат в основе обеих компаний. B&R инвестирует более 10% своей прибыли в исследования и разработки и имеет штат, в котором более 1000 человек работает в исследованиях и разработке приложений. ABB ежегодно тратит 1,5 млрд долл. на НИОКР и насчитывает около 30 тыс. технических специалистов и инженеров. В дальнейшем ABB и B&R продолжат вкладывать значительные средства в исследования и разработки.

Автоматизация оборудования и производственных процессов является ключевым фактором четвертой промышленной революции и IoT. ABB продолжит развивать бизнес-модель B&R, основанную на большом опыте в области разработки новых программных сервисов и решений для сквозной оцифровки. ABB Ability — одному из ведущих предложений в области диджитализации — теперь будет выгодно использовать обширную базу данных, ноу-хау приложений, опыт моделирования программного обеспечения и передовые технические средства B&R.

Штаб-квартира B&R в Эггельсберге (Австрия) станет глобальным центром автоматизации ABB.

www.abb.ru

Создадим будущее вместе

Надежное и инновационное оборудование АББ для нефтегазовой промышленности

www.abb.ru

АЛЕКСЕЙ ПАРШИКОВ:
«Инвестиции в долгосрочную исследовательскую деятельность в России не могут не привести к развитию богатейшего потенциала национальной технической мысли»

SCHNEIDER ELECTRIC & SKOLKOVO: ЗАПУСК ЦЕНТРА НИОКР В ОБЛАСТИ ПО

В конце прошлого года компания Schneider Electric запустила центр НИОКР в области программного обеспечения на территории «Сколково». О задачах центра и направлениях его деятельности, а также преимуществах и нюансах локализации ПО нашему журналу рассказал директор центра НИОКР в «Сколково» Алексей Паршиков.

Какие преимущества дает локализация иностранного ПО в нашей стране?

Безусловно, главное преимущество — это вклад в развитие компетенций российских разработчиков. Отличный пример этого — история самарского завода «Электрощит», который несколько лет назад вошел в состав Schneider Electric. Компания инвестировала средства в модернизацию оборудования, оснащение структурных подразделений инструментами и оргтехникой, а также в реализацию природоохранных мероприятий. Все эти вложения не были бы эффективны без обучения сотрудников, которое проводится непрерывно на протяжении последних трех лет.

Наши инвестиции могут повлиять и на общий рост квалифицированных специалистов в стране. Ведь даже в случае смены работодателя обученный компанией Schneider Electric специалист сможет передать приобретенный опыт новым коллегам, что, несомненно, выгодно для России.

Также необходимо сказать про повышение уровня безопасности. На стратегических объектах может применяться только ПО, прошедшее сертификацию в соответствии с российскими стандартами. Получение сертификации возможно только после анализа исходных кодов ПО. После локализации клиенты Schneider Electric такую возможность получили. Это значит, что в различных отраслях промышленности будет применяться все большее количество современных технологий.

В чем состоит интерес компании Schneider Electric в локализации разработки ПО в России?

За двадцать лет присутствия на российском рынке Schneider Electric инвестировала огромные суммы в локализацию производственных процессов. Сегодня у нашей компании шесть собственных заводов в России и более 10 тыс. сотрудников. Мало кто из западных электротехнических компаний обладает таким уровнем присутствия на российском рынке. А локализация ПО на базе исходного кода — новый значимый шаг для нас в этом направлении.

Какие требования сегодня предъявляет мировой и российский рынок к подобным технологиям? Запросы одинаковы или у нас есть своя специфика?

В отечественном и зарубежном подходах много общего. Но при этом очевидно, что российский рынок предъявляет гораздо более высокие требования к производству ПО, в отличие от западного рынка, которому свойственна консервативность в вопросах импортозамещения.

Отечественные тренды последних лет связаны с потребностью российского рынка в локализации на территории страны иностранных технологий, уже себя зарекомендовавших. Несложно догадаться, что за этим стоит необходимость развивающихся компаний решать собственные бизнес-задачи в разы быстрее, чем несколько лет назад.

В чем особенности локализуемого ПО? Как скоро после внедрения на российских предприятиях оно даст экономический эффект?

Среди особенностей локализуемого ПО нужно отметить функции аналитики и прогнозирования состояния технологического оборудования, а также расчета и контроля выполнения основных показателей эффективности производственного процесса. Применение такого комплексного подхода дает возможность отказаться от покупки многочисленных дорогостоящих программных пакетов для решения конкретных задач.

О прогнозируемом экономическом эффекте на данном этапе говорить сложно, так как ПО является частью целостных решений и проектов. Одно можно сказать с уверенностью: решения в области автоматизации — это обязательное условие конкурентоспособности современных предприятий.

Создаваемый центр НИОКР будет также заниматься адап-

тацией программных продуктов для систем управления солнечными и ветряными электростанциями и систем управления инфраструктурой зарядных станций для электромобилей. Почему выбраны именно эти направления? Для России они кажутся достаточно отдаленной перспективой.

Я бы не стал называть массовое внедрение данных технологий в России отдаленной перспективой. Эти направления выбраны в числе приоритетных далеко не случайно.

Возьмем, к примеру, сегмент возобновляемой электроэнергетики: компания Schneider Electric за прошедший год приняла активное участие в строительстве солнечных электростанций с суммарной установленной мощностью в 100 МВт. У этого рынка есть будущее.

И уже сегодня на улицах Москвы появляются заправочные станции для электромобилей (ЭЗС) производства Schneider Electric. Их установка проходит в рамках реализации, пожалуй, крупнейшего инфраструктурного проекта, предусматривающего расположение 156 ЭЗС в центре города. Таким образом, эти направления, связанные с трендом «зеленых технологий», весьма перспективны. Внедрение программных продуктов для систем управления солнечными и ветряными электростанциями в России уже можно назвать реальностью.

Сможет ли локализация иностранного ПО для промышленности подтолкнуть развитие национальной технической мысли в этом направлении?

Безусловно, сможет — и уже подталкивает. В качестве примера могу привести запуск Schneider Electric совместно с российскими компаниями исследовательских проектов в области кибербезопасности (также на базе «Сколково»).

Наша компания планирует увеличивать объем инвестиций именно в долгосрочную исследовательскую деятельность в России. Это не может не привести к развитию богатейшего потенциала национальной исследовательской мысли.

Как происходит отбор специалистов — разработчиков Центра НИОКР в России? Можно ли провести аналогию с Францией?

Во многом мы действительно заимствовали многолетний опыт наших коллег из центрального R&D-центра во Франции. Но адаптировали существующий подход с учетом тех стратегических задач, которые диктует локальный рынок с присущей ему спецификой. Чтобы попасть в команду разработчиков, кандидатам пришлось пройти многоэтапный отбор, направленный на выявление необходимых поведенческих качеств, знания особенностей технологических процессов заказчиков и языков программирования в комплексе с современными инструментами разработки ПО.

Каким вы видите путь развития НИОКР в России в ближайшей перспективе?

У нас большие планы, связанные с развитием центра. В краткосрочной перспективе это разработка и адаптация ПО в соответствии с российской спецификой, постоянное развитие программных продуктов для локальных систем управления энергоснабжением, систем управления солнечными и ветряными электростанциями, автоматизированной системы предиктивного обнаружения неисправностей, систем управления инфраструктурами электрозаправочных станций, а также систем управления распределенными сетями.

В среднесрочной перспективе мы планируем запуск исследовательской деятельности с привлечением специалистов лучших научно-исследовательских институтов.

Забегая немного вперед, скажу, что мы уже ведем переговоры со штаб-квартирой во Франции о запуске разработок принципиально нового для Schneider Electric программного продукта. Пока я не могу сказать, какого именно, но хочу отметить, что в наших планах — реализовать на базе НИОКР в «Сколково» полный цикл разработки ПО с последующей продажей в тех странах, где компания ведет свой бизнес. ⬣

В ТРЕНДЕ – ПОЛЕЗНАЯ ИНФОРМАЦИЯ

На форуме Connect, прошедшем в Москве в декабре 2016 г., нам удалось пообщаться сразу с двумя ведущими экспертами компании Schneider Electric. Крис Дартнелл, вице-президент по мировым продажам и управлению бизнесом, и Марк де Гиран, вице-президент по продажам и программному обеспечению в европейском регионе, ответили на широкий круг вопросов — от российской специфики развития «Интернета вещей» до ключевых трендов в мире автоматизации.

Как вы считаете, есть ли разница в восприятии концепции IoT зарубежными и российскими производителями?

Марк де Гиран (М. Г.): Нет, никакой разницы нет, потому что основа одна: сейчас есть огромный спрос на соединение технологических устройств в одну сеть, сбор данных, превращение данных в информацию, а информации — в знания. Понятно, что у клиентов разный технологический уровень — и соответствующее понимание, но так обстоит дело в любой стране.

В чем, на ваш взгляд, специфика региона EMEA, Европы и, возможно, России применительно к работе в парадигме «Интернета вещей»? Какие регионы являются более подготовленными?

М. Г.: Я не думаю, что все зависит от географического расположения. Я бы отметил как наиболее важные два вида инициатив: с одной стороны, есть безусловные государственные инициативы, которые диктуются политическими соображениями (как «промышленность будущего» во Франции и «промышленность 4.0» в Германии), — это вопросы модернизации крупной структуры. С этим сейчас сталкиваются все, и понятно, что у России здесь есть своя специфика, связанная в первую очередь с ее размером. Но если брать не государственные, а частные структуры, то для них «Интернет вещей» — это даже не вопрос «надо или не надо», это вопрос их будущего и выживания. В России мы это очень хорошо знаем и видим, хотя бы на примере компаний из горнодобывающего сектора, с которыми у нас давние партнерские отношения. Для этих компаний очень важно — особенно с учетом расстояний между производственными активами — постоянно наблюдать за их работой, оптимизировать ее, убирать «утечки ценности» и таким образом сохранять конкурентоспособность. Потому что сейчас у них появляется много конкурентов — из Австралии, Южной Африки, Латинской Америки.

То есть, с одной стороны, в парадигме «Интернета вещей» присутствуют политические процессы, исходящие от правительства, а с другой, практически везде есть очень серьезное движение со стороны частного бизнеса, который видит в этом возможность сегодня и завтра оставаться конкурентоспособным.

Крис Дартнелл (К. Д.): К разговору о больших расстояниях хотелось бы добавить еще один неочевидный момент. Дело ведь не только в том, чтобы контролировать, как производственные активы работают, но еще и в том, что очень многое в управлении зависит от людей. И в связи с этим могут возникнуть трудности при большой протяженности страны. «Интернет вещей» и облачные технологии позволяют российским предприятиям (и в Африке тоже, например, где много добывающих активов расположено в удаленных областях, куда просто сложно добраться) использовать своих лучших управленцев там, где они могут, не меняя локации, значительно расширять диапазон управления.

В каком направлении будет развиваться «Интернет вещей» в 2017–2018 гг.? И в связи с этим в каких направлениях будет развиваться Schneider Electric?

М. Г.: В первую очередь мы фокусируемся на том, чтобы ценность, полезность разработки становилась быстро доступна клиенту. Именно с этим связана наша инициатива построения соотраслевых решений, включающая в себя и модели промышленных объектов, и дополненную реальность, а также уже существующие курсы подготовки операторов по соединению устройств и по анализу данных для объектов, которые находятся на удаленных территориях или работают в сложных условиях. Наш стратегический подход заключается в том, чтобы клиент мог все это максимально быстро освоить.

К. Д.: Необходимо, чтобы сугубо техническая информация, с которой поставляются наши решения, была понятна и доступна — не только техническим специалистам, но и, например, директору НПЗ или бизнес-лидеру нефтеперерабатывающей компании, чтобы он на основе этой же информации видел то, что нужно ему, общую эффективность работы актива. Этому мы уделяем достаточно много внимания.

Каким вы видите будущее, в котором осуществлены все наши фантазии в области «Интернета вещей»?

К. Д.: В организации будущего тот, кто нужно, получает мгновенный доступ к той информации, которая ему необходима. Каждый человек — от самого верха до самого низа — в зависимости от своей роли получает определенную информацию.

Если переносить эту схему на обычную жизнь, то получится следующее: я могу и буду слушать только ту музыку, которая мне нравится, и читать только те новости, которые мне интересны, а не все на свете новости и не всю мировую музыку.

И, конечно, ничто не остановит ту тенденцию, которую мы видим уже давно: информация должна превращаться в знания, а поскольку они сами по себе ценности не имеют (ценность имеет только то, что делает человек), знания должны превращаться в дальнейшие изобретения и инновации.

М. Г.: Сегодня мы уже фактически начинаем это делать. Например, если взять наше комплексное решение для планирования технологических процессов НПЗ, то мы показываем нашему клиенту, что если он ничего не поменяет в работе оборудования, то перестанет выполнять свои же производственные задачи. Как мы можем помочь? Мы никогда не предлагаем один вариант, всегда несколько: один позволяет быстрее получить одно, второй — другое. Всегда необходимо давать человеку возможность самому понять, какая информация ему нужна.

Возможно ли предложить универсальные решения автоматизации производства «под ключ»?

К. Д.: Тенденция эта не нова. Там, где развивается тенденция на строительство, допустим, промышленных объектов «под ключ», там, конечно, и автоматизация делается «под ключ». С другой стороны, эта тенденция как синусоида — она зависит от разности в циклах строительства и бизнес-циклах. В какой-то момент людям хочется стандартных производственных процессов, чтобы быстро начать производить стандартную продукцию, — идет большой спрос на производство «под ключ». Проходит какое-то время, рынок насыщается и появляется все больше людей, которым нужно дифференцировать свое производство,

поэтому они заказывают уникальные проекты — там «под ключ» уже не получается.

Что происходит с интеграцией операционных, то есть производственных, традиционных, и информационных технологий? Системы управления становятся способны на эволюцию. Сейчас есть машинное обучение, есть технологии, которые позволяют системе после того, как она поработает определенное время, адаптироваться, например, к изменению цепочки поставок или к изменению состава сырья. Система может предсказать, как технологический процесс на это отреагирует, поэтому машинное обучение, предиктивная аналитика — это как раз наше будущее.

М. Г.: К вопросу о мечтах в отношении «Интернета вещей» — наверно, это и есть мечта: аналитика, которая по ходу дела может адаптироваться сама, и система управления, которая может предсказать реакцию техпроцесса на любое изменение среды и предупредить о возможном отказе оборудования; можно сказать, искусственный интеллект.

Какие инновационные технологии Schneider Electric видит наиболее актуальными для российского рынка в ближайшей перспективе?

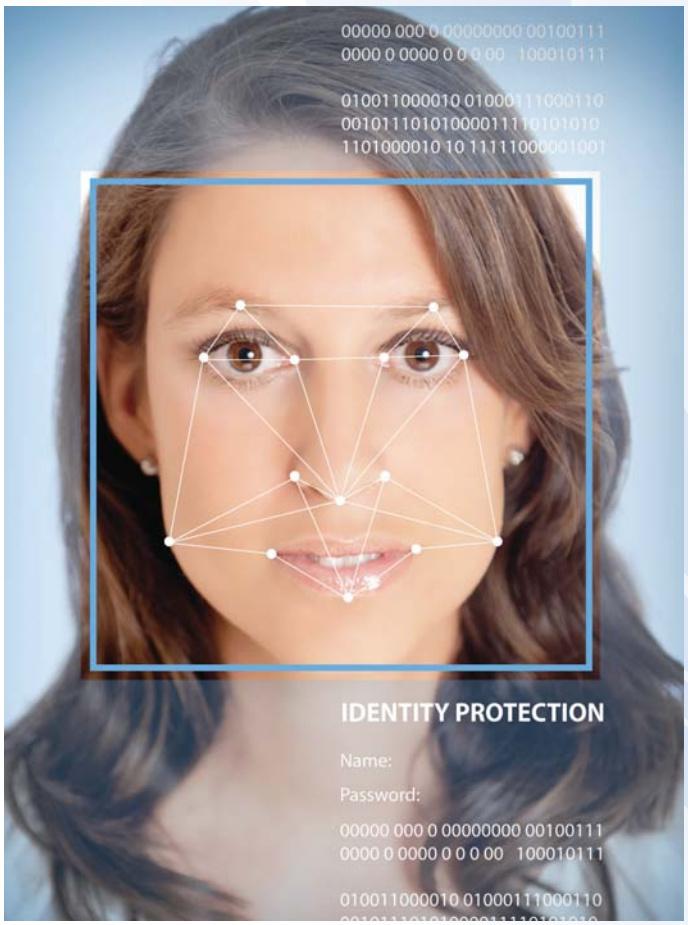
М. Г.: В первую очередь это, конечно, зависит от приоритетов конкретного клиента, но если посмотреть по всей нашей клиентской базе, то я бы сказал, что самое актуальное прямо сейчас — это обработка и корректная интерпретация данных. И в подготовке футбольных стадионов для чемпионата мира по футболу (там много автоматизационных решений), и в базовых отраслях — везде мы видим одно и то же: у людей есть данные, и они хотят, чтобы они были им полезны. Это связано и с географической спецификой России. Важные для компании активы зачастую находятся в сложных, удаленных условиях, и нужно обеспечивать постоянный доступ к данным и аналитику этих данных.

К. Д.: Я приведу один пример. 10–20 лет назад, когда говорили об информатизации производства, речь шла только о постепенном улучшении эффективности производственных процессов внутри периметра завода: чтобы лучше стали работать станок, складская система и т. д. Какие возможности есть сейчас? Например, предвидя, что какой-то технологический процесс потребует остановки, вы можете заранее заказать запчасти, рассчитать расходы, можете перестроить сеть поставок по компании таким образом, чтобы эта остановка ни на что не повлияла.

Обновление версии ПО, миграция, синхронизация, реорганизация и очистка данных в системах и хранилищах промышленных предприятий. Какие программные/аппаратные решения предлагает Schneider Electric для бесшовного осуществления этих процессов?

М. Г.: Я не могу сказать, что у нас всё это обеспечивает какое-то отдельное устройство. АСУ ТП изначально создавалась так, чтобы эти процессы, переходы осуществлялись минимально заметно для людей. Есть другие вендоры АСУ ТП, которые не так параноидально к этому относятся, но мы — именно параноидально, для нас это очень важно.

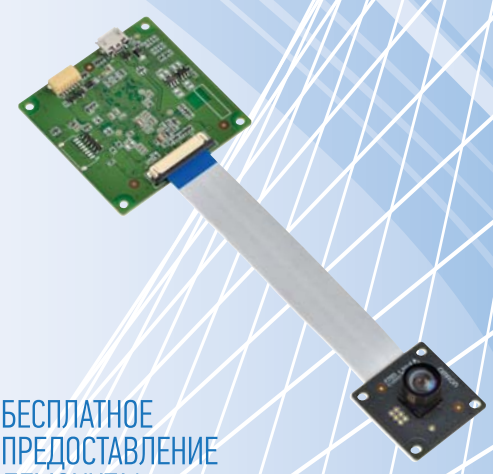
К. Д.: В этом отношении можно посмотреть нашу программную среду «Прометей», в ней заложено все то, о чем мы только что говорили, то есть не только изначально легкое конфигурирование, но и простое подключение к самым разным типам решений и к новым версиям, то есть версионность, миграция данных. ⬣



OMRON

- [ ] Увеличено разрешение камеры до 1600×1200 пикселей
- [ ] Камера вынесена на отдельную плату для большего удобства установки
- [ ] Расстояние распознавания лица увеличено до 3,2 м, расстояние распознавания человеческого тела увеличено до 16,7 м
- [ ] Углы обзора камеры увеличены с 49° (по горизонтали) и 34° (по вертикали) до 54° и 41° у версии B5T-001007-010 до 94° и 76° у версии B5T-001007-020

Обновленный модуль распознавания лиц Human Vision Component (HVC)



БЕСПЛАТНОЕ ПРЕДОСТАВЛЕНИЕ ДЕМОКИТА*

pt ELECTRONICS
Innovations & Technologies

Единый телефон: 8-800-333-63-50
info@ptelectronics.ru
www.ptelectronics.ru

Офисы компании: Санкт-Петербург, Москва, Чебоксары, Нижний Новгород, Екатеринбург, Новосибирск, Ижевск, Таганрог, Пермь, Киев

* – Демокит предоставляется во временное пользование

Реклама

КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

АНДРЕЙ ЧЕРТКОВ
andrei.chertkov@schneider-electric.com

Новый виток развития средств промышленной автоматизации существенно обострил проблему обеспечения кибербезопасности предприятий. В ряде отраслей собственники производств только начинают осознавать значимость этой проблемы и масштаб возможных потерь. Однако эксперты убеждены, что в ближайшем будущем рост числа кибератак заставит пользователей систем автоматизации более взвешенно и комплексно подходить к вопросам защиты своих активов от этой категории рисков.

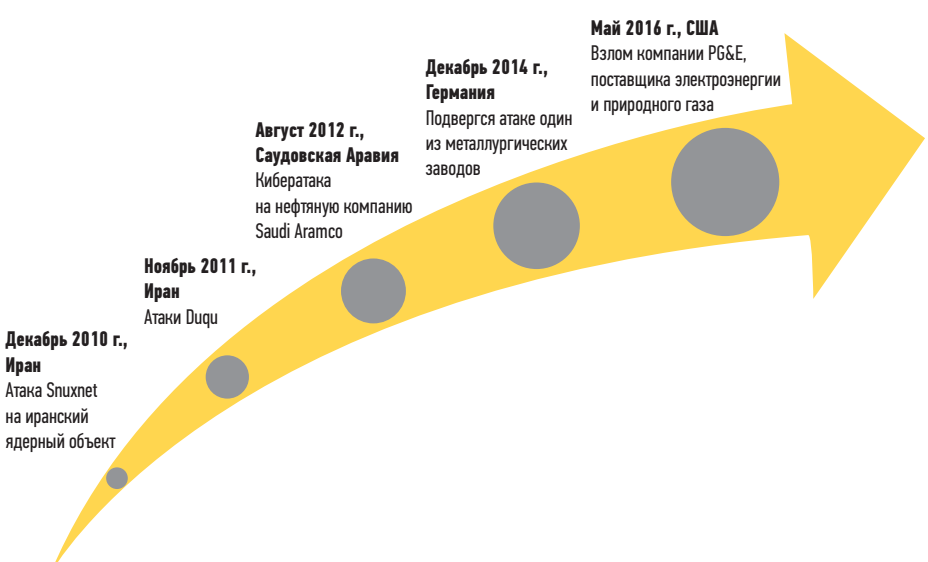
РОСТ УГРОЗ НЕ ВПОЛНЕ ОСОЗНАЕТСЯ

Киберугрозы — явление не новое, но за последнее десятилетие значимость связанных с ними рисков многократно возросла. Дело в том, что раньше автоматизированные системы управления технологическими процессами (АСУ ТП) были физически отделены от локальных вычислительных сетей и Интернета. В современном мире требования к АСУ ТП изменились: они больше не могут оставаться изолированными от внешнего мира. Также важно отметить возрастающую роль решений автоматизации в рамках концепции промышленного «Интернета вещей» (Industrial Internet of Things, IIoT). Эта тенденция заставляет абсолютно по-новому взглянуть на проблему обеспечения кибернетической безопасности в промышленной среде.

Сегодня руководству компаний важно в режиме онлайн контролировать множество показателей технологических процессов, управлять эффективностью производства и обеспечивать коллективную работу через сети, в том числе для территориально удаленных сотрудников. В процессе освоения «Интернета вещей» к промышленным сетям в той или иной мере должны получить доступ третьи компании, к примеру, поставщики оборудования — с целью контроля над его состоянием. Все эти новые возможности АСУ существенно упрощают многие процессы и радикально сказываются на рентабельности, однако при этом создают новые риски для операционной деятельности, связанные с киберугрозами.

Мотивы кибератак многообразны: это получение финансовой выгоды, желание нанести ущерб конкурентам, оказать политическое давление. Порой атаки совершаются по личным мотивам недовольными сотрудниками или подрядчиками. Вне зависимости от причин ущерб от несанкционированного вторжения в АСУ ТП оказывается очень весомым. Это не только внеплановые остановки производства и поломки оборудования, но и серьезные репутационные потери, утечка конфиденциальной информации, угроза жизни и здоровью людей, рост риска аварий и даже техногенных катастроф.

РИС. 1. ▼ Крупнейшие кибератаки на промышленные сети в 2010–2016 гг.



Количество кибератак на промышленные сети неуклонно растет (рис. 1). Так, по данным ICS-CERT (United States Computer Emergency Readiness Team — Американская группа реагирования на чрезвычайные ситуации в киберпространстве), с 2006 по 2012 г. количество киберинцидентов увеличилось на 782%. В 2014 г. было зарегистрировано 245 случаев кибератак на промышленных объектах, а в 2015 г. — уже 295. При этом очевидно, что многие атаки остались вне поля зрения аналитиков. По данным международной консалтинговой корпорации PwC, средний ущерб от инцидента в сфере информационной безопасности в России в 2015 г. составил $5,3 млн, что на 47% выше, чем годом ранее.

Безусловно, все большее распространение киберугроз заставляет собственников промышленных активов искать надежные способы защитить свои сети, а поставщиков решений в сфере АСУ ТП — продумывать комплексные программы минимизации рисков в сфере кибербезопасности.

В отраслях с критически важной инфраструктурой (к примеру, в энергетике, нефтегазовой и атомной промышленности) производства уже

сегодня готовы инвестировать средства в повышение защищенности своих активов. Однако в других отраслях многие пользователи либо не знают о риске кибератак, либо не спешат внедрять на своих предприятиях решения, необходимые для обеспечения безопасности (рис. 2). Ухудшает ситуацию то, что окупаемость инвестиций в кибербезопасность трудно посчитать. В результате многие производственные компании сегодня заняли выжидательную позицию, изменить которую сможет только появление обязательных регулирующих норм или прецедент кибератаки.

ФАКТОРЫ РИСКА

В промышленности объектами киберугроз могут становиться распределенные системы управления (РСУ), программируемые логические контроллеры (ПЛК), системы сбора данных и управления (системы SCADA) и элементы человеко-машинного интерфейса (HMI).

При грамотной оценке ситуации и тесном сотрудничестве с поставщиком решений в области автоматизации большинство уязвимостей, имеющихся в промышленных сетях, реально устранить. Факторы риска вполне можно надежно контролировать, главное, чтобы у персонала промышленного предприятия хватало желания и квалификации, чтобы этим заниматься.

На сегодня один из ключевых факторов уязвимости — общая низкая культура процессов обеспечения кибербезопасности. На многих предприятиях не проводится оценка ключевых рисков и не обеспечивается безопасное управление операциями, включая базовое управление паролями. Отсутствует комплексный аудит, не гарантируется согласованное и эффективное соблюдение политик безопасности, а также недооцениваются доступные инструменты контроля и обнаружения угроз. Даже в современном мире весьма распространенными проблемами остаются недостаточный контроль физического доступа на территорию и халатное отношение к процедурам авторизации и аутентификации при входе в корпоративные и промышленные сети (к примеру, слишком легкие, редко изменяемые пароли).

Программно-аппаратными лазейками для злоумышленников могут становиться незащищенные каналы удаленного доступа, неадекватные межсетевые экраны или неправильно выстроенная архитектура сети, в том числе отсутствие сегментации. Иногда в системах встречаются незащищенные удаленные терминалы, компьютеры, USB-порты, мобильные и периферийные устройства, а также специфические виды устройств человеко-машинного интерфейса.

Постепенный переход к использованию коммерческих ИТ-решений, несомненно, несет коммерческую выгоду и упрощает эксплуатацию и интеграцию систем. Но при этом системы управления оказываются более уязвимыми перед вредоносным программным обеспечением (ПО) и угрозами безопасности, нацеленными именно на коммерческие системы.

Причинами возникновения уязвимостей могут служить разнообразные ошибки «человеческого фактора», в частности неверные действия проектировщика или инсталлятора при конфигурации и установке системы. Негативно сказываются на безопасности неадекватные планы сопровождения и модернизации АСУ ТП, недостаточный уровень квалификации персонала, отвечающего за их внедрение и обслуживание. Производственный сектор гордится высококвалифицированными специалистами по системам автоматизации, однако такая экспертиза в конкретных продуктах и решениях далеко не всегда означает адекватную экспертизу в промышленных ИТ-сетях. Этот пробел ослабляет способность организации разрабатывать всесторонние стратегии защиты и предотвращения угроз.

Порой между ИТ-департаментом и департаментом промышленных систем управления нет достаточного уровня взаимопонимания в силу разных приоритетов. Так, специалисты по АСУ ТП нередко настороженно относятся к внедрению дополнительных мер кибербезопасности. Обновление операционных систем, ПО и средств антивирусной защиты представляется им как потенциальная угроза непрерывности технологического процесса. Справедливости ради заметим, что при неквалифицированном выполнении таких операций угроза может стать вполне реальной.

Серьезным препятствием для повышения уровня кибербезопасности предприятий является и неопределенность в правовом поле, отсутствие требований, закрепленных на законодательном уровне, а также недостаточно развитый уровень стандартизации в сфере защиты от киберугроз.

ПЛАН ЗАЩИТЫ ОТ КИБЕРАТАК

Для предотвращения киберугроз предприятиям необходимо наладить партнерские отношения с поставщиками решений, понимающими специфические характеристики промышленных сетей и уделяющими большое внимание вопросам безопасности. Ответственные

РИС. 2. ▼ Количество кибератак в разных отраслях промышленности в 2016 г., по данным Kaspersky Lab ICS CERT

поставщики средств автоматизации стремятся встраивать средства безопасности во все продукты и сервисы как на стадии разработки, так и на протяжении их жизненного цикла. Такие поставщики помогают заказчикам развернуть многоуровневую систему глубокой защиты средств АСУ ТП, используя для этого комплексный план поэтапного снижения рисков.

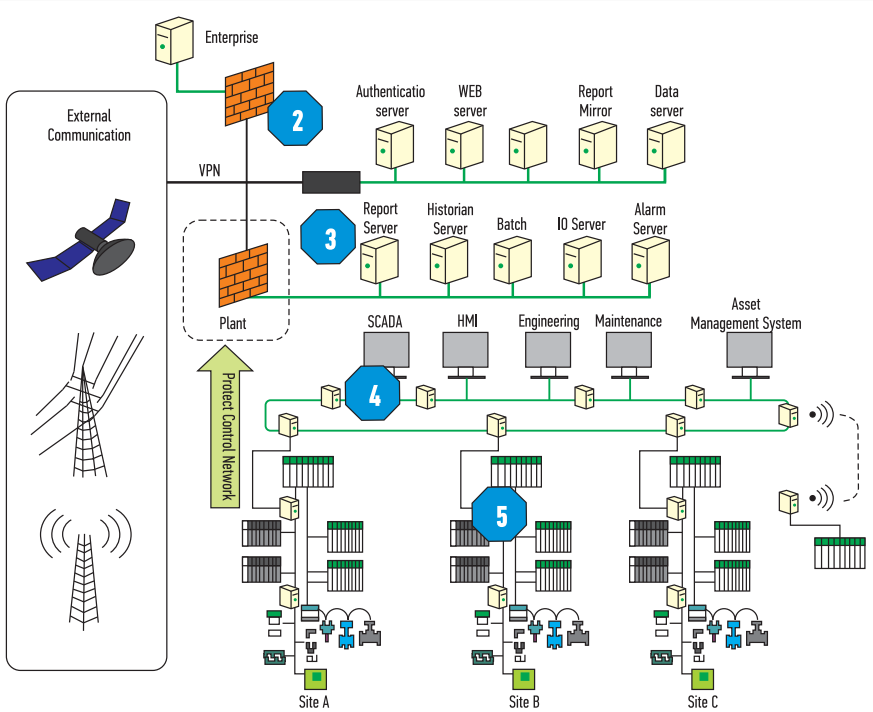
В частности, компания Schneider Electric рекомендует промышленным предприятиям использовать подход Defense-in-Depth. Эта гибридная стратегия многоуровневой защиты реализует комплексный подход к безопасности в масштабе всего промышленного предприятия.

Defense-in-Depth была разработана для оборонных целей Агентством национальной безопасности США, однако впоследствии оказалась применимой и для гражданских отраслей. По мнению ряда экспертов, в будущем данная концепция станет стандартом обеспечения безопасности в промышленной среде.

Подход Defense-in-Depth предполагает шесть ключевых компонентов (рис. 3):

1. Разработка плана по обеспечению безопасности: описание процедур оценки рисков и их минимизации, а также методов аварийного восстановления.
2. Отделение сетей промышленной автоматизации от других сетей путем создания буферных зон, способных защитить промышленную систему от запросов и сообщений из корпоративной сети.
3. Защита периметра от несанкционированного доступа, включающая межсетевые экраны, средства аутентификации, авторизации, VPN (виртуальные частные сети) и антивирусное ПО.
4. Сегментация сети, позволяющая ограничить распространение потенциальной угрозы одним сегментом. Для разделения сети на подсети и ограничения передачи трафика между сегментами используются коммутаторы и VLAN (группа хостов с общим набором требований, которые взаимодействуют между собой независимо от их физического местонахождения).
5. Усиление защиты устройств: управление паролями, определение профилей пользователей и деактивация неиспользуемых сервисов.
6. Регулярный мониторинг и обновление: постоянное наблюдение за активностью операторов и сетевыми коммуникациями, а также своевременное обновление программного и микропрограммного обеспечения.

РИС. 3. ▼ Ключевые компоненты Defense-in-Depth



ПОШАГОВЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Хотя подход Defense-in-Depth приветствует создание и реализацию исчерпывающего плана защиты, будет неверным полагать, что переход к этой концепции осуществляется по принципу «всё или ничего». На самом деле, для достижения быстрых результатов с минимальными затратами клиенты могут придерживаться пошагового подхода. Для этого необходимо следующее:

- идентифицировать пробел в системе обеспечения безопасности, который может привести к наиболее серьезным для предприятия последствиям;
- выявить конкретные производственные зоны, с которыми эти последствия связаны;
- описать наиболее серьезные уязвимости в данной области;
- минимизировать или устранить эти уязвимости.

Обеспечив безопасность наиболее критической зоны, компания может перейти к устранению уязвимостей в другой области. Такой сфокусированный пошаговый подход позволит избежать необходимости менять всю систему сразу и избавит от связанного с этой задачей «аналитического ступора». Он не только гарантирует, что немедленно будут устранены проблемы, ведущие к серьезным последствиям для деятельности предприятия, но и позволит не распылять силы и средства, то есть добиться максимального результата от инвестиций. Тем не менее поэтапная тактика не должна приводить к потере целостной картины.

Также важно помнить, что обеспечение кибернетической безопасности — это процесс, а не единовременное решение. Поэтому неоспоримым преимуществом поставщика средств автоматизации должно быть наличие у него комплексного пакета решений и услуг. Такой пакет может включать:

- услуги по оценке рисков и проектированию систем автоматизации, помогающие клиентам идентифицировать наибольшие риски, определять фокусные области для снижения этих рисков и применять элементы сетевой архитектуры, необходимые для минимизации рисков, связанных с кибернетическими угрозами;

- текущую поддержку по мониторингу, управлению и защите систем автоматизации с целью оперативной изоляции возникающих угроз;
- рекомендации в форме референсных архитектур, помогающие клиентам применять к своим системам подход Defense-in-Depth;
- предложение полного набора средств и инструментов для непосредственного решения задач по обеспечению кибернетической безопасности с учетом перспективы.

Например, в портфеле Schneider Electric есть специальное решение по обеспечению кибернетической безопасности для АСУ ТП — Foxboro Evo, использующее необходимые аппаратные и программные средства для обеспечения защиты на уровне сети управления технологическими процессами и на уровне внешних информационных сетей. Это решение включает в себя применение соответствующих сетевых экранов, проверенных архитектур построения АСУ ТП, встроенную защиту контроллеров от коммуникационных атак, а также комплексный инструментарий для защиты от кибернетических угроз, в который входят следующие компоненты:

- Антивирусное сканирование и обновление файлов антивирусных данных. Это позволяет обнаружить и предотвратить кибератаку и удалить вредоносное ПО, включая системные и компьютерные вирусы и «черви», троянские программы, шпионское и рекламное ПО. Обнаружение и предотвращение угроз на ранней стадии позволяет свести к минимуму возможность повреждения оборудования, входящего в состав системы, и повышает безопасность ведения технологического процесса.
- Подсистема обнаружения несанкционированного вторжения. Эта подсистема отслеживает внешние или внутренние нарушения системной политики безопасности. Она блокирует известные атаки и защищает против несанкционированного просмотра, копирования, изменения и удаления информации и соответствующих системных и сетевых ресурсов и приложений, получающих и хранящих информацию.
- Унифицированная платформа управления безопасностью дает возможность пользователям централизованно отслеживать и управлять работой различных продуктов безопасности.
- Подсистема предотвращения потери данных идентифицирует, отслеживает и защищает конфиденциальные данные (которые находятся в использовании, перемещении, хранении), применяя контекстуальный анализ на предмет безопасности. Также обеспечивается контроль доступа к аппаратным портам, таким как различные типы дисководов, включая CD/DVD или USB-порты рабочих станций системы управления и серверов.
- Сервис администрирования доменных сетей и учетных записей пользователей. Этот сервис производит аутентификацию и авторизацию всех пользователей и компьютеров в доменной сети, а также присваивает и применяет политики безопасности для всех компьютеров и пользователей, производит установку и обновление ПО.
- Процедура повышения «прочности» операционной системы.
- Применение политик «белых» списков используемого ПО для исключения возможности установки и запуска запрещенного, неопознанного или нерекомендуемого к применению ПО.
- Инструментарий для оценки состояния станций и серверов.
- Подсистема резервного хранения и восстановления станций и серверов.
- Подсистема парольной защиты, которая обеспечивает изменение паролей для входа в систему, в том числе на периодической основе, создание индивидуальных паролей пользователей с различным уровнем доступа, блокирование пароля после нескольких неудачных попыток входа в систему, безопасный механизм для сброса пароля и имени пользователя, поддержка в пароле цифро-буквенных и символьных знаков, защита файла с паролями, отслеживание создания, удаления и модификации учетных записей пользователей, отслеживание входа/выхода пользователей и изменений в конфигурации.

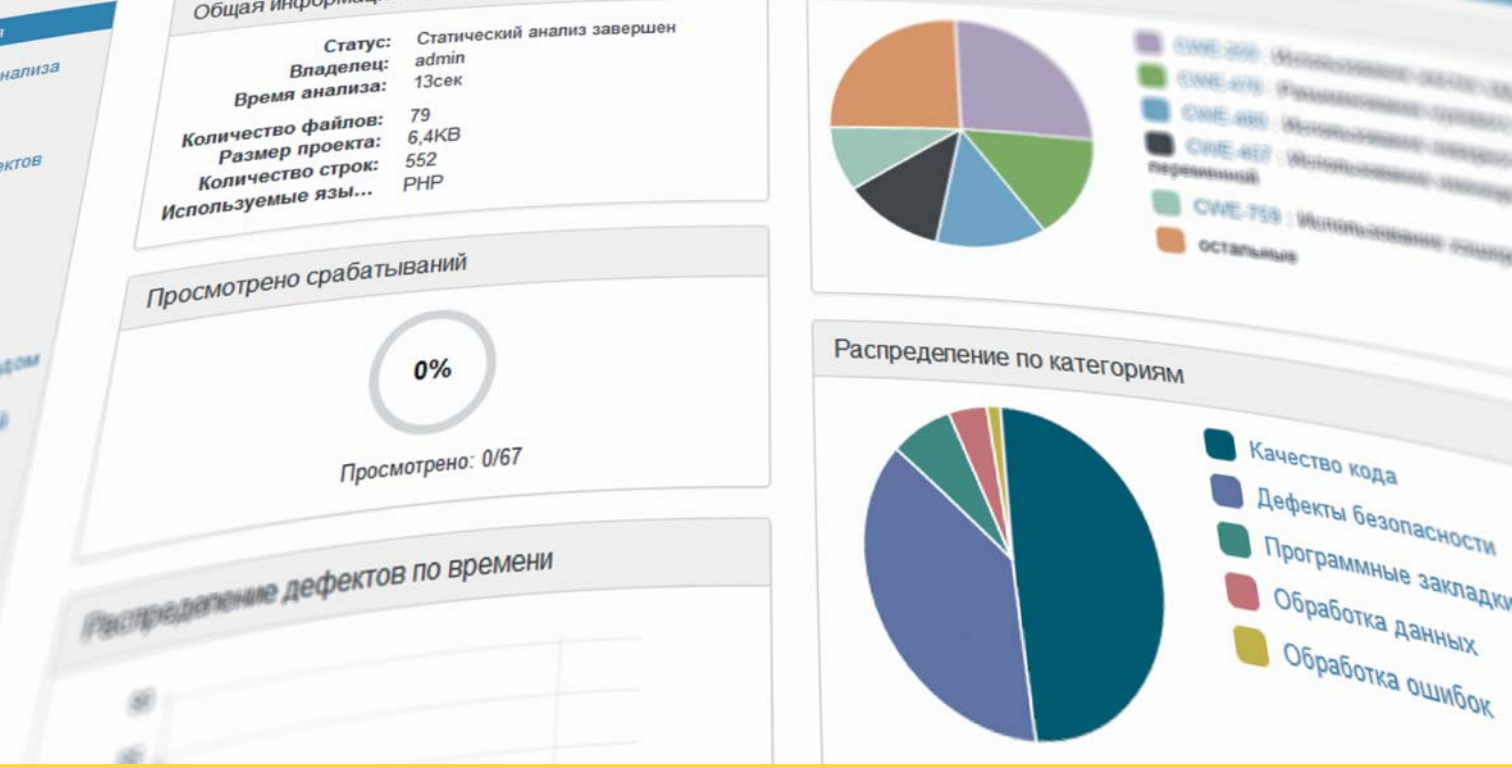
Нужно также принимать во внимание, что кибербезопасность тесно связана с безопасностью предприятия в более широком смысле. Наилучшим вариантом станет сотрудничество с поставщиком, предлагающим не только решения по автоматизации технологических процессов и управлению предприятием, но и системы обеспечения физической безопасности, включая системы контроля доступа, видеонаблюдения, противопожарной защиты. В этом случае план по уменьшению уязвимости предприятия будет цельным и комплексным.

ОБЪЕДИНЕНИЕ УСИЛИЙ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Сегодня большинство промышленных предприятий только начинает осознавать масштаб рисков, связанных с киберугрозами. Тем не менее, по наблюдениям экспертов, уже сегодня видна положительная динамика: компании все чаще задумываются над тем, как защитить свои активы от киберпреступности, которую следует рассматривать в качестве основного препятствия на пути к новому этапу в развитии систем промышленной автоматизации.

Вероятно, в ближайшее время на международном и российском уровне будут разработаны нормативные требования по обеспечению кибернетической безопасности для АСУ ТП. Необходимо выработать единую терминологию, правила сертификации продуктов и стандарты (возможно, таким стандартом мог бы стать IEC 62443 8). В первую очередь они должны коснуться предприятий с критически значимой инфраструктурой.

В любом случае, каждая производственная компания может уже сегодня, не дожидаясь выработки стандартов и законодательных мер, задуматься о собственной защищенности от кибератак. Такой ответственный подход позволит уже сейчас начать пользоваться всеми преимуществами современных открытых АСУ ТП. Со своей стороны, поставщики промышленных систем управления, рассматривающие безопасность как основу своего предложения по автоматизации, станут надежными союзниками в этом вопросе. ●



APPCHECKER — ИНСТРУМЕНТ СТАТИЧЕСКОГО АНАЛИЗА

АНДРЕЙ ФАДИН
a.fadin@npo-echelon.ru
СЕРГЕЙ БОРЗЫХ
s.borzykh@npo-echelon.ru
ПАВЕЛ ГУСЕВ
p.gusev@npo-echelon.ru

В статье рассматривается процесс статического анализа безопасности программного кода с целью выявления его дефектов — ошибок и программных закладок. Приведены примеры таких дефектов и описано программное средство для проведения статического анализа.

ОБЛАСТЬ ПРИМЕНЕНИЯ АНАЛИЗАТОРОВ КОДА

В настоящее время информационные технологии проникли практически во все сферы ведения бизнеса. Для решения бизнес-задач создаются крупные, распределенные, постоянно модифицируемые информационные системы с тенденцией к усложнению. Они могут иметь в своем составе как готовые решения, так и внешние IT-сервисы (SaaS), собственные и заказные разработки, бесплатные продукты с открытым исходным кодом (open source). Проблемы в их работе приводят к нарушению информационной безопасности, а как следствие, к финансовым и репутационным потерям бизнеса. По данным исследования [9], последние четыре года финансовые потери бизнеса растут из-за кибератак. Повышение сложности используемых программных комплексов, их включение в контур систем управления государством и производством промышленной продукции требуют постоянного совершенствования методов тестирования, испытаний и контроля программного обеспечения.

Большинство методов анализа ПО, применяемого в аудите безопасности программных систем, можно разделить на две группы (рис. 1): динамические методы (функциональное тестирование) и статические методы (структурное тестирование).

Динамический анализ представляет собой совокупность всех методов анализа программного обеспечения, реализуемых с помощью программ на реальном или виртуальном процессоре. Такие способы наиболее востребованы при исследовании программ методом «черного ящика» (black box), когда имеется доступ лишь к внешним интерфейсам программного обеспечения без учета их структуры, внутренних интерфейсов и состояния [5]. Этот подход не всегда эффективен при поиске ошибок, связанных с комбинациями редко используемых входных данных, а также при выявлении скрытого программного функционала (программных закладок), внесенного туда преднамеренно.

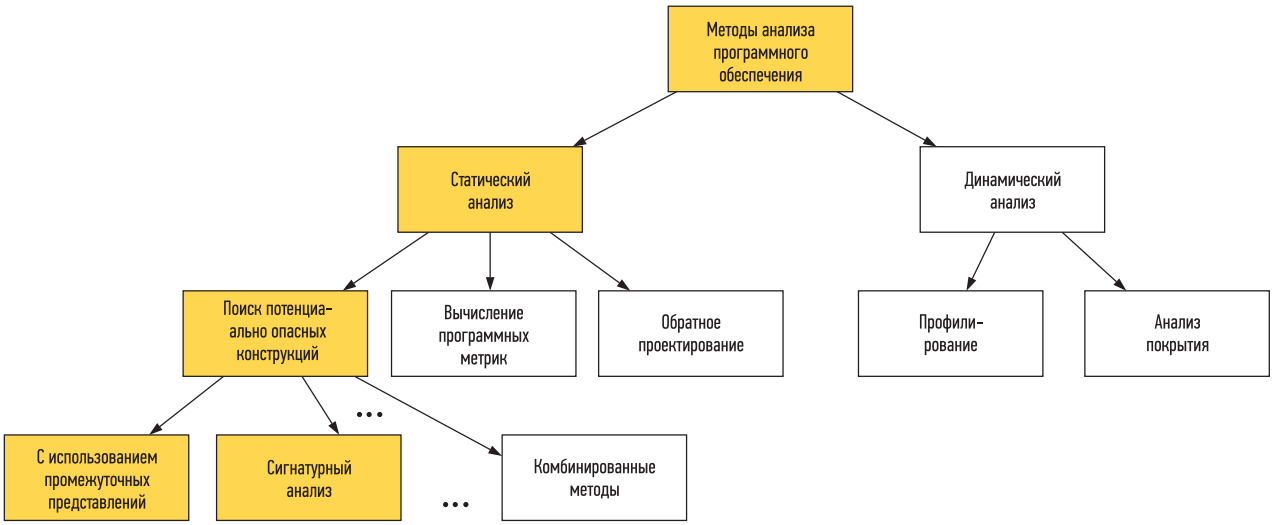


РИС. 1. ▲ Примерная классификация видов анализа программ (цветом выделены те виды анализа, о которых говорится в данной статье)

Для своей работы статический анализ не требует реализации программного кода и допускает полную или частичную автоматизацию процесса, но предполагает доступ не только к загрузочным и объектным модулям, но и к исходным текстам программной системы, к информации, связанной со средой компиляции и выполнением программных компонентов [3–5].

В соответствии с вышеизложенным для одновременного решения задач выявления случайных дефектов кода и программных закладок предлагается использовать методы статического анализа.

МЕТОДЫ СТАТИЧЕСКОГО АНАЛИЗА КОДА

Статический анализ исходных текстов программного обеспечения тесно связан с принципами работы компиляторов. Многие подходы такого анализа основаны на некоторых элементах компиляции, в частности, промежуточное представление исходных текстов в статических анализаторах эволюционирует совместно с развитием теории компиляторов. Современные методы анализа в целях унификации алгоритмов используют различные модели представления кода, например лексический разбор, синтаксическое дерево, дерево Канторовича, графы потока данных и управления и т. д. [1].

Подход, получивший название сигнатурного анализа, подразумевает поиск дефектов в программном коде путем сопоставления фрагментов кода с образцами из базы данных шаблонов (сигнатур) дефектов безопасности. В зависимости от технологии, применяемой при сопоставлении фрагмента кода и шаблона, а также от промежуточного представления, могут использоваться как обычные алгоритмы поиска подстроки в строке, так и регулярные выражения, специальные языки запросов по структурированной информации, в частности XQuery для XML, или специально разработанные для этой задачи способы сопоставления. В [2] приведены примеры правил формирования сигнатур ошибок, соответствующих стандарту CWE. Признакам потенциально опасных конструкций в программных системах и методам оценки их безопасности посвящены статьи 6, 7].

Самый простой способ поиска потенциально опасных конструкций — применение регулярных выражений. Этот вариант достаточно прост в реализации (легко добавляются новые шаблоны уязвимостей), однако имеет несколько критических недостатков. В первую очередь к ним относится невозможность создать шаблоны для сложных дефектов, причем даже для простых дефектов кода регулярное выражение может занимать очень много места, а также очень низкая скорость поиска.

Более эффективным считается построение промежуточного представления кода и его анализ. Именно такой способ используется почти во всех современных анализаторах кода. Общее представление структуры статического анализатора показано на рис. 2.

На начальном этапе решение задачи анализа исходного кода напоминает действия компилятора либо интерпретатора (в случае динамического языка). Исходные тексты разбиваются на лексемы, на основании которых впоследствии строится абстрактное синтаксическое дерево (Abstract syntax tree — AST) и в дальнейшем семантический граф (Abstract semantic graph — ASG). Далее AST

РИС. 2. ▼ Структура статического анализатора

и ASG анализируются механизмом, подобным поиску регулярных выражений в тексте, либо используются скрипты для анализа. Помимо этого, анализ графов выполнения и потоков данных (Data Flow analysis) может дать полезную информацию.

ПРИМЕРЫ ДЕФЕКТОВ КОДА

Самые распространенные виды дефектов кода — ошибки программирования и злонамеренно внесенный код. Следует заметить, что не всякая ошибка программирования приводит к возникновению уязвимости, а только те, в результате эксплуатации которых страдают защищенность, целостность и доступность данных. Злонамеренно внесенный код, как правило, позволяет получить несанкционированный доступ к системе, но бывают и другие типы дефектов, приводящие, например, к удаленному выполнению кода, сбору и отправке конфиденциальной информации либо к реализации несанкционированных действий при наступлении определенного момента времени (time bomb).

К наиболее известным и опасным уязвимостям нужно отнести уязвимости следующих видов:

- отсутствие проверки вводимых данных — может привести к реализации SQL-инъекций, инъекций кода, межсайтового скриптинга, обхода каталогов;
- ошибки работы с памятью — переполнение буфера, необнуленные указатели;
- ошибки реализации системы безопасности — позволяют эксплуатировать давно известные «закрытые» уязвимости.

ОТСУТСТВИЕ ПРОВЕРКИ ВВОДИМЫХ ДАННЫХ

Уязвимость появляется, если не производится проверка данных, поступивших из поля ручного ввода данных; от пользователя ожидается простая информация, например имя, email, текст короткого сообщения. Если при этом в поле ввода дописать код специально сформированной команды SQL или Javascript, то данный код будет выполнен. Например:

```
$name = $_REQUEST['name'];
$res = mysql_query("SELECT *
FROM users WHERE
username ='".$name."'");
```

Если в поле ввода, из которого берется параметр $name, ввести «vasia'; drop table 'users», то таблица users будет удалена, что приведет к потере работоспособности системы. Для предотвращения такого сценария выполнения необходимо использовать безопасный для SQL-инъекции код:

```
$name = $_REQUEST['name'];
$stmt = prepare_query("SELECT *
FROM users WHERE username =?");
$stmt->bind_param($name);
$stmt->execute();
$stmt->bind_result($res);
```

В данном примере каждый параметр передается через отдельный метод bind_param, который и осуществляет фильтрацию специальных символов и ключевых слов.

ОШИБКИ РАБОТЫ С ПАМЯТЬЮ

Чаще всего встречаются ошибки, приводящие к переполнению буфера. Они, как правило, возникают в программах на языках C и C++. Если программа получает данные извне и копирует их во внутренний буфер без проверки размера копируемой области памяти, то при получении достаточно большого объема сведений происходит запись передаваемых данных на место адреса возврата и данных других процедур в области памяти стека. Эта ошибка может быть использована злоумышленником, который подставит нужное значение на место адреса возврата таким образом, чтобы в процессе возврата из подпрограммы переход осуществлялся вовнутрь той же перезаписанной области данных, где можно разместить вредоносный код. Пример уязвимого кода:

```
int main(int argc, char *argv[]) {
    char buf[256];
    strcpy(buf, argv[1]);
    // копирование
    // без проверки длины
}
```

Пример безопасного кода:

```
int main(int argc, char *argv[]) {
    char buf;
    strncpy(buf, argv[1],
sizeof(buf));
// копируется не больше
// размера буфера
}
```

ОШИБКИ РЕАЛИЗАЦИИ

При проектировании и разработке решений для безопасности информационной системы не следует допускать появления в программном коде уязвимостей, которые в дальнейшем могут создать прецеденты нарушения информационной безопасности. К таким уязвимостям относятся:

- хранение паролей в открытом виде, без использования хэш-функций;
- передача данных аутентификации по открытому каналу (HTTP вместо HTTPS);
- отсутствие поддержки CSRF (механизм, предотвращающий XSS-атаки);
- отсутствие проверки качества задаваемых паролей;
- использование устаревших, нестойких криптографических алгоритмов.

ВРЕДОНОСНЫЙ КОД

Один из распространенных примеров вредоносного кода — внедрение разработчиком-злоумышленником возможностей несанкционированного доступа: доступа не только на основании допустимых аутентификационных сведений из базы данных, но и тех данных, о которых знает только разработчик-злоумышленник. Чаще всего к подобной информации относятся пароли-константы, но возможны и пароли, зависящие от даты и времени либо внешних поступающих данных.

Распространены и так называемые логические бомбы, действующие следующим образом: при наступлении определенного момента или при поступлении определенных входных данных программа меняет логику работы на вредоносную.

ЭФФЕКТИВНОСТЬ СТАТИЧЕСКОГО АНАЛИЗА

Сегодня использование статических анализаторов становится объективной потребностью для обеспечения защищенности современных программных систем с высоким уровнем доверия. Введение новых стандартов разработки безопасного ПО подтверждает необходимость эффективных инструментов, поддерживающих качество программного кода.

Использование AppChecker [8] позволяет существенно упростить

и сократить затраты на ревизию кода при разработке программ, а также повысить качество кода и сократить количество ошибок и уязвимостей еще на этапе проектирования, что также позитивно скажется на затратах на доработку и поддержку выпускаемого ПО.

Помимо основного функционала в любом программном обеспечении, взаимодействующем с пользователем, очень важно удобство его применения. Удобный и понятный интерфейс (рис. 3), интеграция в процесс разработки, простота установки, обновления и поддержки становятся важными характеристиками анализаторов кода. Тем не менее сделать анализатор полностью автоматическим, действующим по «нажатию одной кнопки», невозможно.

Как уже упоминалось, работа анализатора во многом близка работе компилятора. И для того чтобы провести качественный анализ, требуются те же действия, которые выполняет система сборки: проанализировать зависимости в проекте, распознать и «подключить» библиотечные функции и т. д., что может потребовать дополнительных настроек процесса анализа. В сравнении с другими статическими анализаторами, AppChecker предоставляет пользователям бóльшую гибкость в настройке: он понятен простым пользователям, а опытные разработчики смогут интегрировать его в процесс сборки любой сложности.

Важной составляющей безопасности кода является применение проверенных сторонних компонентов — библиотек или готовых программ с открытым исходным кодом. Их можно проверить, сообщая авторам о найденных уязвимостях и создавая базу уязвимостей open-source библиотек. Это особенно актуально для поддерживаемых анализатором AppChecker интерпретируемых языков PHP, Javascript, в которых программы хранятся в виде исходных текстов.

ЗАКЛЮЧЕНИЕ

В статье рассмотрен метод статического анализа исходных кодов программного обеспечения, а также основные задачи и проблемы реализации автоматизированной проверки кода на примере статического анализатора AppChecker. Авторы данного продукта разработали эту технологию для удовлетворения потребностей рынка средств управления качеством исходного кода программ. ⬣

ЛИТЕРАТУРА

1. Компиляторы: принципы, технологии и инструментарий / Ахо А. В. [и др.]. М.: ООО «И. Д. Вильямс». 2016. 1184 с.
2. Марков А. С., Фадин А. А. Систематика уязвимостей и дефектов безопасности программных ресурсов // Защита информации. Инсайд. 2013. № 3 (51). С. 56-61.
3. Markov A., Fadin A., Shvets V., Tsirlov V. The experience of comparison of static security code analyzers, International Journal of Advanced Studies. 2015. Т. 5. № 3. С. 55-63.
4. Markov A.S., Fadin A.A., Tsirlov V.L. Multilevel Metamodel for Heuristic Search of Vulnerabilities in the Software Source Code, International Journal of Control Theory and Applications. 2016. Т. 9. № 30. С. 313-320.
5. Аветисян А. И., Белеванцев А. А., Чукляев И. И. Технологии статического и динамического анализа уязвимостей программного обеспечения // Вопросы кибербезопасности. 2014. № 3 (4). С. 20-28.
6. Жидков И. В., Кадушкин И. В. О признаках потенциально опасных событий в информационных системах // Вопросы кибербезопасности. 2014. № 1 (2). С. 40-48.
7. Рибер Г., Малмквист К., Щербаков А. Многоуровневый подход к оценке безопасности программных средств // Вопросы кибербезопасности. 2014. № 1 (2). С. 36-39.
8. Релиз версии 1.5.10 / ООО «Эшелон Инновации». 2015. www.iechelon.ru/version_1-5-10/.
9. 2016 Cyber Crime Study & the Risk of Business Innovation. Ponemon Institute. www.ponemon.org.

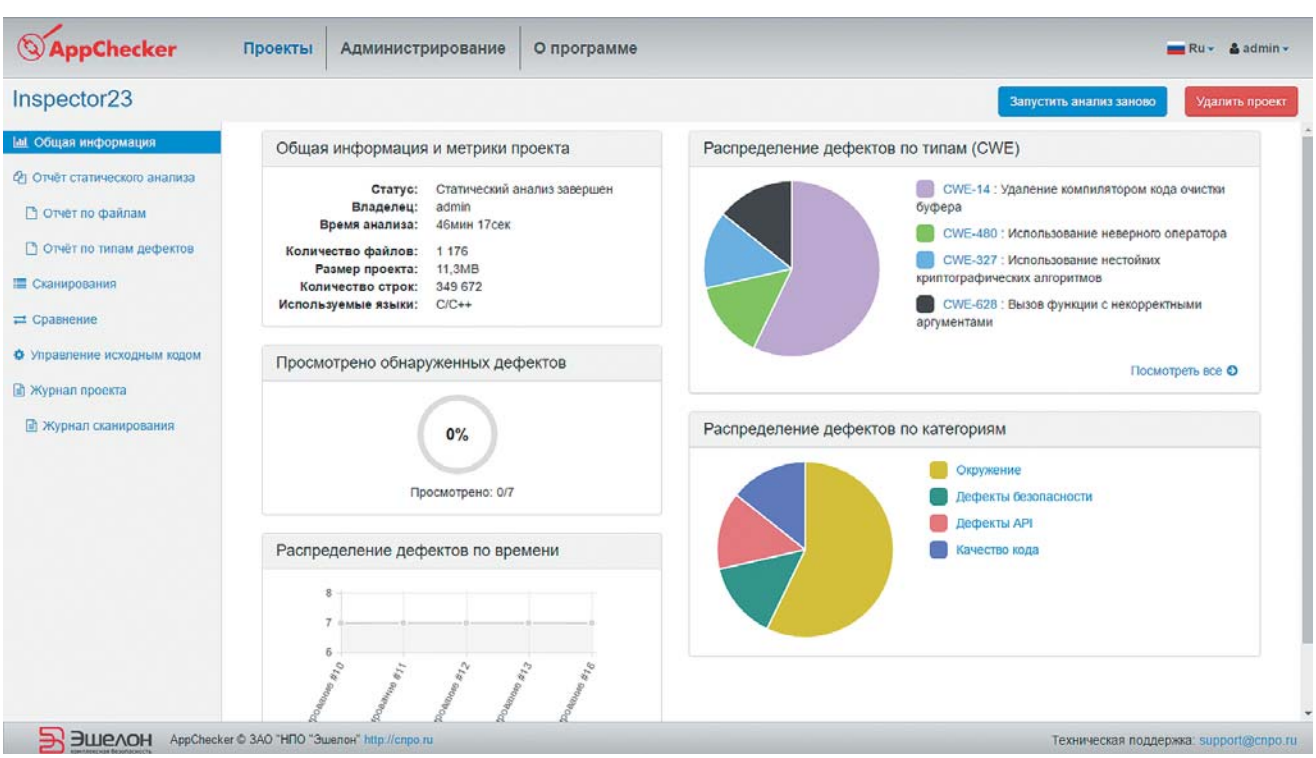


РИС. 3. ▼ Общий вид рабочего экрана AppChecker

ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ SCADA В ЭПОХУ «ИНТЕРНЕТА ВЕЩЕЙ»

ЭД НЬЮДЖЕНТ (ED NUGENT)
МАЙК РЭТТ (MIKE RATTE)

По мере того как индустриальный «Интернет вещей» (Industrial Internet of Things, IIoT) играет все более важную роль, меняется и традиционное использование программного пакета автоматизированной диспетчерской системы управления технологическим процессом — SCADA (Supervisory Control and Data Acquisition). Системы SCADA изначально не были предназначены для выполнения требований кибербезопасности, поэтому сегодня предприятиям нужно как-то приспосабливаться к новой реальности.

SCADA, а также более широкие системы управления производством — ICS (Industrial Control System), которые включают в себя SCADA, человеко-машинные интерфейсы (Human-Machine Interface, HMI), системы управления и обслуживания здания (Building Management System, BMS), системы оперативного управления производством (Manufacturing Execution System, MES), а также компьютеризированные системы управления техническим обслуживанием (Computer Maintenance Management System, CMMS), — решают задачи в области конкретных присущих им технологий, традиционно изолированных от инфраструктуры корпоративных информационных технологий (ИТ). Соответственно, эти платформы изначально не были разработаны с целью обеспечения требований по кибербезопасности.

Сегодня традиционная роль систем управления производством расширилась. Она стала не только включать в себя обеспечение предприятия информацией, в том числе ее обработку, но и отвечать на указания от ERP — системы планирования ресурсов предприятия (Enterprise Resource Planning; подразумевает полное планирование ресурсов, управления и оптимизации, начиная с момента поступления заказа и заканчивая поставкой продукции). Если рассматривать все это в целом, как законченную систему, то мы увидим потенциальные киберугрозы для таких систем, что и было наглядно продемонстрировано в проведенном Центром по защите национальной инфраструктуры анализе «Обеспечение перехода на IP-основе SCADA / PLC сети», который строился на обзоре четырех лучших практических решений сетей SCADA на основе IP-адресов [1]. Сейчас, когда акцент в сфере подключаемых технологий сфокусирован на «Интернете вещей» и тесно связанных с ним индустриальном «Интернете вещей» (IIoT) или «Индустрии 4.0», у производителей есть огромное потенциальное преимущество в стратегии агрегации данных и ситуационной осведомленности. Но поскольку IIoT-устройства используют протоколы Интернета (IP), это увеличивает их подверженность кибератакам.

Все преобразования, связанные с IIoT, изменяют роль традиционной диспетчерской с ее тенденцией к использованию мобильных устройств для контроля и управления [4]. Возникающий при этом в системах управления производством с поддержкой IIoT контекстный компонент человеко-машинного интерфейса обеспечивает повышение производительности для организаций, эксплуатирующих и обслуживающих системы управления производством, при одновременном расширении периметра этих систем. Однако необходимо добавить в систему и элементы защиты от киберугроз.

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Чтобы система менеджмента качества соотвествовала уровню требований ISO 9001 в области разработки

и выпуска продукции, поставщики современных программных платформ систем управления производством включают в них элементы управления кибер-рисками (Cyber Risk) и устойчивостью (Resilience Management), разработанные Software Engineering Institute (Институт программной инженерии Карнеги-Меллон, США). Их цель состоит в том, чтобы обеспечить необходимую прозрачность внутренней или внешней уязвимости и при этом достаточно быстрое реагирование на угрозу для минимизации риска для клиентов.

Участие в процессе обеспечения кибербезопасности таких организаций в области стандартизации, как Институт инженеров электротехники и электроники (IEEE) и Международная электротехническая комиссия (IEC), посредством открытого обсуждения проблем и соответствующей обратной связи, призвано содействовать достижению должной прозрачности. Их деятельность имеет решающее значение для быстрого претворения в жизнь исходящих от них рекомендаций. Так, Национальный институт стандартов и технологий США (NIST) предоставил схему, которая имеет большое значение для систематического определения критически важных активов организации, обеспечения их безопасности и выявления угроз [4]. Эта схема состоит из четырех базовых элементов (рисунок): идентификации, защиты, обнаружения и реагирования.

РАСПОЗНАВАНИЕ И ИДЕНТИФИКАЦИЯ ПОДОЗРИТЕЛЬНОГО ПОВЕДЕНИЯ

Приведем пример: перед Бостонским марафоном 2016 г. Национальная администрация по ядерной безопасности (NNSA) провела оценку фонового излучения по всей дистанции с использованием низколетящих вертолетов. Такие измерения естественного фонового излучения для установки базовых уровней являются нормальной составляющей обеспечения безопасности и готовности к чрезвычайным ситуациям [4].

Поэтому и для определения базового нормального поведения ICS крайне важно заблаговременно провести инвентаризацию активов и потоков данных. Промышленные сети могут быть большими и сложными, а их протоколы отличаются от тех, что применяются в корпоративных ИТ-сетях. Решением вопроса может стать использование автоматизированных инструментов, которые отображают и контролируют сетевое оборудование с помощью простых протоколов управления сетью (SNMP), тем самым повышая эффективность и точность такой инвентаризации.

Важный фактор в создании надежной базовой линии для ICS — это инструменты инвентаризации и мониторинга, которые являются частью системы управления. Вместе с технологией, которая способна обеспечить базовый шаблон связи между ICS, программируемым логическим контроллером (Program Logic Controller, PLC) и другими элементами управления, большое значение имеет мониторинг ICS. При идеальном раскладе такие системы будут способны на:

- извлечение метаданных из сетевого потока с помощью пассивных датчиков;
- быстрое построение визуализированных списка компонентов и карты соединений;
- изучение ICS и выдачу статистических и поведенческих описаний нормального функционирования системы управления;
- выдачу рекомендаций по принятию необходимых превентивных мер;
- инициацию ответа на инцидент при наличии заданного компромисса.

IIoT-устройства часто обмениваются данными с помощью беспроводных технологий, поэтому, в отличие от обычных ИТ-сетей, сети ICS не используют статический IP-адрес. Когда промышленные сети подключаются к еще более обширной сети — Интернету, системы мониторинга работоспособности ищут изменение или дублирование IP- и MAC-адресов, отслеживают перемещение устройств или переключение кабелей, а также несанкционированные подключения. Кроме того, условия эксплуатации сильно усложняются из-за мобильных датчиков, подключенных через точки беспроводного доступа с динамическими IP-соединениями [6].

ЗАЩИТА РАССРЕДОТОЧЕННОГО ПЕРИМЕТРА

На недавнем саммите Tech Talks в Массачусетсе Майк Ратте обсудил с участниками современное состояние ИТ-безопасности [2]. Главная его мысль: «Идентичность — это новый периметр». Он аргументировал это тем, что:

- почти половина нарушений кибербезопасности вызвана именно скомпрометированными полномочиями;
- хакеры нацелены на все классы пользователей, включая привилегированных пользователей;
- традиционная безопасность на основе периметра недостаточна;
- основа безопасности находится в области контекстных политик.

Эта стратегия хорошо сочетается со все большим рассредоточением периметра ICS, который пользуется преимуществами открытой связи, и поэтому ему пойдет на пользу, если им займутся специалисты по безопасности предприятия.

В связи с тем что 63% подтвержденных нарушений данных связаны со слабыми, дефолтными (установленными по умолчанию) или украденными паролями [8], управление учетными данными занимает одно из первых мест в списке киберугроз для ICS. Возможность физического доступа через украденные или потерянные мобильные устройства также обусловливает необходимость в эффективном управлении учетными данными.

Промышленные сети обеспечивают первый уровень защиты с помощью брандмауэров, виртуальных частных сетей (VPN) и коммутаторов. Поставщик платформы ICS должен шифровать конфигурационные

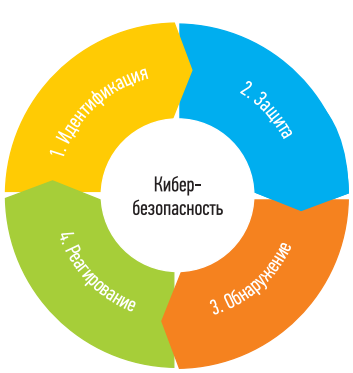


РИС. ◀ Основы кибербезопасности по NIST

файлы, обеспечивать мониторинг необычных попыток подключения, использовать защищенные протоколы, такие как HTTPS, и предоставлять расширенные права пользователя, интегрированные с Microsoft Active Directory. Благодаря этим возможностям платформа ICS может вписаться в мир управления идентификацией как его устойчивая часть. Применяя Active Directory в качестве основного репозитария такого управления, для всех приложений пользователя ICS можно использовать один вход.

В управлении мобильным персоналом краеугольным камнем являются контекстные политики. Права, требующиеся операторам, варьируются в зависимости от их рабочей зоны, а сервер мобильных устройств ICS обеспечивает применение соответствующих жестких контекстных политик, управляя доступом к ресурсам, основанным на географической основе и при этом синхронизируясь с активным каталогом.

Еще один важный момент в решении данной проблемы связан с невозможностью управлять выведенными за рамки системы пользователями и выполнять отключение их учетных записей. Например, у подрядчика, нанятого для работы на объекте, есть возможность иметь временную учетную запись, которая остается открытой и может использоваться в случае, если подрядчику когда-нибудь будет необходимо вернуться на объект. В связи с этим может возникнуть определенная сложность, потому что, когда есть «острова идентичности», трудно распознать, находится ли он (подрядчик) на объекте или вне его. Централизованное управление идентификацией устраняет проблемы с потерянными учетными записями, избавляет от необходимости использования корневых паролей и от упомянутых «островов идентичности». Это значительно упрощает управление и интеграцию учетных данных в соответствии с корпоративными политиками.

ОБНАРУЖЕНИЕ ПОДОЗРИТЕЛЬНОГО ПОВЕДЕНИЯ

С четкой инвентаризацией активов и базовыми шаблонами, отражающими поведение сети и приложений в штатном режиме, система мониторинга промышленной сети будет готова идентифицировать ненормальное состояние системы. Если базовые шаблоны сравниваются в реальном времени с текущим функционированием ICS, то система может генерировать сигналы тревоги и быстро реагировать на угрозу установленного компромиссного поведения.

Существует еще один важный аспект обнаружения ненормальной работы системы, который связан с тенденцией к увеличению мобильности. Управление мобильными устройствами, или MDM (Mobile Device Management), используется предприятиями для развертывания своих политик путем предоставления соответствующих прав своему персоналу. Примером может быть политика отключения камеры устройства на рабочем месте, разрешающая ее включение при выходе за его пределы.

Лучшие в своем классе решения для систем управления обеспечены защитой, позволяющей устройству реагировать на угрозы даже при отключении от сети. Такие системы быстро обнаруживают несанкционированно подключенные и взломанные устройства, а также атаки типа «человек посередине» (тип интернет-атак, при которых злоумышленник перехватывает канал связи, получая полный доступ к передаваемой информации), т. н. состояния тихого взлома и потерянные или украденные устройства и сетевые атаки [9].

МИНИМИЗАЦИЯ УЩЕРБА И ОБЕСПЕЧЕНИЕ ВОССТАНОВЛЕНИЯ СИСТЕМЫ

Для мобильного устройства автоматический ответ на ненормальное поведение включает в себя блокировку или стирание информации устройства, его перезагрузку в безопасное состояние или отключение доступа к сети. Лучшие в своем классе системы также уведомляют о таком инциденте персонал службы безопасности.

При этом крайне важно обеспечить надежное управление в области контроля и сохранения версий программного обеспечения. Это необходимо для того, чтобы после инцидента и его устранения можно было восстановить систему в ранее созданной безопасной контрольной точке. Управление версиями, развернутое на защищенном сервере, помогает поддерживать целостность конфигурации системы и обеспечивает отслеживание любых изменений, внесенных в файлы конфигурации.

К сожалению, восстановление системы до предыдущей версии может, в зависимости от того, где хранятся операционные данные, привести к потере исторических данных. Резервированные контроллеры, сети, исторические серверы и коммуникационные серверы уже давно стали отличительной чертой лучших в своем классе решений SCADA. Этого, однако, недостаточно для предотвращения последствий от киберугроз, которые могут скомпрометировать и первичные, и резервные элементы системы.

Для снижения риска потери данных в системе могут использоваться виртуальные машины, или VM (Virtual Machine), выступающие как хосты ICS. Развертывание на виртуальной машине услуги послеаварийного восстановления в качестве сервиса DRaaS (Disaster Recovery as a Service) позволяет сократить время восстановления системы до 15 минут [7]. Но, поскольку время между вторжением и его обнаружением все равно остается значительным [8], это все еще может привести к потере данных.

На основе всего сказанного можно сделать вывод, что в эпоху «Интернета вещей» самым надежным вариантом защиты от несанкционированного воздействия на системы SCADA и их наилучшей защитой от взломщиков является развитое управление учетными данными. ⬣

ЛИТЕРАТУРА

1. Centre for the Protection of National Infrastructure. Securing the Move to IP-Based SCADA/PLC Networks. London: Centre for the Protection of National Infrastructure. 2011.
2. Centrify Overview and Company Strategy. 2016.
3. National Nuclear Security Administration. NNSA to conduct Aerial Radiation Assessment Survey over Boston area, March 31, 2016 // National Nuclear Security Administration Press Release.
4. Nugent E., Hoske M.T. SCADA cyber security. Control Engineering. July 2015.
5. Nugent E., Bailliencourt P., Kaltenbacher A. The Architecture of the SCADA Mobility Infrastructure. July 28, 2015. www.automation.com.
6. Robles R. J., Kim T.H. Architecture for SCADA with Mobile Remote Components // Proceedings of the 12th WSEAS International Conference on Automatic Control, Modelling and Simulation. 2010. 346.
7. The Always On Enterprise. 2016 // Veeam.
8. Verizon. 2016 Data Breach Investigations Report. 2016.
9. Mobile cybersecurity for remote workforces. 2016 // ViaSat.

Панели оператора для автоматизации тяжеловесного транспорта, сельскохозяйственных машин и других промышленных применений

WINMATE
www.winmate.com

Панели оператора серии G-WIN S65

Удобная система управления и ввод данных с помощью проекционно-ёмкостного экрана P-CAP в элегантном, ударопрочном и виброустойчивом, полностью защищённом от проникновения пыли и влаги корпусе

- Процессор Intel® Celeron® Bay Trail-M N2930 или Freescale® Cortex ® A9 i.MX6 Dual Core
- ОС Windows, Android, Linux
- Проекционно-ёмкостный P-CAP сенсорный экран
- Полностью защищенный от пыли и влаги корпус IP65
- Порты ввода/ вывода M12: USB 2.0, RS-232/422/485, LAN
- Соответствие военному стандарту MIL-STD-810F/G (механический удар, вибрация)
- Широкий диапазон входного напряжения

7”, 1024 x 600, Freescale® Cortex ® A9 i.MX6 Dual Core

10.1”, 1280 x 800, Freescale® Cortex ® A9 i.MX6 Dual Core, Intel® Celeron® Bay Trail-M N2930

12.1”, 1024 x 768, Freescale® Cortex ® A9 i.MX6 Dual Core, Intel® Celeron® Bay Trail-M N2930

15”, 1024 x 768, Freescale® Cortex ® A9 i.MX6 Dual Core, Intel® Celeron® Bay Trail-M N2930

Реклама

pt AIR
Innovations & Technologies

Единый телефон: 8-800-333-63-50
info@pt-air.ru
www.pt-air.ru

Офисы компании: Санкт-Петербург, Москва, Чебоксары, Нижний Новгород, Екаиеринбург, Новосибирск, Ижевск, Таганрог, Пермь, Киев

CISCO FIREPOWER 2100 — МЕЖСЕТЕВОЙ ЭКРАН СЛЕДУЮЩЕГО ПОКОЛЕНИЯ ДЛЯ ИНТЕРНЕТ-ГРАНИЦЫ

МИХАИЛ КАДЕР

Межсетевой экран Cisco Firepower 2100 Series Next-Generation Firewall (NGFW) разработан для предприятий, имеющих дело с большим количеством конфиденциальных транзакций, таких как банки и розничные сети. С его помощью можно обеспечить безотказную работу и защиту критически важных бизнес-функций и данных.

В марте этого года компания Cisco представила новые средства управления информационной безопасностью, упрощающие работу с устройствами, сетью и облаком: Cisco Firepower Device Manager (для управления устройствами), Cisco Firepower Management Center (для централизованного управления информационной безопасностью) и Cisco Defense Orchestrator (для облачного управления).

В связи с переходом к цифровым бизнес-моделям решения кибербезопасности должны поддерживать масштабирование для добавления новых функций и противостояния новым угрозам и уязвимостям без ухудшения производительности сети и приложений. В реальности это, к сожалению, не так. Включение функции обнаружения вторжений на межсетевом экране может привести к снижению пропускной способности как минимум в два раза. Из-за этого существенно страдают такие веб-приложения для взаимодействия с заказчиками, как интернет-банк и электронная коммерция, которым необходима максимальная производительность и которые чаще других становятся мишенью для злоумышленников. Ради повышения производительности некоторые предприятия отключают функционал обеспечения информационной безопасности, подвергая риску как себя, так и своих заказчиков.

НАДЕЖНАЯ ЗАЩИТА И ПРОИЗВОДИТЕЛЬНОСТЬ

В межсетевых экранах от Cisco 2100 серии впервые в отрасли реализована архитектура с двумя многоядерными ЦПУ, которая позволяет повысить скорость ключевых функций — шифрования, экранирования и защиты. Модели этой серии разработаны для удовлетворения потребностей заказчиков в постоянном поддерживании надлежащего уровня безопасности и вместе с тем — производительности, даже при задействованном функционале анализа угроз.

РИС. 1. ▶ Cisco Firepower 2110 и 2120

РИС. 2. ▶ Cisco Firepower 2130 и 2140

В новую линейку Cisco Firepower 2100 Series NGFW входят четыре платформы, ориентированные на отражение угроз (2110, 2120, 2130 и 2140), которые обеспечивают пропускную способность от 1,9 до 8,5 Гбит/с и могут использоваться в различных корпоративных конфигурациях — от границы до облака. Все платформы выполнены в компактном форм-факторе 1RU и характеризуются удвоенной плотностью портов с поддержкой 10 GbE и высокой надежностью, необходимой для поддержания непрерывной работоспособности сети. В моделях 2110 и 2120 (рис. 1) 16 фиксированных портов 1 GbE, а модели 2130 и 2140 (рис. 2) отличаются модульностью: могут иметь до 24 портов 1 GbE и 12 портов 10 GbE. Архитектура всех моделей, основанная на двух многоядерных ЦПУ, позволяет поддерживать стабильную пропускную способность при включении функций защиты, добавлять новые функции и методы защиты, а Fast Path ускоряет передачу потоков, не требующих анализа, тем самым еще больше повышая производительность. Также есть возможность интеграции Cisco Firepower NGIPS и Cisco AMP.

ПРОСТОЕ И ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ

Самые внушительные взломы компьютерных сетей показали, что ахиллесовой пятой защиты от киберугроз становится управление. Как отмечается в ежегодном отчете Cisco по кибербезопасности Cisco 2017

Annual Cybersecurity Report, основные проблемы для подразделений обеспечения информационной безопасности связаны с неправильным конфигурированием и пропуском аварийных сообщений. Для борьбы с этими затруднениями Cisco разработала усовершенствованные средства локального, централизованного и облачного управления, которые помогают заказчикам более рационально выстраивать операционные процессы и экономить средства, одновременно удовлетворяя индивидуальные потребности корпоративных пользователей:

- **Firepower Device Manager**. Веб-интерфейс управления (on-box) с помощью мастеров настройки позволяет разворачивать устройства Cisco Firepower NGFW за несколько минут, управлять стандартными политиками и задачами защиты.
- **Firepower Management Center (FMC)**. Дает возможность простого и полнофункционального администрирования большого количества устройств. В новых моделях масштабируемость управления увеличилась на 50% по сравнению с предыдущими. Для дальнейшего улучшения защиты FMC позволяет автоматизировать задачи обеспечения информационной безопасности, включая оценку, тонкую настройку, корреляцию, локализацию (containment) и ликвидацию последствий. При использовании вместе со стандартизованными FMC технологии Cisco Threat Intelligence Director (TID) можно автоматически загружать и коррелировать результаты анализа угроз, поступающие от заказчиков и третьих фирм, обеспечивая дополнительную защиту на уровне датчиков безопасности в сети (рис. 3).
- **Cloud Defense Orchestrator (CDO).** Простой облачный инструментарий позволяет рационализировать и масштабировать управление политиками безопасности, унифицируя разработку и внедрение политик по всей организации. ⬣

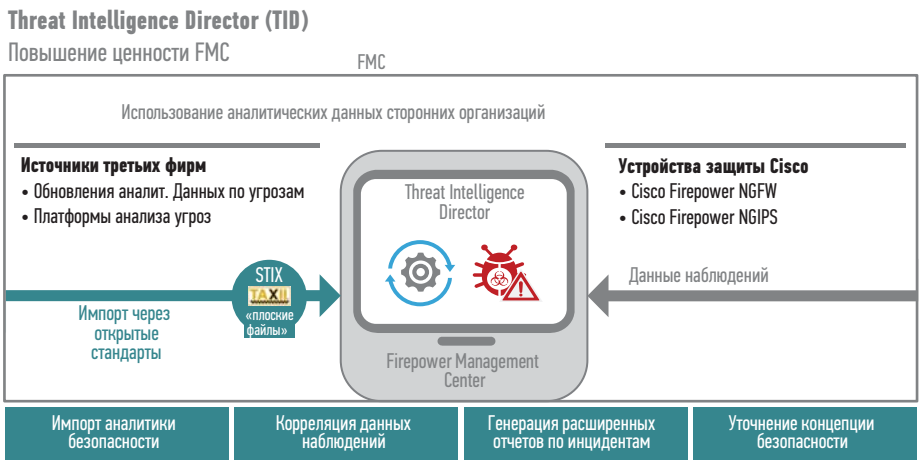


РИС. 3. ▲ Схема работы Threat Intelligence Director

Реклама

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ

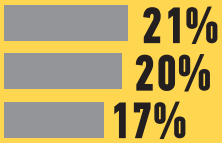
Компания Cisco провела опрос специалистов в сфере информационной безопасности, представляющих более 200 российских организаций. Его результаты приведены в данной инфографике.

57% **российских компаний уже привлекли к себе пристальное внимание в результате взлома систем безопасности**

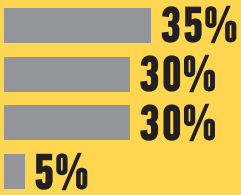
Каждая третья российская компания уже требует от своих поставщиков строго придерживаться рекомендаций по кибербезопасности

Почти половина российских компаний пострадала от простоев длительностью более 5 часов, вызванных нарушениями защиты

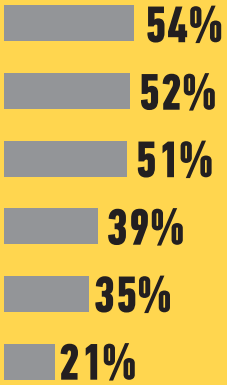
Доля российских компаний, пострадавших в 2016 г. в результате взлома систем безопасности

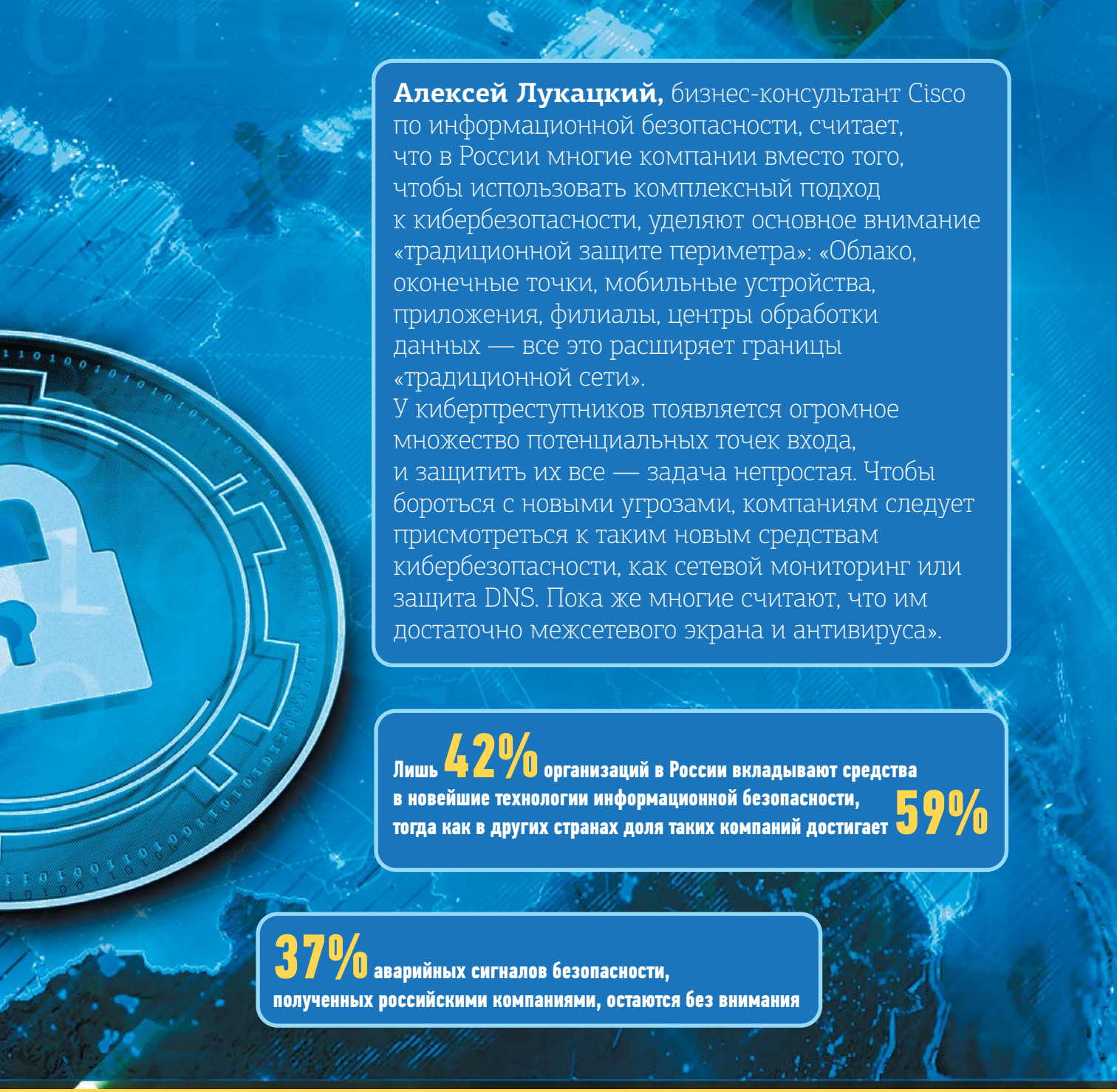


Как российские компании приобретают средства безопасности



Доля российских компаний, использующих различные редства безопасности





Алексей Лукацкий, бизнес-консультант Cisco по информационной безопасности, считает, что в России многие компании вместо того, чтобы использовать комплексный подход к кибербезопасности, уделяют основное внимание «традиционной защите периметра»: «Облако, оконечные точки, мобильные устройства, приложения, филиалы, центры обработки данных — все это расширяет границы «традиционной сети».
У киберпреступников появляется огромное множество потенциальных точек входа, и защитить их все — задача непростая. Чтобы бороться с новыми угрозами, компаниям следует присмотреться к таким новым средствам кибербезопасности, как сетевой мониторинг или защита DNS. Пока же многие считают, что им достаточно межсетевого экрана и антивируса».

Лишь 42% организаций в России вкладывают средства в новейшие технологии информационной безопасности, тогда как в других странах доля таких компаний достигает 59%

37% аварийных сигналов безопасности, полученных российскими компаниями, остаются без внимания

Что же делать?

- Упростить инфраструктуру обеспечения информационной безопасности, пересмотреть принципы закупки и внедрения средств безопасности.
- Повысить эффективность уже имеющихся инструментов.
- Отдать на субподряд функции обеспечения информационной безопасности.
- Изменить модель расходов: например, перенести часть функций в облако.

ПРАВИЛЬНО ВЫБРАННАЯ ТЕХНОЛОГИЯ ШИФРОВАНИЯ — КЛЮЧ К БЕЗОПАСНОСТИ

ЯКОБ ЗЕМАН (JAKOB SEEMANN)

Угрозы, возникающие в результате применения новых технологий, регулярно становятся темой обсуждения в популярных СМИ — будь то кражи автомобилей с Keyless Go[1], скандалы, связанные с незаконным наблюдением, кражи личных данных, взлом паролей в Интернете или фишинг-атаки. Заметим, что наибольший вред во всех подобных случаях наносится не пользователям, хотя для них ущерб, несомненно, есть. Больше всего убытков терпят производители. После того как негативная реклама сделала свое черное дело по отношению к продукту или его производителю, возникает серьезная угроза для всего его бизнеса. Чтобы избежать потерь, связанных с изложенным выше, технологии шифрования предлагают достаточно эффективное с экономической точки зрения решение. Кроме того, при обработке персональных данных, в соответствии с законодательством об их защите, шифрование требуется в любом случае.

Проблемой обеспечения безопасности особенно часто пренебрегают в отношении встраиваемых систем. Как результат, они могут быть взломаны и впоследствии использованы с целью промышленного шпионажа. Преступники получают возможность проникнуть в корпоративную сеть предприятия, осуществить несанкционированный доступ к интеллектуальной собственности компании и ее коммерческим тайнам, а также манипулировать данными предприятия, нанося ему урон через систему управления. Что касается пользователей домашних интеллектуальных устройств, то через взлом автоматизированных систем управления и несанкционированное проникновение в камеры безопасности потенциальным злоумышленникам может стать доступна информация о наличии людей в доме или даже открыты для проникновения в дом двери и окна. Автомобили, благодаря наличию систем автономного вождения и беспроводного обновления встроенного программного обеспечения, тоже подвержены практически неограниченной уязвимости.

Когда перечисленные случаи становятся известны широкой публике, то доверие клиентов к устройству, или даже всему бизнесу, безвозвратно теряется. С учетом этого, шифрование должно быть в верхней части списка приоритетов для всех производителей подключаемого (сетевого) оборудования.

Цель шифрования сосредоточена на трех ключевых направлениях — обеспечение подлинности, конфиденциальности и целостности передаваемой информации. Когда пользователь использует беспроводное подключение для объединения в сеть нескольких продуктов в своем доме, то здесь, например, важно следующее: подключаться к сети должно только авторизованное, а не постороннее оборудование. То есть защиту необходимо реализовать непосредственно на месте, и она должна обеспечивать надежное противостояние всем трем типам угроз — несанкционированному доступу к сети (подлинность), перехвату данных (конфиденциальность) и манипуляции (целостность).

МЕТОДЫ ШИФРОВАНИЯ

Криптография современного технического уровня охватывает все эти три аспекта, при этом она доступна в двух принципиально различных режимах: симметричном и асимметричном шифровании, с одним ключом для шифрования и дешифрования, и двухключевом шифровании с открытым ключом.

Симметричное шифрование

Особенность симметричного шифрования заключается в том, что для шифрования и дешифрования используется один и тот же ключ. Наиболее известным и наиболее часто используемым методом является AES (Advanced Encryption Standard) — симметричный алгоритм блочного шифрования, принятый в качестве стандарта правительством США. В технологии AES размер блока 128 бит, а ключи могут быть 128-, 192- или 256-битные. Даже 128-битные ключи AES, в соответствии с текущим состоянием дел в этой области, классифицируются как безопасные.

При симметричном шифровании, например AES, один и тот же ключ используется на обоих концах (для шифрования и дешифрования). Наибольшая проблема технологии шифрования AES заключается в управлении ключами.

[1] Keyless Go — интеллектуальная электронная система санкционированного доступа к управлению автомобилем, при наличии которой водителю перед посадкой в автомобиль или запуском двигателя нет необходимости держать ключ в руках. Все двери открываются и закрываются автоматически без нажатия на кнопку дистанционного управления. — Прим. перев.

Следует отметить, что в современной криптографии все еще сохраняет свое значение принцип, сформулированный Огюстом Керкгоффсом (Auguste Kerckhoffs) еще в 1883 г. Он гласит, что безопасность метода шифрования основана на секретности ключа, а не на секретности используемого алгоритма. Это особенно важно в отношении такого метода симметричного шифрования, как AES, так как в этой технологии один и тот же ключ используется на обоих концах (для шифрования и дешифрования). Если ключ известен, или он раскрывается, то весь процесс шифрования обнуляется. Следовательно, наибольшая проблема технологии шифрования AES заключается в управлении ключами. При этом должны быть обеспечены: генерация ключей с использованием генератора истинных случайных чисел, а не псевдослучайной последовательности; хранение ключей в защищенном элементе системы шифрования; невозможность перехвата ключей непосредственно во время их передачи.

Асимметричное шифрование

Асимметричное шифрование всегда использует два разных ключа — закрытый и открытый. При этом они всегда генерируются в виде связанной пары. Закрытый ключ всегда остается у его отправителя, в то время как открытый ключ передается по незащищенному каналу принимающей стороне. Открытый ключ может использоваться для шифрования сообщений, которые могут быть расшифрованы только с помощью связанного с ним закрытого ключа. Закрытый ключ может генерировать электронную подпись, с помощью которой получатель получает возможность однозначно идентифицировать отправителя с помощью связанного открытого ключа.

При асимметричном шифровании используются два разных ключа — закрытый и открытый. Асимметричные методы являются практически целесообразными только для обработки небольших объемов данных.

Асимметричное шифрование основано на идее использования односторонних математических функций. Они должны быть как можно более простыми для расчета, но для них очень сложно выполнить обратное вычисление. Поскольку постоянное повышение вычислительной мощности улучшает способность компьютеров в части вычисления сложных реверсивных функций, то для обеспечения надлежащей безопасности ключи должны быть соответствующей длины. В настоящее время как безопасные классифицируются ключи на 2048 бит, такие как RSA 2048. Поскольку, по мере увеличения длины ключа, скорости шифрования и дешифрования уменьшаются, то асимметричные методы являются практически целесообразными только для обработки небольших объемов данных.

Эллиптическая криптография

Альтернативой для традиционного асимметричного шифрования является эллиптическая криптография, основанная на методе эллиптических кривых над конечными полями (Elliptic Curve Cryptography, ECC). Данный метод реализуется на том же подходе, что и асимметричная технология, но использует для шифрования точки на эллиптических кривых. Это делает вычислительные операции гораздо более сложными, таким образом, в соответствии с текущим уровнем техники, безопасный уровень достигается даже при использовании 256-битных ключей. Технология шифрования ECC с 256 точками уже не требует значительного увеличения затрат времени на выполнение операций по сравнению с относительно безопасными симметричными методами шифрования.

Гибридная технология

Если выбирается симметричное шифрование пользовательских данных, но при этом не достигнут требуемый уровень безопасности, технология может быть улучшена с помощью гибридного шифрования. В этом случае симметричный ключ отправляется в зашифрованном виде с помощью асимметричного открытого ключа. Это означает, что только авторизованный получатель с соответствующим закрытым ключом может принять и расшифровать переданный симметричный ключ. В то же самое время отправитель симметричного ключа использует свой закрытый ключ для создания электронной подписи, которая позволяет получателю, используя соответствующий открытый ключ, однозначно его идентифицировать. Основа для организации симметрично зашифрованного канала связи будет заложена только после того, как произошел обмен этими ключами и они были расшифрованы.

Эллиптическая технология реализуется на том же подходе, что и асимметричная, но здесь для шифрования используются точки на эллиптических кривых. Эллиптическая криптография обеспечивает повышение скорости шифрования.

Этот комбинированный способ устраняет недостатки двух отдельных методов, а именно: небезопасная передача ключа для симметричного шифрования и малая скорость, присущая асимметричной технологии шифрования.

ШИФРОВАНИЕ: АППАРАТНОЕ ИЛИ ПРОГРАММНОЕ?

Каждый метод шифрования может быть реализован с помощью программного обеспечения или аппаратно. Шифрование на основе программного обеспечения имеет существенный недостаток: программа не является автономной и самодостаточной составляющей, она всегда зависит от своего окружения, такого как, например, операционная система. В результате она чувствительна к ошибкам, сбоям и атакам. Здесь есть и еще один отрицательный момент: если микроконтроллер или процессор встроенной системы должен дополнительно обрабатывать сложное шифрование и дешифрование, то при этом неизбежна потеря производительности.

При гибридном шифровании симметричный ключ отправляется в зашифрованном виде с помощью асимметричного открытого ключа. Этот комбинированный метод устраняет недостатки двух отдельных технологий — симметричной (небезопасная передача ключа) и асимметричной (малая скорость).

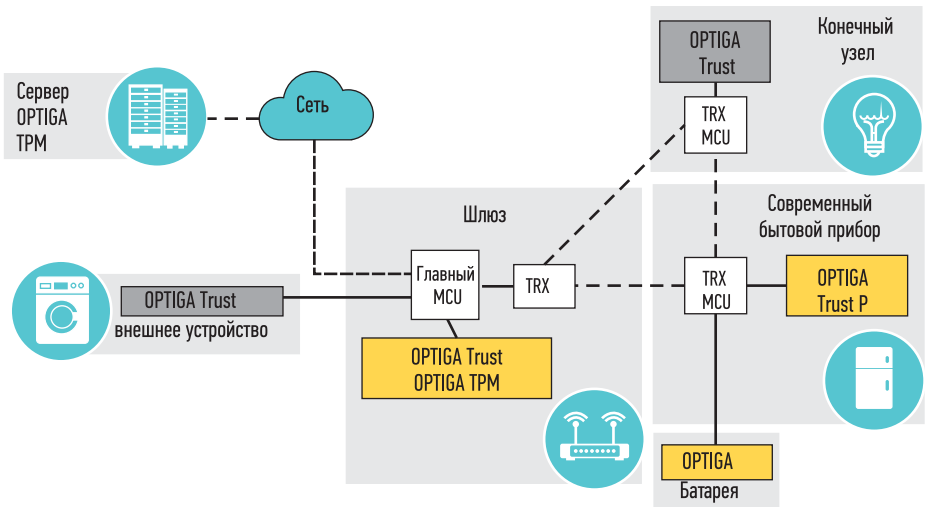


РИС. Различные методы аппаратного шифрования позволяют создать безопасный во всех отношениях «умный дом»

Альтернативой является шифрование с использованием специально разработанных микросхем. Поскольку их единственная и основная функция — это операции, связанные с шифрованием, то в системе нет потери в производительности. Многие микросхемы шифрования дополнительно защищены еще и от физических атак. Таким образом, безопасность этих компонентов, а следовательно, и ключей, не зависит от безопасности системы в целом.

В настоящее время имеется целый ряд различных решений в виде микросхем для шифрования, которые отвечают требованиям целого ряда приложений. Это и простые чипы аутентификации, такие как микросхемы серии Infineon Optiga Trust, которые используются для асимметричного шифрования (ECC 163). И микросхемы, которые являются хорошим выбором для аутентификации оригинальных аксессуаров из области потребительской электроники, такие как, например, серия микросхем Optiga Trust E с ECC 256 и SHA 256, которые обеспечивают аутентификацию медицинского оборудования. Они также используются в системах безопасности «умных домов», в промышленности и в технологии облачных вычислений для аутентификации и управления лицензиями. Серия микросхем Optiga Trust P с ECC 521 и RSA 2048 оснащена операционной системой на базе Java, в которой могут быть запрограммированы выделенные апплеты (прикладные миниприограммы). Продукты компании STMicroelectronics STSAFE (ECC 384, SHA 384, AES 256) также предлагают самую высокую защиту, основанную на надежной аутентификации, шифрованной связи, защищенном депонировании ключей, а также защите при запуске обновления прошивки. Кроме того, имеются и стандартизированные модули Trusted Platform Modules[2] (TPM), сочетающие в себе шифрование высокой сложности и безопасное депонирование большого количества ключей и подписей с защитой от физического считывания данных, хранящихся в них. Они, например, предлагаются компаниями Infineon и Microchip/Atmel[3].

ШИФРОВАНИЕ НА ПУТИ ОТ ОКОНЕЧНЫХ УСТРОЙСТВ ДО ОБЛАКА

Microchip/Atmel разработала и предложила весьма интересную концепцию. В августе 2016 г. она стала первой компанией в мире, которая смогла запустить решение для защиты каналов передачи информации «от начала до конца» в структуре «Интернета вещей» (IoT), использовав для этого подключение к облачному сервису Amazon Web Services IoT (AWS IoT[4]).

AWS IoT работает в соответствии со строгими критериями проверки подлинности и всеобъемлющего шифрования на всех соединительных точках пути передачи информации. Это гарантирует, что обмен данными между устройствами и AWS IoT никогда не происходит без подтвержденного идентификатора. Новые микросхемы–идентификаторы для аутентификации от Microchip/Atmel AWS-ECC508 позволяют максимально упростить соответствие требованиям AWS IoT Cloud. Это связано с тем, что компаниям — производителям конечного оборудования, не нужно загружать какие-либо закрытые ключи или сертификаты в микросхему во время своего производственного процесса. Дело в том, что микросхема AMC-ECC508 заранее должным образом уже сконфигурирована на предприятии-изготовителе и полностью готова к тому, чтобы сразу же быть обнаруженной в качестве одобренного устройства в системе технологии AWS IoT Cloud.

ШИФРОВАНИЕ В СИСТЕМЕ «УМНОГО ДОМА»

Приведенный на рисунке простой практический пример иллюстрирует использование микросхем шифрования в системе «умного дома». Это не только простые чипы аутентификации, такие как Optiga Trust SLS, которые гарантируют, что лишь авторизованные устройства, например элементы управления затвором цифровой камеры или камерами наблюдения, которые установлены пользователем, могут «залогиниться» и войти в систему через центральный шлюз «умного дома». Микроконтроллер STSAFE Secure шифрует каналы связи между камерами и центральным шлюзом. А TPM в центральном шлюзе обеспечивает хранение ключей, обновление встроенного программного обеспечения, а также передачу всех данных в облако. В результате покупатель может быть уверен, что задачи сохранения подлинности, конфиденциальности и целостности передачи информации выполнены.

[2] TPM — название спецификации, описывающей криптопроцессор, в котором хранятся криптографические ключи для защиты информации, а также обобщенное наименование реализаций указанной спецификации. — Прим. перев.

[3] Компания Microchip приобрела Atmel 21 января 2016 г.

[4] Платформа AWS IoT обеспечивает подключение устройств к сервисам AWS и другим устройствам, защиту данных и безопасность взаимодействий, обработку данных устройств и действия с ними, а также взаимодействие приложений с устройствами даже при отсутствии подключения к Интернету. — Прим. перев.

КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ: ЧТО ТАКОЕ DLP-СИСТЕМА И ЗАЧЕМ ОНА НУЖНА БИЗНЕСУ

РОМАН БОЖКОВ
R.Bazhkou@falcongaze.ru

Говоря о киберугрозах, мы обычно представляем себе беспрерывно стучащих по клавиатуре хакеров в черных толстовках, однако на деле большинство корпоративных утечек данных происходит не вследствие хитроумных технологичных взломов, а гораздо более тривиальными путями. В частности, через инсайдеров — сотрудников организации, намеренно или случайно предоставляющих конфиденциальную информацию злоумышленникам. Именно на предотвращение такой ситуации ориентированы DLP-решения (Data Leak Prevention), такие как разработка компании Falcongaze — система SecureTower.

ПРИНЦИП РАБОТЫ DLP

Для предотвращения утечек SecureTower интегрируется в корпоративную сеть организации и контролирует весь внутренний и внешний трафик, такой как электронная почта, веб-активность, мессенджеры, USB-подключения и т. д. Для мониторинга применяются две схемы перехвата (рис. 1) — серверный и агентский. В первом случае решение анализирует трафик на сервере, во втором перехват происходит непосредственно на рабочих станциях. Второй способ перехвата позволяет значительно расширить перехватываемые каналы, охватив в том числе большинство мессенджеров и веб-трафик по протоколу HTTPS. В зависимости от нужд заказчика способы перехвата могут комбинироваться или использовать только определенные модули системы. Также существуют методы перехвата без установки агентов, такие как совместная работа SecureTower с proxy-устройствами при помощи ICAP-интеграции (контроль веб-трафика) и интеграция с почтовым сервером (контроль корпоративной почты).

Все перехваченные данные анализируются системой для выявления инцидентов, представляющих интерес для соответствующей службы. Их анализ происходит на основе заранее заданных правил безопасности, которые могут быть самыми разными

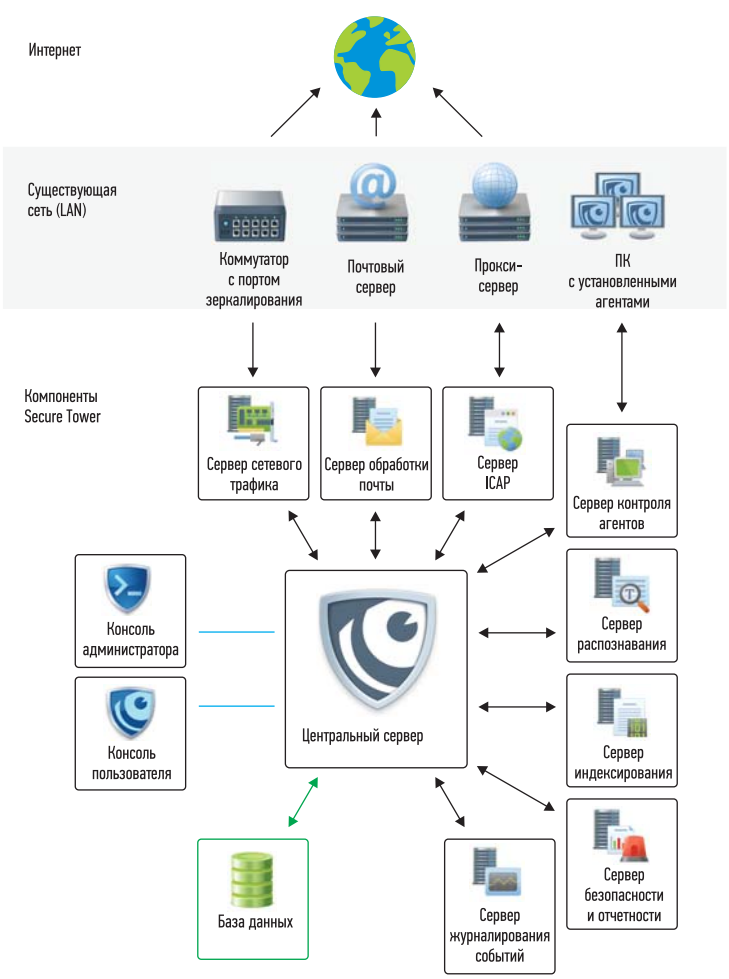


РИС. 1. ◀
Схема внедрения SecureTower

и сколь угодно сложными: система способна, например, уведомлять о передаче большого числа файлов на печать сотрудниками определенного отдела или блокировать передачу по электронной почте документа, содержащего данные из базы конфиденциальных документов. Все уведомления о событиях отправляются ответственному лицу, которое уже принимает решение, был ли инцидент правомерным или необходимо начать расследование.

ДЛЯ ЧЕГО НУЖНА DLP

Первоочередная задача, решаемая с помощью внедрения DLP-системы, — защита корпоративных данных от утечки. Использование системы — один из ключевых элементов в процессе построения эффективной системы управления информационной безопасностью. Без нее говорить о какой-либо защищенности от инсайдеров в компании бессмысленно.

Эффективность DLP проявляется не только в упреждении угроз информационной безопасности, но и в работе с бизнес-процессами. Благодаря тому что весь информационный трафик становится доступен для просмотра и оценки, появляется возможность для существенной оптимизации процессов — в том числе с точки зрения бизнес-составляющей. Задачи, на которые без DLP уходили бы значительные временные и человеческие ресурсы (например, классификация информационных активов), решаются значительно быстрее и качественнее.

DLP-система является эффективным инструментом для руководителей и HR-менеджеров. С помощью нее можно получать полную картину рабочего дня сотрудников, корректировать сроки и распределение задач, выявлять слабые места во взаимодействии персонала. В системе также возможен учет рабочего времени и активности сотрудников в рабочих программах.

Для создания полной картины информационных потоков DLP сохраняет все переданные и полученные данные. Это позволяет использовать SecureTower как инструмент ведения архивов бизнес-коммуникации. Любой диалог, а также переданный или полученный документ, можно восстановить из архива.

КАК РАБОТАТЬ С DLP

Для работы с системой предусмотрены две консоли — для администратора и для клиента. Первая позволяет взаимодействовать с серверными компонентами, а вторая предназначена для непосредственной работы с продуктом.

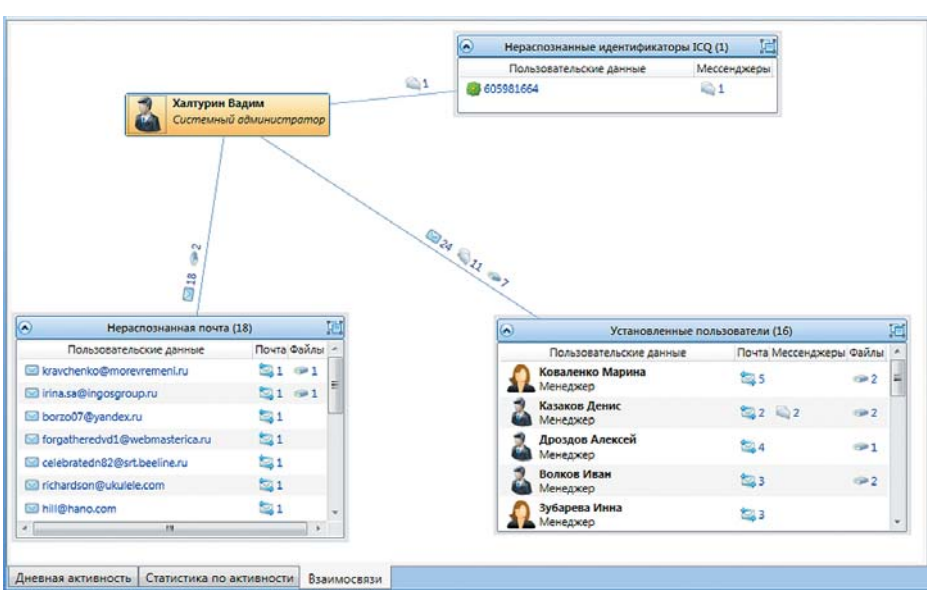
В клиентской консоли для работы с системой доступны семь модулей: модуль активности пользователей, модуль поиска информации, мониторинг файловых систем, модуль комбинированного поиска, центр обеспечения безопасности, центр отчетности и мониторинг в режиме реального времени.

Активность пользователей

Система в автоматическом режиме сохраняет всю перехваченную пользовательскую информацию. Данный модуль обеспечивает возможность ее просмотра и ретроспективного анализа. Здесь можно увидеть всю активность работника за любой период времени. Для каждого сотрудника в системе заводится профайл, в который можно экспортировать данные из Active Directory, а также дополнить его почтовыми адресами, аккаунтами в мессенджерах и т. д. В ходе работы системы профайлы могут заводиться и на всех внешних абонентов, с которыми сотрудник ведет общение, т. е. если сотрудник общается с каким-то внешним контактом, есть возможность посмотреть, с кем еще из работников организации ведет переписку этот контакт. Для удобства все эти данные визуализированы в граф-анализаторе (рис. 2).

Пользователей можно структурировать по группам, в зависимости, например, от отдела. Доступна статистика по активности каждого сотрудника в течение рабочего дня: количество полученных и отправленных писем, пересылаемых документов, использование принтера и т. д. Все документы можно просмотреть непосредственно в системе или сохранить их на локальный компьютер. В этом же модуле можно увидеть скриншоты рабочего стола пользователя, автоматически создаваемые через заданные промежутки времени.

РИС. 2. ▼
Граф-анализатор



Поиск информации/ комбинированный поиск/ мониторинг файловых систем

Данные модули позволяют осуществлять поиск нужных документов в перехваченной информации и на компьютерах пользователей. С помощью простого поиска можно находить нужные файлы среди перехваченных документов. Параметры запроса можно конфигурировать, а в результатах поиска просмотреть, когда и какими сотрудниками был передан искомый документ.

Мониторинг файловых систем позволяет выявлять конфиденциальные корпоративные документы, которые по какой-то причине оказались на компьютерах сотрудников. Для контроля передвижения критически важных данных в системе можно создать банк эталонных документов, оборот которых необходимо контролировать. Монито-

ринг рабочих станций сотрудников осуществляется автоматически: настроенные в системе правила безопасности срабатывают при появлении на компьютере того или иного работника документа, совпадающего с образцом, хранящимся в банке данных.

При комбинированном поиске можно использовать сложные правила и задавать несколько условий: например, вести поиск среди перехваченной информации определенного отдела документа определенного формата, более чем на 70% совпадающего с конфиденциальным.

Центр обеспечения безопасности

В этом разделе можно задать правила безопасности и просматривать архив уведомлений об их нарушениях. Правила устанавливаются как обычные, так и статистические. Также существует возможность задания правил безопасности с контролем по словарю (словари создаются предварительно в системе) или цифровым отпечаткам (базы данных цифровых отпечатков основаны на конфиденциальных документах). Для каждого установленного правила можно назначать подписчиков на уведомления — как сотрудников службы безопасности, так и, например, руководителей отделов.

Центр отчетности

В этом модуле можно просмотреть отчеты за произвольный промежуток времени по всем пользователям (или группам пользователей) и перехватываемым каналам. Отчеты полностью настраиваемые и дают возможность как оценить ежедневную работу сотрудников, так и получить актуальную информацию по инцидентам безопасности. Здесь же можно настроить автоматическое создание отчетов по расписанию и отправку их на электронную почту.

Мониторинг в режиме реального времени

В данном модуле можно в режиме реального времени подключиться к компьютеру работника. Доступен как аудиомониторинг (через подключенную к компьютеру гарнитуру), так и режим просмотра рабочего стола сотрудника.

ВНЕДРЕНИЕ DLP

На первом этапе компании, решившей внедрить у себя DLP-систему, следует провести пилотное тестирование выбранного продукта. Для его проведения предоставляется бесплатная триальная версия на ограниченное количество рабочих мест. Уже во время тестирования становятся видны первые результаты работы системы — выявляются остававшиеся до этого незаметными нарушители. Полученные результаты чаще всего обеспечивают окупаемость системы уже на стадии пилота.

Отличительной чертой внедрения SecureTower является простота этого процесса. Для установки этой системы не требуется привлечение консалтинга или наличие специального оборудования, настройка производится из одной консоли, а развертывание и запуск системы занимает считанные часы.

После внедрения работа с DLP становится частью ежедневных процессов службы безопасности. Постоянное улучшение правил безопасности и выявление критических мест позволяет обеспечить должный уровень защищенности организации.

Реклама

НА ШАГ ВПЕРЕДИ: НОВЫЕ РАЗРАБОТКИ КОМПАНИИ HARTING

ТАТЬЯНА ИЛЬИНЫХ
tatyana.ilinyh@fsmedia.ru

24–28 апреля в Ганновере пройдет одна из крупнейших в мире выставок высоких технологий, инноваций и промышленной автоматизации — HANNOVER MESSE. Вот уже 70 лет подряд она становится местом встреч производителей и поставщиков промышленной продукции. Накануне этого события известная компания HARTING Technology Group познакомила журналистов со своими новыми разработками, которые будут представлены на этой выставке.

Компания HARTING привозит свои новинки на Ганноверскую ярмарку на протяжении семидесяти лет и в этом юбилейном году с гордостью выступит под девизом «HARTING@Hannover Messe: прочное соединение уже 70 лет». Безусловно, в случае с HARTING участие в этом мероприятии можно назвать доброй семейной традицией, которая бережно чтится с 1947 г.

Семье Хартинг поистине есть чем гордиться: история компании, которая носит их имя, насчитывает несколько десятков лет. Основанная Вильгельмом и Марией Хартинг 1 сентября 1945 г., компания Wilhelm Harting Mechanische Werkstatten занималась производством товаров народного потребления в ангаре размером 100 кв. м в городе Минден силами десяти наемных рабочих. Неуклонно растущий спрос на продукцию вызвал необходимость в увеличении количества рабочих рук, и в 1947 г. компания расширила свое производство, а также впервые приняла участие в ярмарке в Ганновере.

Время скоротечно: на смену утюгам, энергосберегающему осветительному оборудованию, электрическим плитам быстро пришли ленточные магнитофоны, музыкальные аппараты и точное медицинское оборудование. В жизни компании HARTING новую эру открыл запатентованный в 1956 г. силовой соединитель Han. С 1970 г. производство и продажа разъемов стала приоритетным направлением их деятельности, а большой интерес заказчиков к этой продукции подтвердил правильность выбора направления.

В 1979 г., со старой закалкой, но с новым именем, HARTING Elektronik GmbH начала покорять Европу, а затем и весь мир. Франция была первой страной, открывшей перед семейным бизнесом HARTING свои двери, впоследствии к ней присоединились Австралия, Бельгия, Бразилия, США, Швеция, Китай, Великобритания, Япония — и это далеко не полный перечень. Сегодня HARTING имеет собственное производство в тринадцати странах, включая Россию, и представительства в сорока трех странах на разных континентах.

Компания HARTING старается всегда быть на шаг впереди своих конкурентов. Вот и в этом году на Ганноверской ярмарке — событии, к которому ежегодно тщательно готовится вся команда, предлагая свои решения и новинки в области Integrated Industry (в рамках Industrie 4.0), — компания представит своим заказчикам сразу несколько новинок. Их презентация для журналистов состоялась 7 февраля в местечке Эспелькамп, где, начиная с 1950 г. находится сердце компании HARTING.

«Мы всегда стремимся увеличить выгоду для заказчиков. Используя наши продукты и решения, они могут сделать свои производственные процессы более эффективными», — сообщил председатель совета директоров компании Филип Хартинг (Philip Harting) на этой пресс-конференции.

В качестве примера, подтверждающего эти слова, можно привести одну из недавних разработок HARTING — Smart HALL4YOU factory, которая доказывает, что интегрированные технологии — это уже не размытое представление о будущем, а вполне определенная реальность. Smart HALL4YOU factory демонстрирует, каким образом с помощью встраиваемых технологий можно увеличить прибыль и сделать производственный процесс более эффективным.

Там же, в Эспелькампе, команда разработчиков HARTING представила несколько миниатюрных новинок: Harting ix Industrial, HARTING T1 Industrial и M8 D-coded — решения в области соединения для промышленности будущего.

К примеру, HARTING Miss M8ty, название которого происходит от M8 D-кодирования, разработанного компанией HARTING в помощь производителям устройств в нынешнем тренде миниатюризации, решает проблему не только размеров, но также оцифровки и стандартизации. Даже самые маленькие полевые компоненты должны быть способны подключаться к суперсетям и говорить с ними на языке Ethernet.

Miss M8ty (рис. 1) — это тонкое и элегантное двухточечное Ethernet-

РИС. 1. ◀
Miss M8ty

РИС. 2. ◀
Разъем Harting ix Industrial

решение, обеспечивающее весь путь от облака до самого маленького датчика. Благодаря 100Mbits и PoE, veM8 с D-кодированием позволяет снабжать всех потребителей питанием и данными через маленький интерфейс, который ощутимо обогнал предыдущие системы шин.

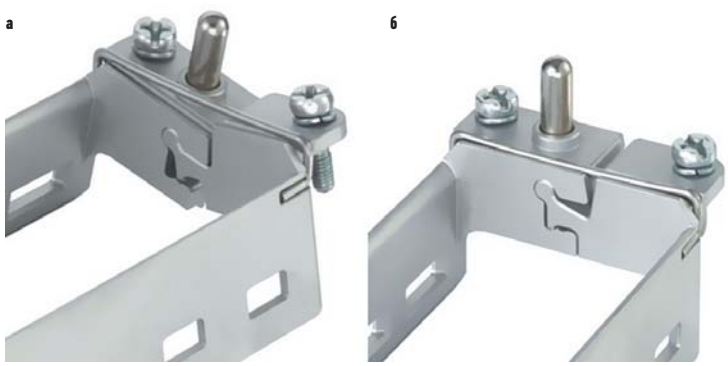
Особый акцент пресс-конференции был сделан на новом разъеме Harting ix Industrial (рис. 2) для интернет-соединения, который полностью покрывает потребности сегодняшнего рынка в компактных и надежных коннекторах с большой производительностью.

Как известно, спрос рождает предложение. Сегодня наиболее часто используемый коннектор RJ45 начинает сдавать свои позиции, электронные устройства становятся все меньше и меньше и популярные разъемы для них слишком велики, что и натолкнуло команду HARTING на разработку универсального компактного разъема, обладающего всеми необходимыми характеристиками.

Еще одна интересная новинка серии Han-Modular (рис. 3) — это соединительное решение для Industrie 4.0. Оно представляет собой надежную и прочную конструкцию с удобным

РИС. 3. ◀
Han-Modular

РИС. 4. ▶
Рамка Han-Modular Plus: а) открытая; б) закрытая



защелкивающимся замковым устройством, в которой можно комбинировать любые модули в зависимости от потребностей заказчика.

Ее составляющая, шарнирная рамка Han-Modular Plus (рис. 4), это новая надежная основа для серии Han-Modular: простая установка позволяет экономить время монтажа до 40%.

РИС. 5. ▶
Han Pneumatic Module Metal

Вниманию посетителей ярмарки также будет представлен новый пневматический модуль — Han Pneumatic Module Metal (рис. 5). Эта разработка призвана удовлетворить возросший спрос на более гибкие конструкции интерфейсов с прочными и долговечными металлическими контактами, которые можно подсоединять и отсоединять не менее 10 тыс. раз. Новый модуль позволит пользователям осуществлять подачу сжатого воздуха к приводам, блокам управления, тормозам, креплениям, разгрузочным блокам и т. д. даже в тех случаях, когда обычно для этого необходима полная модернизация производственного оборудования.

Кроме того, компания HARTING продолжает развивать экосистему MICA (рис. 6), уникальные возможности которой были продемонстрированы журналистам во время ознакомительного тура на производство HARTING.

Например, в этом году на ярмарке Hannover Messe впервые будет официально представлена измерительная система HARTING MICA Energy. Она позволяет просто и эффективно осуществлять сбор данных с существующего оборудования. Данные могут поступать как в MICA, так и в проприетарные решения, что несомненно является преимуществом данной системы.

На ярмарке в Ганновере восемь партнеров из MICA.network представят свои разработки в области перевода производства на цифровые технологии и IIoT (промышленный «Интернет вещей»), и основной акцент будет сделан на решениях для модернизации, которые позволяют особенно быстро увидеть выгоду в стоимости.

По мнению специалистов компании HARTING, промышленная цифровизация уже совсем близко, и своими новыми решениями и разработками они готовы это подтвердить. Для этого не нужно строить новые производства, достаточно лишь модернизировать то, что уже есть. HARTING уверенно движется по пути создания решений и продуктов, способных оптимизировать затраты и время своих заказчиков. ⬣

РИС. 6. ▼
Экосистема MICA

ИНТЕРФЕЙСЫ СРЕДСТВ ИНДИКАЦИИ

ТИМУР РУЗИЕВ
displays@ptelectronics.ru

Устройства графического отображения информации, модули ЧМИ уже давно нашли применение в автоматизированных комплексах и системах. Шкафы управления, операторские панели сегодня сложно представить без основного окна коммуникации между пользователем и автоматикой — без монитора. При выборе компонента отображения перед специалистами всегда стоит вопрос упрощения инженерных разработок в проекте и оптимизации издержек, особенно остро — в высокосерийных повторяющихся проектах. Обычно проектировщики останавливаются на более простых в плане интеграции решениях с интерфейсами VGA и DVI, реже HDMI. Эта статья предлагает классификацию интерфейсов средств индикации, а также описывает проблемы, с которыми сталкиваются разработчики, выбирая устройство отображения. Кроме того, будут рассмотрены предполагаемые решения этих, порой непростых инженерных задач.

ВВЕДЕНИЕ

В статье пойдет речь об индустриальном и коммерческом сегментах дисплеев. Их подробное описание и сравнение характеристик дано в материале, опубликованном в одном из прошлых номеров журнала «Control Engineering Россия» [1]. Для правильного понимания таких терминов, как «дисплей» и «монитор», рекомендую ознакомиться с упомянутой публикацией.

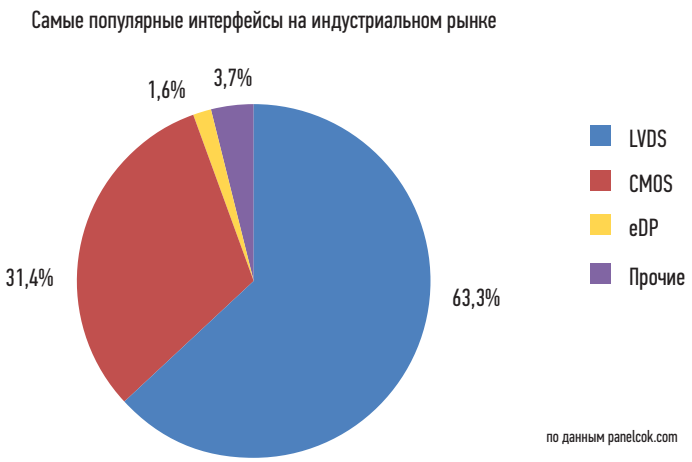
Для начала уточним, что дисплей, он же TFT-модуль/панель/матрица, — это лишь функциональный узел, отвечающий только за отображение информации. В то же время монитор — устройство более высокого уровня, с привычными для нас интерфейсами (VGA/DVI/HDMI), корпусом, OSD-панелью управления.

Что касается разделения «коммерческий/индустриальный», то условимся так: «коммерческие» TFT-модули — продукт для изделий массового спроса, в частности бытовой техники, мобильных устройств, телевизоров. Этому сегменту матриц свойственна высокая серийность, крайне низкая стоимость и весьма короткий срок нахождения в производстве. TFT-модули индустриального класса, напротив, стабильно изготавливаются 3–5 лет и больше, и зачастую, но не всегда имеют расширенные эксплуатационные параметры, а перед снятием их с производства обычно анонсируется модель-«преемник», близкая по характеристикам. В свою очередь, стоимость данного сегмента TFT-матриц заметно выше коммерческого класса. В дальнейшем разговор пойдет преимущественно об индустриальном сегменте матриц.

ОСНОВНЫЕ ИГРОКИ

Самыми распространенными интерфейсами управления

РИС. 1. ▶ Статистика eDP/LVDS/CMOS



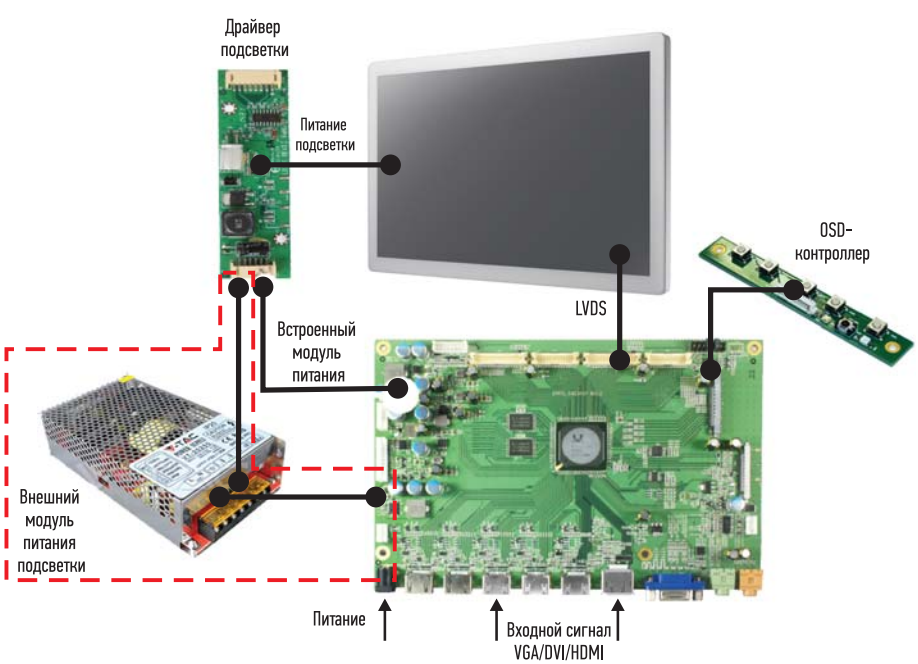
TFT-матриц считаются CMOS, MIPI и LVDS. CMOS является весьма популярным для индустриального сегмента, но при этом используется в TFT-модулях с небольшим разрешением (до 800×480 пикселей), а MIPI — интерфейс преимущественно коммерческого мобильного сегмента. Поэтому далее мы будем рассматривать стандарт LVDS и коснемся ныне набирающего популярность интерфейса eDP (рис. 1).

НЕТРАДИЦИОННЫЙ LVDS

Многие разработчики всячески стараются избежать использования LVDS при дизайне проектов и делают это небезосновательно. По данному стандарту можно управлять 6-, 8-, 10-битным цветом. Также LVDS позволяет управлять матрицами как с RGB-, так и с RGBW-пикселем. Кроме того, есть модификации стандарта dual LVDS и V-by-One HS (для управления дисплеями с высоким разрешением). Столь высокая вариативность интерфейса, с одной стороны, дает специалистам множество возможностей для реализации поставленных технических задач, с другой — сильно затрудняет работу с ним в силу малой стандартизованности интерфейса.

Отдельной проблемой можно назвать отсутствие каких-либо стандартов в пиновке разъема в целом, да и выбор самого разъема в частности. Каждый производитель дисплейных модулей волен самостоятельно выбирать тип подсоединяемого коннектора и расположения контактов на нем. Из-за этого подключение TFT-матриц требует высокой степени кастомизации.

РИС. 2. ▼ Структурная схема подключения TFT-модуля через контроллер преобразования интерфейсов



КОНТРОЛЛЕР ПРЕОБРАЗОВАНИЯ ИНТЕРФЕЙСОВ

Зачастую в применениях, не нуждающихся в особой корпусной защите устройства вывода графической информации (например, средство отображения должно быть встроено в стенку шкафа управления автоматикой), можно сократить производственные издержки, выбрав как раз дисплей с управлением по LVDS.

Предположим, в шкафу находится некий Box-PC, информацию с которого разработчик должен вывести на устройство отображения в стенке шкафа. Разработчик ограничен в бюджете и для сокращения затрат решает не переплачивать за готовый монитор, а воспользоваться более дешевым вариантом — TFT-матрицей с LVDS-интерфейсом. В таком случае незаменимой станет плата преобразования интерфейсов с привычного VGA/DVI на LVDS.

Производители плат преобразования интерфейсов, такие как Forenex, ICS Components и др., кроме самих контроллеров поставляют также необходимые аксессуары и кабели соединения всех узлов комплекта, причем делают это комплексно. В комплекс входят LED-драйверы, OSD-контроллеры, сенсорные экраны. Подобный способ избавляет разработчика от множества проблем, сокращая конечную стоимость устройства отображения до 30% по сравнению с готовым индустриальным монитором.

Однако у такого решения не может не быть недостатков. Главными минусами являются не самое удобное крепление матрицы (у TFT-панелей чаще всего монтажные отверстия находятся в торцах модуля) и компонентов и большое количество кабелей, находящихся в шкафу (рис. 2).

VGA/DVI VS. LVDS

Значительно меньшую конструктивную проблему представляет собой использование в качестве управляю-

щего дисплеем сигнала LVDS напрямую с компьютера.

Производители одноплатных компьютеров нередко устанавливают на своем устройстве отдельный LVDS-интерфейс под TFT-матрицу. Таким образом, главная задача, лежащая на плечах разработчика, — поиск необходимого кабеля для подключения двух узлов. Подобные кастомизированные кабели любой длины и пиновки смогут за относительно небольшие деньги сделать азиатские производители дисплейной периферии.

ДАЛЬШЕ НАС ЖДЕТ EDP

Стандарт eDP (Embedded Display Port) относительно новый, о нем заговорили только в 2010 г. eDP был разработан как альтернатива интерфейсу LVDS и стремительно завоевал популярность в сегменте коммерческих ноутбучных матриц. Довольно быстрое развитие eDP в этом сегменте TFT-модулей вызвано сразу несколькими факторами, главный из которых — битрейт, приходящийся на сигнальную пару. По сравнению с классическим LVDS-каналом он выше в 2–3 раза: до 21,6 Гбит/с вместо 7,5 Гбит/с у LVDS. Соответственно, для передачи одной и той же картинки eDP потребуется меньшее количество сигнальных пар, а значит, весь соединительный тракт упрощается. Кроме того, eDP считается более помехозащищенным и менее энергопотребляющим интерфейсом.

Стремительно покорив рынок коммерческих ноутбучных TFT-матриц, eDP замедлился в своем внедрении в другие сегменты дисплейных продуктов, однако продвигается и в них. Не стал исключением и сегмент индустриальных матриц. «Топовые» производители индустриальных TFT-модулей уже серийно выпускают дисплеи, управление которыми осуществляется по eDP. На данный момент таких TFT-матриц на рынке найдется всего пара десятков штук, но если взглянуть в «роадмапы» изготовителей индустриальных дисплеев, то можно сказать, что есть положительная тенденция увеличения доли стандарта eDP по отношению к LVDS. Конечно, LVDS еще долго будет присутствовать на рынке и вряд ли полностью себя изживет, но в ближайшие несколько лет eDP будет определенно его теснить.

Со временем и производители одноплатных компьютеров будут все чаще закладывать eDP-стандарт в базовую комплектацию своих девайсов. Сейчас эта функция преимущественно является опциональной, за разработку которой компании-изготовители чаще всего требуют дополнительную плату.

В заключение можно сказать, что в недалеком будущем мы увидим размытие границ между готовым монитором и дисплеем как узлом отображения информации. Во многом этому поспособствует развитие стандарта eDP. ⬢

ЛИТЕРАТУРА

1. Рахман Т. Цветная эволюция. TFT-модули в промышленной электронике. Часть 1 // CONTROL ENGINEERING Россия. 2015. № 1. www.controleng.ru/wp-content/uploads/40.pdf
2. Wiley C. The New Generation Digital Display Interface for Embedded Applications // DisplayPort Developer Conference. Westin Taipei. December 6, 2010.
3. Сайт www.vesa.org
4. LVDS Application and Data Handbook. www.ti.com/lit/ug/slld009/slld009.pdf
5. www.en.wikipedia.org/wiki/DisplayPort

Реклама

СОВРЕМЕННЫЕ МЕТОДЫ КОНТРОЛЯ И ЗАЩИТЫ ЦЕПЕЙ ПИТАНИЯ ОТ ТОКОВ ПЕРЕГРУЗКИ В СИСТЕМАХ АВТОМАТИКИ

АЛЬБЕРТ БАИШЕВ
abaishev@phoenixcontact.ru

Несмотря на устоявшееся мнение, что создание автоматизированных конвейерных производственных линий и роботизированных систем в самых разных областях промышленности — это прерогатива исключительно зарубежных компаний, в России появляется все больше отечественных предприятий, специализирующихся на модернизации, обслуживании, а также проектировании и создании таких систем. Именно специалистам этих компаний в первую очередь может быть интересно оборудование, о котором пойдет речь в данной статье.

Системы автоматики производственных линий должны работать бесперебойно, зачастую в режиме 24×7. Важную роль в обеспечении бесперебойной работы играет надежная система распределения питания по конечным нагрузкам (контроллерам, датчикам или исполнительным механизмам) с возможностью селективного отключения неисправностей. Чаще всего в таких приложениях используется централизованная система питания с резервированием. В таких условиях обязательно должен быть исключен сценарий, когда короткое замыкание или длительная перегрузка в одной из подключенных к системе питания нагрузок может вызвать перебой в питании всех остальных нагрузок, особенно контроллеров.

Новые многоканальные автоматические выключатели от Phoenix Contact серии CBMC (рис. 1) предлагают решение по селективной защите и контролю с возможностью адаптации параметров под каждое конкретное приложение.

РАЗВИТИЕ СИСТЕМ ЭЛЕКТРОПИТАНИЯ В АВТОМАТИЗАЦИИ ПРОИЗВОДСТВА

В подавляющем большинстве случаев в системах автоматики в настоящее время используются импульсные источники питания (ИП). Они могут обладать разными возможностями и функциональностью, но всех их объединяет одно общее свойство: в случае перегрузки в выходных цепях (вызванной аварией или ошибками при проектировании системы питания), если у ИП не хватает резерва мощности, он просаживает свое выходное напряжение. Это, в свою очередь, может вызвать ошибки в работе контроллеров и сбой в системе в целом.

Современные ИП становятся все более и более интеллектуальными. Зачастую производители указывают их устойчивость к коротким замыканиям, предлагают устройства с динамическим или статическим резервом мощности и возможностью конфигурирования параметров. Тем не менее единственным способом гарантированно защитить систему от просадки выходного напряжения по-прежнему является защита и мониторинг каждого отдельного выходного канала или нескольких групп нагрузок с помощью внешнего специализированного устройства.

ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ НА ОСНОВЕ СТАНДАРТОВ

Контроллер — это центральный элемент системы. Если с ним происходит сбой, то все останавливается. Диагностика ошибки требует значительно больше времени, если контроллер не успел сделать соответствующую запись, т. к. ошибка может быть где угодно.

Стандарт IEC-61131-2 регламентирует требования к программируемым логическим контроллерам (ПЛК). Он содержит основные параметры, требуемые для безопасной работы ПЛК, включая диапазон питающего напряжения и время, в течение которого напряжение может быть за пределами данного диапазона. ПЛК должен работать в нормальном режиме в диапазоне 20,4–28,8 В. Но при напряжении, например, ниже 20,4 В контроллер без внешней батареи может продержаться не более 10 мс. Соответственно, система питания должна или предотвратить падение выходного напряжения при неисправности одной из нагрузок, или как можно быстрее отключить неисправную выходную цепь. Но поскольку в каждом приложении всегда есть свои особенности и разные причины неисправностей, предотвратить падение напряжения на выходе ИП не всегда возможно. Это означает, что единственным надежным способом избежать сбоев в системе является мониторинг неисправностей в выходных каналах с помощью электронных автоматических выключателей. Отключение должно происходить в течение 10 мс после обнаружения неисправности.

КАКУЮ ХАРАКТЕРИСТИКУ ОТКЛЮЧЕНИЯ ВЫБРАТЬ?

В настоящее время в таких приложениях автоматизации производства широко применяются тепловые или термомагнитные защитные устройства. Токи перегрузки разогревают биметаллическую пластину или воздействуют на катушку, которая, в свою очередь, отключает часть, нуждающуюся в защите. В случае неисправности данные устройства генерируют высокие токи, повышающие риск остановки системы. В некоторых случаях для отключения неисправности номинальный ток должен увеличиться от 8 до 15 крат. Многие импульсные ИП не способны продолжительно питать систему в таких условиях, и в результате система отключается целиком.

Кроме того, современные устройства оснащаются все более чувствительной электроникой, что делает их более уязвимыми при высоких токах. Новые многоканальные электронные выключатели CBMC от Phoenix Contact обеспечивают более точный мониторинг тока в нагрузках и предлагают улучшенную защиту для электронных устройств.

ИНТЕЛЛЕКТУАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Современные методы измерения и интеллектуальное программное обеспечение (ПО) позволяют, во-первых, реагировать на неисправность при даже небольших изменениях тока. Это значительно снижает требуемый резерв мощности для ИП. Во-вторых, это позволяет более точно анализировать текущее состояние защищаемых цепей и реагировать в соответствии с этим. Например, можно отслеживать загрузку канала более 80% от установленного значения, длительную небольшую перегрузку и короткое замыкание. Также такая комбинация позволяет исключать ложные отключения при запуске нагрузки с большой емкостью и большими пусковыми токами. Все эти функции предлагают новые автома-

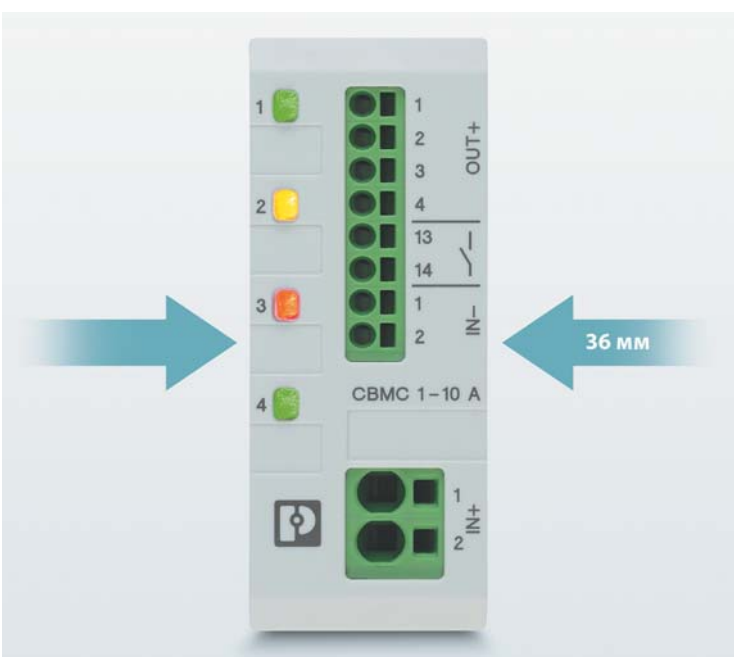


РИС. 1. ◀ Многоканальные электронные автоматические выключатели CBMC

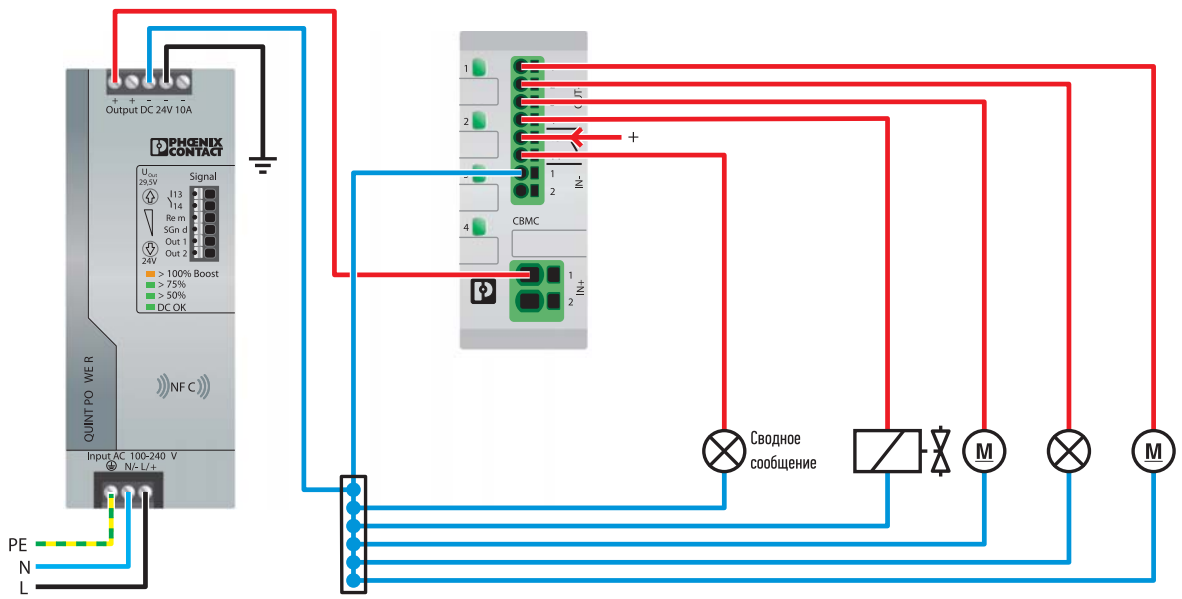


РИС. 2. ▲
Пример установки CBMC

тические выключатели серии CBMC (рис. 2), которые контролируют бесперебойное электропитание системы, используя интеллектуальный анализ изменений токов нагрузки.

Компактная конструкция CBMC позволяет встраивать их в существующие установки без изменения планировки шкафа. Особенности CBMC:

- Четыре независимых канала, каждый из которых может быть настроен по номинальному току в диапазоне 1–10 А с шагом 1 А с помощью светодиодных кнопок.
- При необходимости устройство может быть заказано с требуемыми настройками.
- Светодиодные кнопки на лицевой панели отражают текущий статус каждого канала.
- Сигнал об изменении состояния выходных каналов может быть передан дистанционно с помощью сухих контактов.

Основные параметры CBMC представлены в таблице.

ОТКЛЮЧЕНИЕ НЕИСПРАВНОСТЕЙ С ВЫСОКОЙ ТОЧНОСТЬЮ

Одной из причин широкого распространения механических автоматических выключателей, в частности термомагнитных автоматических выключателей, является большое разнообразие электронных устройств, для эффективного селективного отключения которых требуются различные характеристики срабатывания. Но использование механических автоматических выключателей всегда требует высоких отключающих токов. Это, в свою очередь, может потенциально нарушать стабильную работу электрической системы. С появлением электронных автоматических выключателей значительно повышается точность срабатывания защитных устройств за счет измерения и анализа токов, протекающих в защищаемых цепях. В результате надежное отключение возможно в диапазоне от 1,1 до 2 крат от установленного номинального значения. Это значительно упрощает проектирование системы в целом, отпадает необходимость закладывать большие резервы по мощности, что в свою очередь позволяет сокращать общие габариты системы.

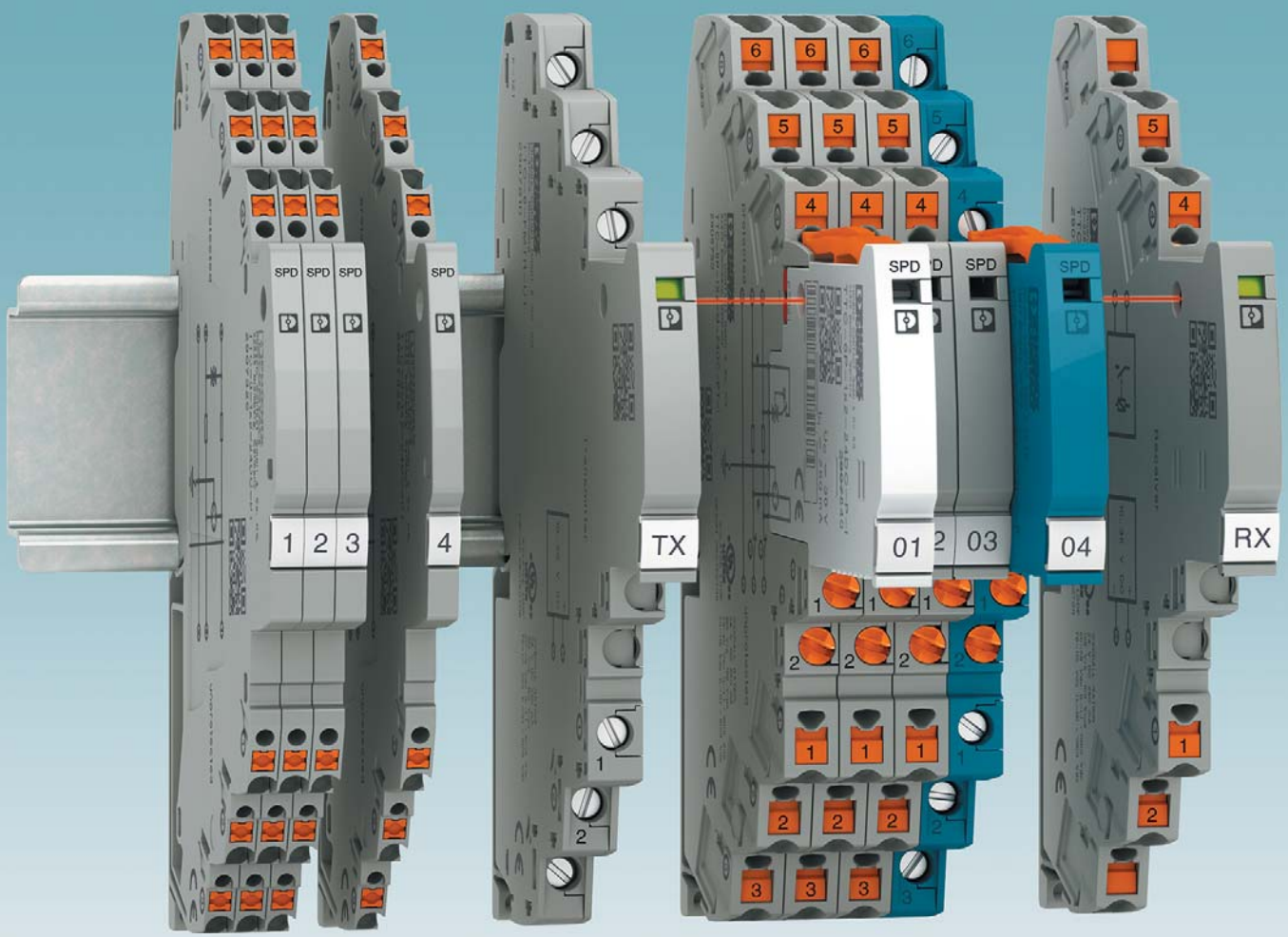
ТАБЛИЦА. ОСНОВНЫЕ ПАРАМЕТРЫ CBMC

Параметр	Значение
Номинальное напряжение, В DC	24
Диапазон рабочих напряжений, В DC	18–30
Количество выходных каналов	4
Настройка каждого выходного канала	1/2/3/4/5/6/7/8/9/10 A DC
Требуемые номиналы предохранителей	Не требуется, встроенный элемент Fail-Safe
Внутренний предохранитель на каждом выходе	15 A DC (4 A DC для версии CBMC E4 24DC/1-4A)
КПД, %	>99
Время на отключение в цепи нагрузки	≤10 мс (при коротком замыкании >2,0×I_N); 1 с (при (1,2...2,0)×I_N)
Индикатор состояния	Светодиодный (зеленый, желтый, красный)
Дистанционная сигнализация	Общий аварийный сигнал, сухой контакт Н.З.
Диапазон температур окружающей среды (при эксплуатации), °C	–25...+60
Степень защиты	IP20
Габариты (ВхШхГ), мм	90×36×98

ЗАКЛЮЧЕНИЕ

Использование электронных автоматических выключателей CBMC позволяет гарантированно защитить систему от возможных сбоев в связи с просадкой выходного напряжения ИП. Используемые при этом методы измерения и алгоритмы позволяют решить эту задачу без значительных резервов мощности ИП. Это упрощает проектирование, уменьшает габариты системы, одновременно увеличивая ее надежность. ⬣

TERMITRAB complete



Выбирая новую серию УЗИП от PHOENIX CONTACT, Вы получаете:

- Значительную экономию пространства в шкафу, т.к устройства имеют ширину от 3,5 мм
- Возможность выбрать устройство с функциональностью, точно соответствующей Вашему конкретному приложению:
  - С монолитной или штекерной конструкцией;
  - С контролем состояния и защитой от длительной перегрузки или без;
  - Со встроенными ножевыми размыкателями или без;
  - С винтовым или пружинным (Push-in) подключением проводов;
  - Для изолированных цепей или с общим опорным потенциалом;
  - Устройства для всех уровней типовых напряжений;
  - С возможностью использования во взрывоопасных зонах.
- Возможность всегда точно знать в каком состоянии находятся Ваши защитные устройства благодаря модулям дистанционной сигнализации

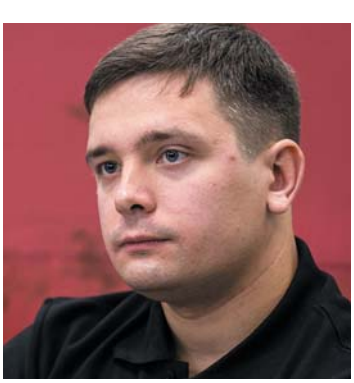
Подробная информация на сайте www.phoenixcontact.ru

Реклама

PHOENIX CONTACT
INSPIRING INNOVATIONS

БИОМЕХАТРОНИКА: ШАГИ НАВСТРЕЧУ ЭНЕРГОЭФФЕКТИВНЫМ РОБОТАМ

Недавно компания Boston Dynamics всколыхнула научную и широкую общественность видео, демонстрирующим акробатические способности своего нового робота Handle [1]. Это является еще одним доказательством того, что роботы становятся все более «умелыми», впечатляют силой, ловкостью и скоростью, но за кадром по-прежнему часто остается их энергоэффективность. Пока разработчики решают проблему «методом грубой силы», подтягивая силовой кабель, устанавливая аккумулятор побольше или используя двигатели внутреннего сгорания в качестве энергетической установки, но экономность — это прежде всего умение тратить. До сих пор не удалось создать робота, который мог бы конкурировать даже с человеком (не говоря уже о гепардах) одновременно по скорости, устойчивости и эффективности расходования энергии на собственное перемещение. Это мотивирует инженеров и ученых пристальнее взглянуть на то, как устроены живые системы.



СЕРГЕЙ КОЛЮБИН, к. т. н., Университет ИТМО
s.kolyubin@corp.ifmo.ru

ВИКТОР МУСАЛИМОВ, д. т. н., Университет ИТМО
musvm@yandex.ru

БИОМЕХАТРОНИКА

Биомехатроника — это прикладная междисциплинарная наука, объектом изучения которой является взаимодействие биологических организмов и мехатронных систем во всех его аспектах. Она объединяет в себе передовые наработки из механики, теории управления и обработки информации, компьютерного зрения, электроники, биологии и медицины.

Чаще всего под биомехатронными системами подразумевают интеллектуальные протезы и ортезы

(рис. 1–3), однако эта область гораздо шире. Кроме рук и ног, у человека масса органов, работе которых можно помочь благодаря внедрению «умных механизмов», включая сердечно-сосудистую и дыхательную системы.

Эта тематика сейчас крайне актуальна, а признанными лидерами в области биомехатроники считаются Чикагский реабилитационный институт, Массачусетский технологический институт и Университет Беркли в США, а также Университет Твенте в Нидерландах.

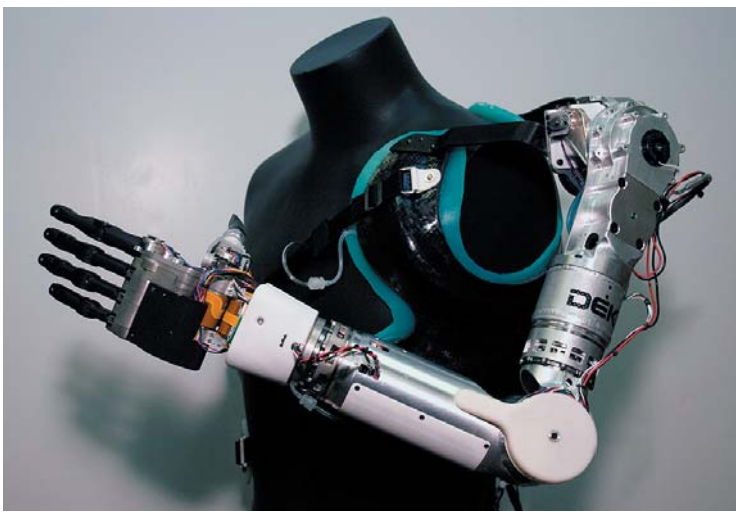


РИС. 1. ◀ Интеллектуальный протез руки

ПРАКТИЧЕСКИЕ ПОДХОДЫ И НАПРАВЛЕНИЯ ИССЛЕДОВАНИЙ

Базовым знанием в биомехатронике является понимание того, как работает сложная система — тело человека: как она движется, обменивается информацией и энергией.

Ответить на вопрос о том, как координируются перемещения всех составляющих опорно-двигательного аппарата человека при ходьбе, беге и других упражнениях, и построить соответствующие математические и компьютерные модели помогают системы захвата движения — как оптические (маркеры и высокоскоростные камеры), так и кинестетические, состоящие из датчиков механических перемещений и инерциальных сенсоров.

Другое активное направление в биомехатронике — это создание систем очувствления, которые отвечают за безопасное и эффективное физическое взаимодействие робота с человеком и окружающей средой. Для этого используются датчики сил и моментов, искусственная кожа и биологические сенсоры. При этом равное по важности значение имеет специальное алгоритмическое обеспечение для комплексирования и фильтрации измерений, а также реализации соответствующих законов управления движением. К слову, зачастую «железные» сенсоры заменяются на виртуальные, то есть существующие в виде программного кода (т. н. наблюдатели состояния). Вообще технологии тактильного очувствления и коммуникации (haptics) активно разрабатываются за рубежом для массы приложений, но авторам неизвестно ни об одной специализированной лаборатории в этой области в России.

Отдельное поле для исследований в биомехатронике — системы с эластичными элементами регулируемой жесткости. Они востребованы в широком спектре медицинских приложений, от ассистивной хирургии и диагностических комплексов до интеллектуальных протезов, ортезов или экзоскелетов (рис. 4–5). На крупнейших научных мероприятиях этим вопросам посвящают отдельные секции, круглые столы и мастер-классы. Не была исключением и Международная конференция по интеллектуальным роботам и системам, прошедшая в Корее в октябре 2016 г. [2].

Помимо существенного снижения риска травмирования человека по сравнению с жесткими конструкциями, наличие в роботе «пружин» позволяет уменьшить суммарные затраты энергии на цикле движения и при этом развивать большие пиковые значения сил и момен-

РИС. 2. ◀ Биомехатронная ступня

РИС. 3. ◀ Протез ноги

РИС. 4. ▶
Экзоскелет

тов, необходимые, например, для того, чтобы подняться по лестнице, встать со стула, подпрыгнуть или ударить по мячу. Однако для реализации полного потенциала этого подхода необходимо решить нетривиальные научно-технические задачи как при продумывании дизайна конструкций, так и при синтезе алгоритмов планирования и управления движением.

Можно пойти дальше и использовать в разработках принцип со-дизайна физической и кибернетической составляющих, который является основополагающим в проектировании киберфизических систем [3]. Применительно к роботам речь идет о со-дизайне конструкции, актюаторов, сенсорного оснащения, вычислителей и программного обеспечения для управления, сбора, обработки и передачи информации.

В этой статье мы подробнее затронем механизмы рекуперации энергии [4–5], которые заложены в тело человека. Их более глубокое изучение и воспроизведение в мехатронных системах позволит создать значительно более энергоэффективных роботов.

МЕХАНИЗМЫ РЕКУПЕРАЦИИ ЭНЕРГИИ

Во время бега с любой скоростью человек сохраняет около 80% полной механической энергии. С ростом скорости передвижения существенно увеличивается доля энергии, сохраненной за счет ее передачи между звеньями тела, и уменьшается ее передача — за счет перехода кинетической энергии движения в потенциальную в поле силы тяжести и обратно.

Именно эффект рекуперации энергии определяет механическую эффективность движений человека. В настоящее время считается, что сохранение и повторное использование, или рекуперация, механической энергии происходит за счет действия трех механизмов:

1. Перехода кинетической энергии в потенциальную энергию гравитации и обратно.
2. Перехода (или передачи) механической энергии от одного звена к другому.
3. Перехода кинетической энергии движения в потенциальную энергию деформации мышц и сухожилий и обратно.

Первый механизм рекуперации. Сохранение полной энергии по этому механизму требует строго противофазного изменения кинетической и потенциальной фракций энергии. Такое явление наблюдается не во всех звеньях тела. Например, в беге и ходьбе потенциальная и кинетическая энергии стопы одновременно достигают нулевого значения в опорной фазе. Чем выше над опорой располагается звено, тем больше энергии оно может сохранить. Считается, что первый механизм рекуперации энергии обеспечивает в целом в естественных локомоциях экономию энергии в диапазоне 12–23%.

Второй механизм рекуперации. Механическая энергия может передаваться от звена к звену тела человека за счет воздействия через суставные сочленения посредством контактных сил, совершающих работу по изменению энергии соседнего звена. Здесь разумнее говорить о переходе энергии поступательного движения, когда прикладываемая к плато сила (последовательное вертикальное нагружение) преобразуется за счет спиральной анизотропии большеберцовой кости и особого шарнира-сочленения в энергию ее вращательного движения. По различным оценкам, рекуперирование энергии по механизму ее передачи от звена к звену составляет от 30 до 42% от полной энергии.

Третий механизм рекуперации энергии. Вследствие того что мышцы человека работают только на сокращение, основному движению предшествует движение в противоположном направлении. Происходящее в таких предварительных движениях растяжение мышц приводит к накоплению в них энергии упругой деформации, используемой затем в основном движении. Если быть совсем точным, то растягиванию подвергаются мышечно-сухожильные структуры. Степень использования энергии упругой деформации зависит от условий выполнения движений, в частности от времени между растягиванием и укорочением мышц. При увеличении паузы между предварительным растягиванием и последующим укорочением за счет релаксации мышц и сухожилий снижается энергетическая экономичность. Интервал времени, за который должна накопиться и использоваться энергия упругой деформации, определяется постоянной времени релаксации, например, для сгибания коленного сустава она равна 1,4 с. Если время

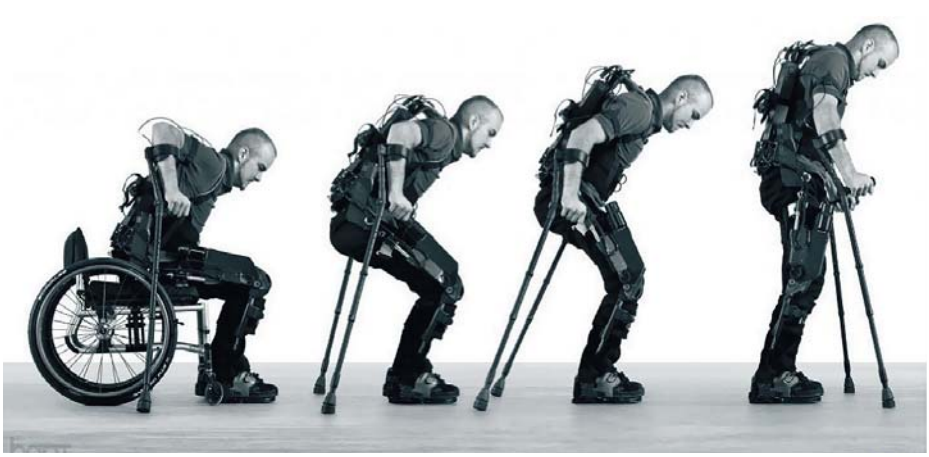


РИС. 5. ▼
Экзоскелет на человеке

движения больше времени релаксации, накопленная энергия полностью рассеивается и последующая фаза движения осуществляется только за счет метаболической энергии мышечного сокращения. По разным данным, рекуперация энергии в мышечно-сухожильных структурах составляет от 6 до 37%.

Рассмотрим один из подходов к оценке рекуперационного эффекта. В работах [6–8] представлены экспериментальные исследования кинематики коленного сустава.

Исследователи установили, что кости бедра и большеберцовой кости совершают угловые перемещения относительно друг друга по следующим анатомическим осям (рис. 6):

- первичное сгибание/разгибание;
- вторичное вращение внутрь/наружу большеберцовой кости;
- вторичное отведение/приведение.

Сгибание и разгибание являются необходимыми элементами движения во время ходьбы, в то время как вторичные движения принимают на себя прикладываемые нагрузки, осуществляя рекуперацию энергии. Цикл ходьбы начинается с фазы опоры/удара пяткой, который следует за опорой на обе ноги, когда обе ступни контактируют с землей. Затем происходит опора на одну ногу, после чего идет фаза переноса. В период фазы опоры формируется контактное давление в коленном суставе между мыщелоками бедренной кости и плато большеберцовой кости. В рамках неклассического подхода к задачам теории упругости [9] эти контактные давления поддаются расчету, после чего определяются приведенные жесткости контакта.

Интересен тот факт, что в течение цикла ходьбы вращение большеберцовой кости изменяется (по данным эксперимента) от +4° до –4°, в то время как угол сгибания-разгибания изменяется от нуля до значения 30°. Значение +4° соответствует удару пяткой при начальном контакте ноги с опорной поверхностью, а –4° — завершению контакта. Исследователи [6–8] объясняют такое поведение особенностью кинематической связи в суставах.

Дальнейшее моделирование динамики позволило им уловить тенденцию взаимодействия указанных звеньев без учета очевидной кубической нелинейности. В этом-то и просматривается путь к оценке рекуперативных свойств системы. Анализ показывает, что динамическое поведение системы берцово-бедренного контакта характеризуется замкнутой траекторией, которая называется релаксационным колебанием.

ПОДСКАЗКИ БИОМЕХАНИКИ

Для повышения энергоэффективности, а также безопасности и удобства физического взаимодействия биомехатронной системы с человеком конструктивные решения и системы управления «умных» ортезов и протезов должны учитывать ряд свойств естественного движения человека.

Так, объясняя феномен поворота большеберцовой кости, следует обратить внимание на особенности не только кинематической связи в суставах, но и физико-механической структуры большеберцовой кости, которую можно промоделировать упругим эквивалентным спирально-анизотропным стержнем: он при продольном сжатии-растяжении скручивается/раскручивается [11]. Таким образом, динамическая система коленного сустава представляет собой колебательную систему, что и обеспечивает в ней рекуперацию энергии.

Если продолжить путь учета колебательности рассматриваемой системы, то на «следующем повороте» мы столкнемся с самосинхронизацией [12]. У человека при ходьбе происходит самосинхронизация систем левой и правой ног (как и других конечностей). Соответственно, и в реабилитационных системах следует обеспечить синхронизацию системы здоровой ноги и реабилитируемой системы нога-ортез уже на уровне аппаратных средств. Кроме того, реализация самосинхронизации левой и правой ног в антропоморфных роботах обеспечит лучший режим движения для рекуперации энергии в системе. ⬣

ЛИТЕРАТУРА

1. http://spectrum.ieee.org/automaton/robotics/humanoids/boston-dynamics-handle-robot
2. www.iros2016.org/workshops_and_turorials.html
3. https://ru.wikipedia.org/wiki/%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D1%84%D0%B8%D0%B7%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0
4. http://biofile.ru/bio/16440.html
5. www.inva-life.ru
6. Ribero A. A biomechanical multibody knee model based on ellipsoid: modeling, simulation and analysis. MSc Thesis, University of Milano. 2010.
7. Lafortune M.A., Cavanagh P.R., Sommer H.J., Kalenak A. Tree-dimensional kinematics of the human knee during walking. J. Biomech. 25(4), 347-357. 1992.
8. Ribero A., Rasmussen J., Flores P., Silva L.F. Modeling of the condyle elements within a biomechanical knee model. Multibody System Dynamics. V.28, Nos.1-2, Springer. 2012. P.181-197.
9. Ворович И. И., Александров В. М., Бабешко В. А. Неклассические смешанные задачи теории упругости. М: Наука. 1974.
10. Гилмор Р. Прикладная теория катастроф. Кн.2.-М.:Мир. 1984.
11. Мусалимов В. М., Мокряк С. Я., Соханев Б. В., Шиянов В. С. Определение упругих характеристик гибких кабелей на основе модели спирально-анизотропного тела // Механика композитных материалов. 1984. №1.
12. Блехман И.И. Вибрационная механика. М.: Физматлит. 1994.

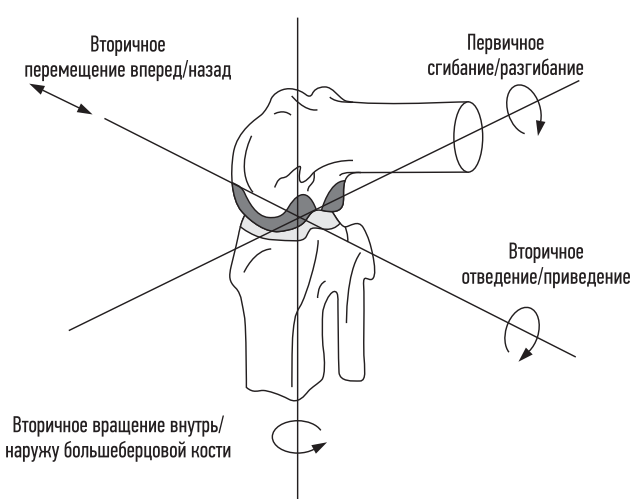


РИС. 6. ◀
Смещения бедренной и большеберцовой костей при ходьбе человека

РОЛЬ ЭЛЕКТРОННО-КОМПОНЕНТНОЙ БАЗЫ В РОБОТОТЕХНИКЕ

От выбора компонентов на ранней стадии создания проекта зависит успешность и финальные характеристики робототехнической системы. Национальная Ассоциация участников рынка робототехники (НАУРР) побеседовала с Максимом Гурбашковым, коммерческим директором «АВИ Солюшнс», и Владиславом Сычковым, руководителем Сибирского центра Фонда перспективных исследований (ФПИ), о состоянии и перспективах развития российского рынка робототехники и компонентов.

МАКСИМ ГУРБАШКОВ,
КОММЕРЧЕСКИЙ ДИРЕКТОР «АВИ СОЛЮШНС»

ВЛАДИСЛАВ СЫЧКОВ,
РУКОВОДИТЕЛЬ СИБИРСКОГО ЦЕНТРА ФПИ

Какие тренды развития робототехники в России вы можете выделить?

Владислав Сычков (далее — В. С.): Один из последних трендов развития робототехники — концепция «софт-роботикс» (англ. Soft robotics)[1]. Это направление предполагает повышение адаптивности промышленных и гражданских сервисных роботизированных комплексов (РТК), оно ориентировано на активное взаимодействие с человеком как с партнером по работе. В целом, все больше внимания уделяется психологическому восприятию РТК.

Развитие робототехники во многом определяется совершенствованием компонентной базы. Какие вы можете назвать драйверы мирового рынка компонентов? Технологические новинки?

Максим Гурбашков (далее — М. Г.): Существует ряд технологий и компонентов, являющихся ключевыми для робототехники. Это приводы и их компоненты, датчики, бортовые вычислители, инерциальные датчики и системы, аккумуляторы и системы питания.

Если говорить о приводах и их компонентах, то можно выделить нескольких мировых лидеров: maxon motor (Швейцария, малогабаритные двигатели и приводы), Harmonic Drive AG (Германия, волновые передачи и приводы на их основе), Elmo (Израиль, малогабаритные контроллеры привода), TQ Robodrive (Германия, встраиваемые бескорпусные двигатели и приводы на их основе). Каждая из этих компаний обладает рядом уникальных технологий и компетенций и широко востребована в определенных областях промышленности, включая робототехнику. Отдельного внимания заслуживает технология магнитной передачи: преимущества такого редуктора особенно важны при работе в жестких климатических условиях.

Если говорить про датчики угла поворота, то в настоящий момент очень активно развиваются технологии работы с магнитным полем. Сегодня технологии позволяют построить магнитный датчик угла поворота на одном чипе с высокой точностью (до 22 бит). При этом неоспоримым преимуществом такого датчика являются его малые габариты и высокая интегрируемость в конструкцию РТК.

Активно развиваются и аддитивные технологии. Все больше используется метод 3D-печати, причем особый интерес представляет 3D-печать по металлу. 3D-принтеры по металлу позволяют получить высокоточные качественные компоненты не только на этапе прототипирования, но и при серийном выпуске. Отдельного внимания заслуживает технология трехмерной печати схем на пластиках 3D-MID.

Как вы оцениваете состояние отечественного рынка компонентов? В каком направлении он движется?

М. Г.: Дать оценку объема российского рынка компонентной базы для робототехники достаточно сложно, поскольку большую его часть составляет оборонно-промышленный комплекс. Тем не менее рынок еще далек от насыщения и потенциал его роста высок.

В. С.: В России есть существенный НТ-задел для развития собственной компонентной базы, однако технологические возможности и опыт реализации проектов, направленных на изготовление серийных изделий ЭКБ[2], способных конкурировать и замещать зарубежные анало-

[1] Область робототехники, сосредоточенная на построении систем с обеспечением гибкости на различных уровнях, что позволяет РТК работать в условиях недетерминированной окружающей среды. Гибкость достигается за счет конструктивной гибкости системы, использования мягких материалов, гибкости алгоритмов управления , включая адаптивное (здесь и далее — прим. НАУРР).

[2] ЭКБ — электронно-компонентная база.

ги, начали формироваться только в последние 5–7 лет.

На развитие отечественной компонентной базы влияние оказывают также тренды и тенденции, свойственные зарубежному рынку. Как развивается рынок компонентов за рубежом? Насколько отстает от него российский рынок?

М. Г.: Прежде всего стоит отметить, что у западных и российских производителей существенно отличается подход к ведению опытно-конструкторских разработок. Многие российские предприятия, которые занимаются производством приводов, ведут собственные научно-исследовательские разработки, но — точечно, под заказ или узкий круг задач. Такой подход к научным и опытно-конструкторским разработкам накладывает существенные финансовые нагрузки на конкретный заказ или проект, что отпугивает потенциальных потребителей и формирует у них привычку обращаться к каталогу.

На Западе сформирован другой подход. Крупные компании ежегодно выделяют часть своей прибыли на ведение R&D[3] по актуальным направлениям в инициативном порядке, опираясь на результаты маркетинговых исследований, запросы и обратную связь от заказчиков. Это позволяет создать технологический задел в компании и сформировать «библиотеки» наработанных технических решений. В совокупности с готовностью вести доработки изделий под требования заказчика это дает существенное сокращение сроков разработки специализированных решений и уменьшение расходов. В результате до 90% оборота компании обеспечивается заказами на специализированные решения, максимально соответствующие индивидуальным требованиям проекта.

В. С.: Отставание России от мирового уровня в разработках компонентов РТК в среднем составляет 5 лет. Поэтому сегодня требуется реализовать меры, направленные на сокращение этого отставания и разработку типовых рядов РТК различного применения.

По сравнению с ведущими мировыми странами, в России повышенное внимание к робототехнике и компонентам наблюдается недавно. Чего, по-вашему, не хватает российским компаниям для того, чтобы сократить отставание от ведущих мировых производителей?

М. Г.: Несмотря на приверженность традиционным методам ведения работ, у российских разработчиков есть свои преимущества. Их отличает сильная инженерная школа, опыт разработки, оригинальные конструкторские решения. Если говорить о компонентах, то одной из проблем российского рынка является разрыв между наукой и практическим применением результатов исследований. Требуется развивать компетенции компаний, связанных с внедрением разработок на практике, подготовкой и запуском серийного выпуска актуального для рынка продукта, а также выведением его на рынок. Российским компаниям— разработчикам компонентов необходимо учиться создавать конечный продукт, изучать рынок и внедрять этот продукт в конечные применения, поддерживать его на всех этапах реализации, включая послепродажное обслуживание.

В. С.: Российским робототехническим компаниям, в свою очередь, не хватает кооперации. Большинство предприятий пытается «единолично» выполнять свои проекты и разработки, не привлекая внешних специалистов. Из-за этого результат страдает, т. к. робототехника — комплексное направление, охватить все его аспекты в рамках одного предприятия практически невозможно. Необходима профилизация: кто-то делает мехатронную часть, кто-то — связь и навигацию, кто-то — алгоритмику, интерфейсы и т. д. Также нужен инструмент организации профессионального сообщества и средство эффективного обмена информацией о существующих предприятиях и их компетенциях.

Развитие производства во многом зависит от состояния отрасли. Какие меры поддержки вы считаете необходимыми для развития российского рынка робототехники и отечественной компонентной базы?

В. С.: Не хватает кадров — налицо проблема популяризации. Несмотря на сильную техническую школу, о которой сказал Максим Гурбашков, в робототехнике наблюдается острый дефицит действительно эффективных специалистов. Поэтому необходима популяризация робототехники, проведение конкурсов, создание профильных программ поддержки молодых ученых и специалистов, налаживание взаимодействия между предприятиями-разработчиками и предприятиями-производителями с вузами по вопросу подготовки специалистов-робототехников. Нужно вводить заказ на количество и профиль таких специалистов.

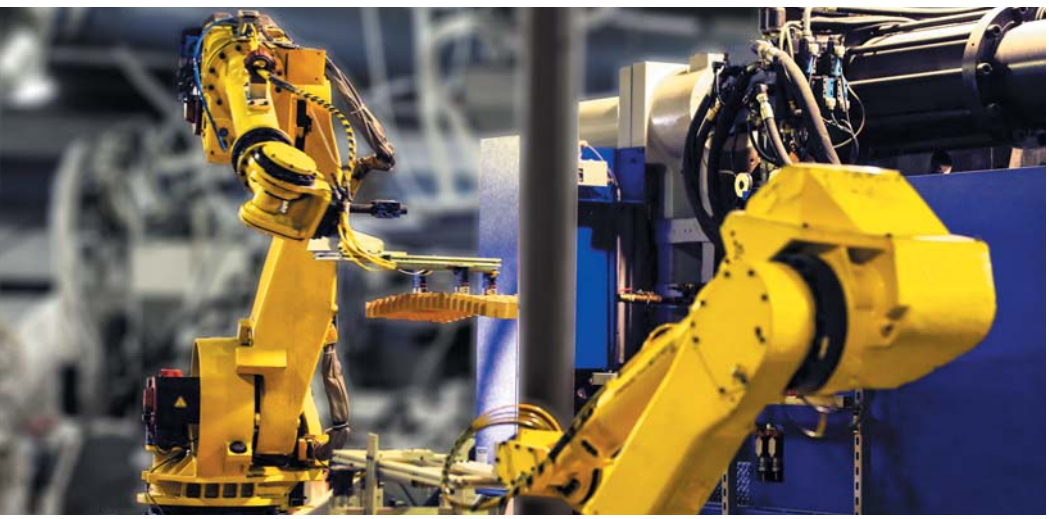
М. Г.: Мероприятия — это отдельная тема. Мероприятия способствуют не только популяризации отрасли, но и пониманию рынка его игроками. Например, практические мероприятия (конференции, семинары) облегчают изучение нужд и особенностей рынка. Это площадки, на которых возможна продуктивная коммуникация между разработчиками и производителями компонентной базы и ее потребителями, создателями робототехнических проектов. К примеру, одним из таких мероприятий практической направленности является международная практическая конференция «РобоСектор», которая уже третий год подряд собирает экспертов робототехнической отрасли, представителей вузов и НИИ, разработчиков и производителей робототехнических систем, носителей технологий и производителей компонентов.

Цель конференции — дать ответ на прикладной вопрос разработчика: «Какие технологии и компоненты можно использовать для решений той или иной практической задачи?». Мы стремимся организовать диалог между всеми участниками профессионального робототехнического сообщества как из России, так и из других стран для обмена идеями, знаниями, опытом, технологиями, которые есть у каждого из них. Именно поэтому девизом конференции выбрана фраза «Объединяя опыт и технологии».

Развитию производства способствует и активное государственное участие. Как государство может оказать поддержку производителям робототехники и компонентов?

М. Г.: Все, о чем мы до этого говорили, подводит нас к мысли о том, что нужна целостная система изменений в отрасли, а этого не достичь без государственной поддержки. Причем она должна быть комплекс-

[3] R&D — Research and Development (рус. научно-исследовательские и опытно-конструкторские работы, НИОКР).



ной и системной: таможенные процедуры и ввозные пошлины, система обучения и подготовки кадров для отрасли, поддержка разработок и стартапов, налоговые льготы и послабления и т. д.

В ряде стран правительство предоставляет реальные ощутимые льготы для бизнеса, который хочет и готов запустить новое производство. Если мы хотим успешно развивать определенные отрасли и конкурировать с экономиками других стран, мы должны искать пути создания благоприятной среды, способствующей изучению и развитию технологий, запуску производств, созданию новых рыночных ниш.

В. С.: Одним из направлений поддержки является создание профильных целевых программ, о котором мы уже говорили. От государства прежде всего требуется формирование профильных средств субсидирования, механизма льготного кредитования, введение льготных налоговых режимов. Кроме того, сейчас в отрасли отсутствуют стандарты и правила, общие (унифицированные) требования к продукции, и это тоже мешает работать. Необходимо выработать ГОСТы, определить регламенты сертификации продукции, задать основные правила игры. Нужно помнить, что нормативное, правовое и методическое обеспечение производства робототехники и компонентов должно осуществляться в соответствии с современными международными практиками и стандартами.

Фонд перспективных исследований был создан на основании ФЗ от 16 октября 2012 г. в целях содействия осуществлению перспективных высокотехнологических разработок в интересах обороны страны и безопасности государства. Какие формы сотрудничества с ФПИ доступны робототехническим компаниям? Что делает ФПИ для поддержки и развития гражданской робототехники?

В. С.: Во-первых, Фонд с интересом рассматривает заявки организаций, касающиеся предложений по разработке перспективных технологических решений в области робототехники — по всем направлениям исследований. Сейчас в разной степени проработки есть проектные предложения по физико-техническому и медицинскому направлениям исследований.

Во-вторых, непосредственно с перспективными идеями и разработками, необходимыми РТК, у нас работает Национальный центр развития технологий и базовых элементов робототехники.

В-третьих, несмотря на то, что проекты Фонда направлены в первую очередь на решение задач, связанных с обеспечением безопасности государства, все без исключения технологии впоследствии можно использовать и в гражданском секторе экономики. Ведь не секрет, что большое количество ноу-хау, присутствующих в передовых образцах ВВТ[4], интегрируются производителями в комплексы и системы гражданского назначения.

Фонд открыт для предложений от всех разработчиков — будь то конструкторские бюро и научно-технические центры государственных корпораций или небольшие коллективы инновационных коммерческих предприятий России. К тому же ФПИ, при условии положительного решения, финансирует проект на все 100% утвержденного бюджета, необходимого для получения максимально эффективного результата.

Тренд последних десятилетий — автоматизация, курс на отказ от участия человека в производственном процессе. Какими вы видите перспективы развития робототехники и компонентной базы?

В. С.: Уже сейчас мы видим, что в будущем большую роль в развитии робототехники, особенно промышленной, будет играть «Интернет вещей», его применение на производстве будет включать РТК.

Также уже сейчас ведется активная работа в направлении создания «полноценно» автономных машин, повышается уровень автономности РТК. Одна из тенденций развития робототехники — максимизация замены функционала аппаратной части программным обеспечением.

М. Г.: Что касается российской робототехники, кооперация внутри отрасли, обмен опытом и изучение опыта других стран, совместное выполнение проектов способствуют как повышению качества отдельных проектов, так и развитию отрасли в целом. Передовые производители робототехнических систем осознают это и начинают взаимодействовать с производителями компонентов на ранних этапах производства, что позволяет сделать систему более гибкой, избежать вероятных ошибок проектирования.

Лучшее, что можно посоветовать производителям компонентов в России, — не ждать заказ на исследование какого-то технологического направления, а начинать самостоятельно разрабатывать перспективные направления, что позволит в будущем сократить сроки работы над конкретными проектами и повысить возможности адаптации продуктовой линейки компании к запросам рынка. ⬢

Материал подготовили Алиса Конюховская, вице-президент НАУРР, и Валерия Цыпленкова, аналитик НАУРР.

[4] ВВТ — вооружение и военная техника.

МЕЖДУНАРОДНЫЙ ВОЕННО-МОРСКОЙ САЛОН

INTERNATIONAL MARITIME DEFENCE SHOW

IMDS

IMDS 2017

28 июня-2 июля

РОССИЯ

Санкт-Петербург

- ЭКСПОЗИЦИЯ ОБРАЗЦОВ ПРОДУКЦИИ ПРЕДПРИЯТИЙ
- ДЕМОНСТРАЦИЯ ВООРУЖЕНИЯ И ТЕХНИКИ
- КОНФЕРЕНЦИИ, СЕМИНАРЫ, КРУГЛЫЕ СТОЛЫ, ПРЕЗЕНТАЦИИ
- VIP-ПЕРЕГОВОРЫ
- ПОСЕЩЕНИЕ ПРЕДПРИЯТИЙ

Организатор:

МИНПРОМТОРГ РОССИИ

При участии:

Министерство обороны

Федеральная служба по военно-техническому сотрудничеству

Министерство иностранных дел

Администрация Санкт-Петербурга

АО «Рособоронэкспорт»

Устроитель:

IMDS

ООО «Морской Салон»

www.navalshow.ru

"Через сотрудничество – к миру и прогрессу!"

Реклама

ИНТЕГРИРОВАННЫЙ СЕРВОПРИВОД EMCA

ДМИТРИЙ ВАСИЛЬЕВ
dmitry.vasiliev@festo.com

В промышленной автоматизации все чаще появляются задачи изменения формата, перестройки на другой продукт, перемещения упоров. Традиционно такие задачи решались с помощью или ручной подстройки (например, колесо и винтовая передача), или двигателей постоянного тока. Однако ручные операции существенно снижают производительность, и в автоматизированных линиях их сегодня стараются не использовать, а двигатели постоянного тока обладают ограниченным ресурсом. Именно для таких задач локальной автоматизации компания Festo разработала новый компактный сервопривод с интегрированным контроллером на базе бесколлекторного двигателя постоянного тока (BLDC), который лишен самого основного недостатка — щеток. Рассмотрим подробнее устройство, особенности нового сервопривода, а также основные области его применения.

РИС. 1. ▶
Сервопривод EMCA

УСТРОЙСТВО И ОСОБЕННОСТИ СЕРВОПРИВОДА EMCA

EMCA (рис. 1) построен по принципу интегрированного сервопривода: двигатель, энкодер, силовая и управляющая электроника расположены в едином конструктиве. В качестве двигателя используется компактная синхронная машина с постоянными магнитами. Бесколлекторная коммутация обмоток реализуется с помощью силовых ключей — МОП-транзисторов. Управление коммутацией, контурами обратной связи, задание траектории движения возложено на микропроцессорный контроллер, также размещенный в корпусе устройства.

Такое конструктивное решение позволяет избежать длинных силовых и энкодерных кабелей и, как следствие, улучшить электромагнитную совместимость устройства и сократить время на монтаж и ввод в эксплуатацию сервопривода.

Поскольку основной задачей EMCA является позиционирование, в базовую функциональность встроен генератор траекторий движения и таблица позиций на 64 записи. То есть при

необходимости перехода в конкретную точку достаточно выбрать номер позиции и дать команду «старт».

КОМПЛЕКТАЦИЯ И ОПЦИИ EMCA

Сервопривод имеет один типоразмер и может быть выполнен в двух вариантах длины: S и M (короткая и средняя). Стандартно EMCA оснащен абсолютным магнитным энкодером на 12 бит для задач коммутации и позиционирования, однако в качестве опции можно установить электронный многооборотный абсолютный энкодер (с памятью позиций до семи суток без источника питания). Более подробно технические характеристики сервопривода представлены в таблице.

Поскольку довольно часто перемещение упоров должно выполняться вертикально, предусмотрена опция стояночного тормоза. Тормозом можно управлять и с помощью внешних сигналов.

Для управления устройством предлагается на выбор три варианта протокола: CANopen, EthernetIP и логические входы/выходы. Надо отметить, что интерфейс необходимо выбрать при заказе. Нельзя, например, заказать CANopen, а потом управлять через входы/выходы. С помощью CANopen, помимо позиционирования, можно реализовать и взаимосвязанное управление сервоприводами. Для этого предназначен протокол DS-402.

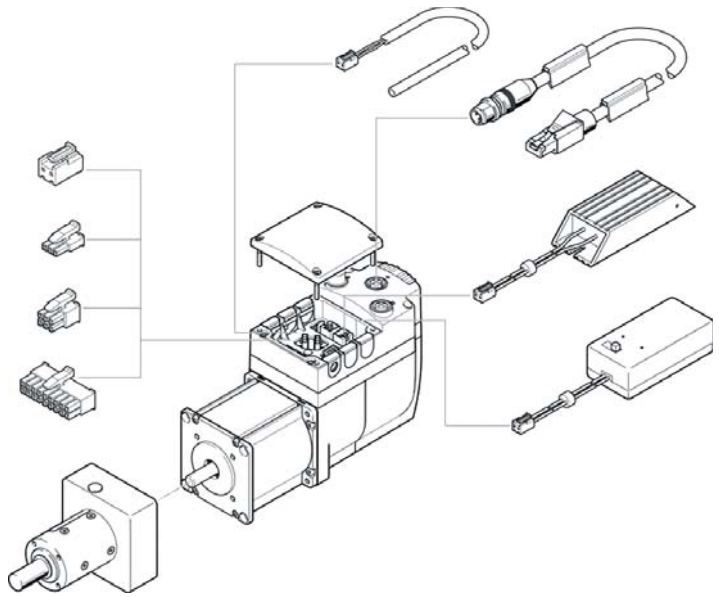


РИС. 2. ◄ Кабели и аксессуары EMCA: редуктор EMGC, внешний тормозной резистор, внешний аккумулятор, разъемы, кабели

Интегрированный сервопривод EMCA представляет собой самостоятельное устройство, управляющее движением, поэтому для работы с ним предусмотрены функции, обеспечивающие безопасность, — STO (Safe Torque Off — безопасное отключение крутящего момента).

В зависимости от зоны, где будет установлен сервопривод, следует выбрать степень защиты от воды и пыли: базовую IP54 или увеличенную IP65. Для такого рода двигателей степень защиты должна быть не ниже IP54, потому что установка и двигателя, и электроники происходит прямо на линии без шкафа управления.

Для обеспечения необходимых параметров движения имеются опциональные компактные планетарные редукторы с широким набором передаточных чисел, а также внешний

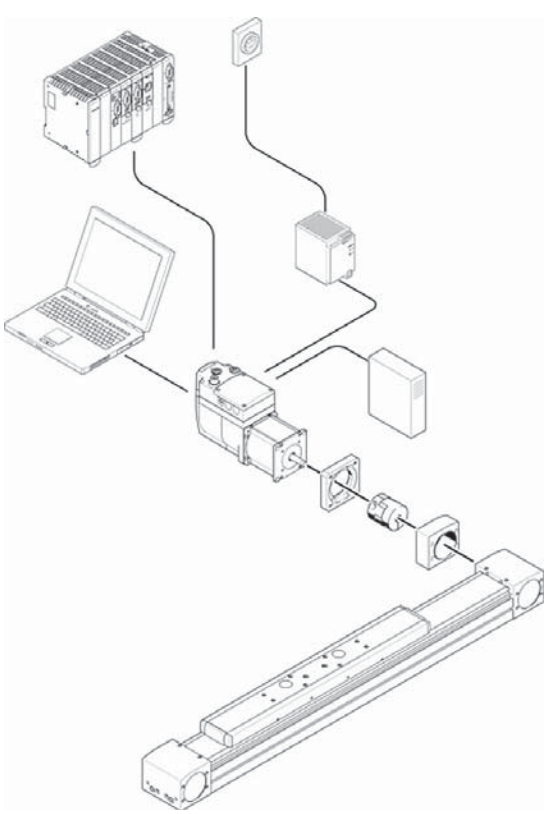


РИС. 3. ▼ Пример монтажа и подключения сервопривода EMCA, линейного привода с кареткой, ПЛК, источника питания и компьютера для настройки

ТАБЛИЦА. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ СЕРВОПРИВОДА EMCA

Электрические характеристики		
Размер	S	M
Номинальное напряжение, В	24 ±20%	
Номинальный ток, А	6,9	7,2
Пиковый ток, А	10,2	10,3
Номинальная мощность, Вт	120	150
Пиковая мощность, Вт	158	200
Максимальный ток, логические выходы, мА	100	
Логика переключения вход/выход	PNP	
Технические данные, двигатель		
Размер	S	M
Номинальная скорость, об/мин	3100	3150
Максимальная скорость, об/мин	3500	3300
Номинальный момент, Н•м	0,37	0,45
Пиковый момент, Н•м	0,85	0,91
Момент инерции ротора, кг•см²	0,175	0,301
Допустимая нагрузка на вал		
Осевая, Н	60	
Радиальная, Н	100	

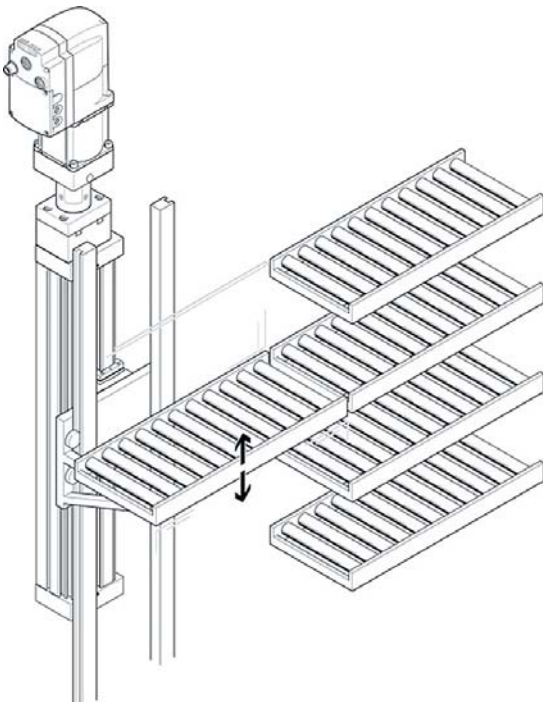
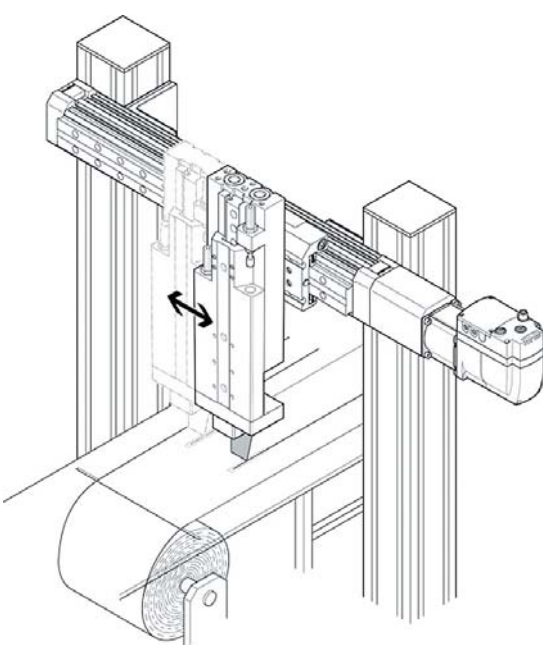


РИС. 4. ▲ Подстройка сортирующих конвейеров

тормозной резистор (рис. 2). Требования по активному теплоотводу не позволяют встроить тормозной резистор прямо в корпус EMCA.

Для монтажа сервопривода на электромеханических приводах Festo предлагаются монтажные комплекты (фланцы, муфты). Таким образом, можно получить комплектное решение задачи перемещения (рис. 3).

РИС. 5. ▼ Изменения формата реза



Настройка и конфигурация привода происходит с помощью интуитивно понятного программного обеспечения FCT (Festo Configuration Tool) по сети Ethernet. При компоновке с электромеханическими приводами Festo настройка привода занимает считанные минуты.

ПРИМЕНЕНИЯ ИНТЕГРИРОВАННОГО СЕРВОПРИВОДА

Сервопривод EMCA может быть использован как для перемещения упоров или изменения форматов (рис. 4–5), так и для задач локальной автоматизации (толкатели, делители потоков, поворотные столы). Функциональность EMCA позволяет использовать его и в манипуляторах (рис. 6). Машины печати и постпечатной подготовки, упаковочные и этикетировочные автоматы, деревообрабатывающее оборудование, текстильные машины, медицинские технологии, конвейеры, маркировка и изготовление электроники — таковы области применения интегрированного сервопривода EMCA от Festo.

ПРЕИМУЩЕСТВА ИНТЕГРИРОВАННОГО СЕРВОПРИВОДА EMCA

Благодаря интегрированной конструкции сервопривод EMCA может быть установлен прямо на линии без использования шкафа управления, что повышает электромагнитную совместимость, удобство и скорость монтажа. Применение необслуживаемого бесколлекторного двигателя гарантирует надежную работу установки без длительных простоев. Наличие опций — многооборотного энкодера, стояночного тормоза, дополнительно планетарного редуктора, внешнего тормозного резистора — позволяет решать широкий круг задач при оптимальных характеристиках, удовлетворяя требования конкретного применения. ⬣

ООО «ФЕСТО-РФ»
+7 (495) 737-3487
sales@festo.com, www.festo.com

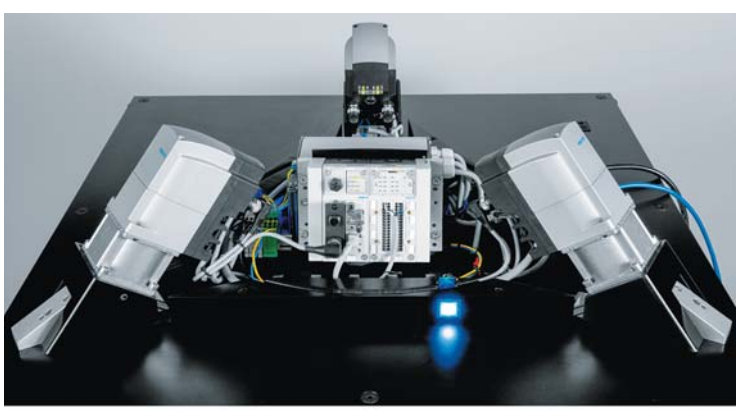


РИС. 6. ▲ Использование EMCA в качестве сервопривода для мини-Трипода без шкафа управления

WIS networks

ВИДЕОНАБЛЮДЕНИЕ
без проводов

Горнодобывающая промышленность
Тоннели
Метро

Нефтегазовая промышленность

Лифтовое оборудование
Подъемники

Удаленные районы без развитой инфраструктуры

Отели
Жилые комплексы

Корпоративный сектор
Образование

ПРЕИМУЩЕСТВА

- Быстрый монтаж независимо от расстояния
- Снижение стоимости решения по отношению к проводному соединению, при увеличении расстояния
- Высокая скорость (до 500 Мбит/с)
- Высокая масштабируемость и возможности для доработок
- Отличная гибкость и совместимость

ТИПОВАЯ СХЕМА ПРИМЕНЕНИЯ

WIS-IPC20P/L
-2MP 1080P
-Auto ICR
-H.264
-Onvif compatible
-IP67

WIS-IPC13P/L
-1.3MP 960P
-Auto ICR
-H.264
-Onvif compatible
-IP67

WIS-IPC20PD/L
-2MP 1080P
-Auto ICR
-H.264
-Onvif compatible
-IP67

EuroMobile
ТЕХНОЛОГИИ БЕСПРОВОДНОЙ СВЯЗИ

- Поставки оборудования напрямую от дистрибьютора
- Более 12 лет на рынке телеметрии
- Отдел разработок и проектирования
- Техническая поддержка и сервис
- Топовые позиции на складе
- Широкий модельный ряд
- Индивидуальный подход

ЕвроМобайл Россия
Санкт-Петербург, пр. Энгельса, д.71,
тел./факс +7 (812) 331-7576
8 800 555 75-76 (звонок бесплатный)
http://euromobile.ru;
info@euroml.ru

Реклама

ЗАЧЕМ НУЖЕН WI-FI В ТОРГОВОМ ЦЕНТРЕ

ЕВГЕНИЙ МИРОШНИЧЕНКО
evgeniy.miroshnichenko@euroml.ru

По мере того как носимые устройства становятся доступнее и появляются в руках у все большего числа людей, очевиднее становится необходимость обеспечить общественные места — будь то магазин, вокзал или даже улица — покрытием Wi-Fi. Каким образом удобнее и выгоднее достичь этой цели, например в торговом центре?

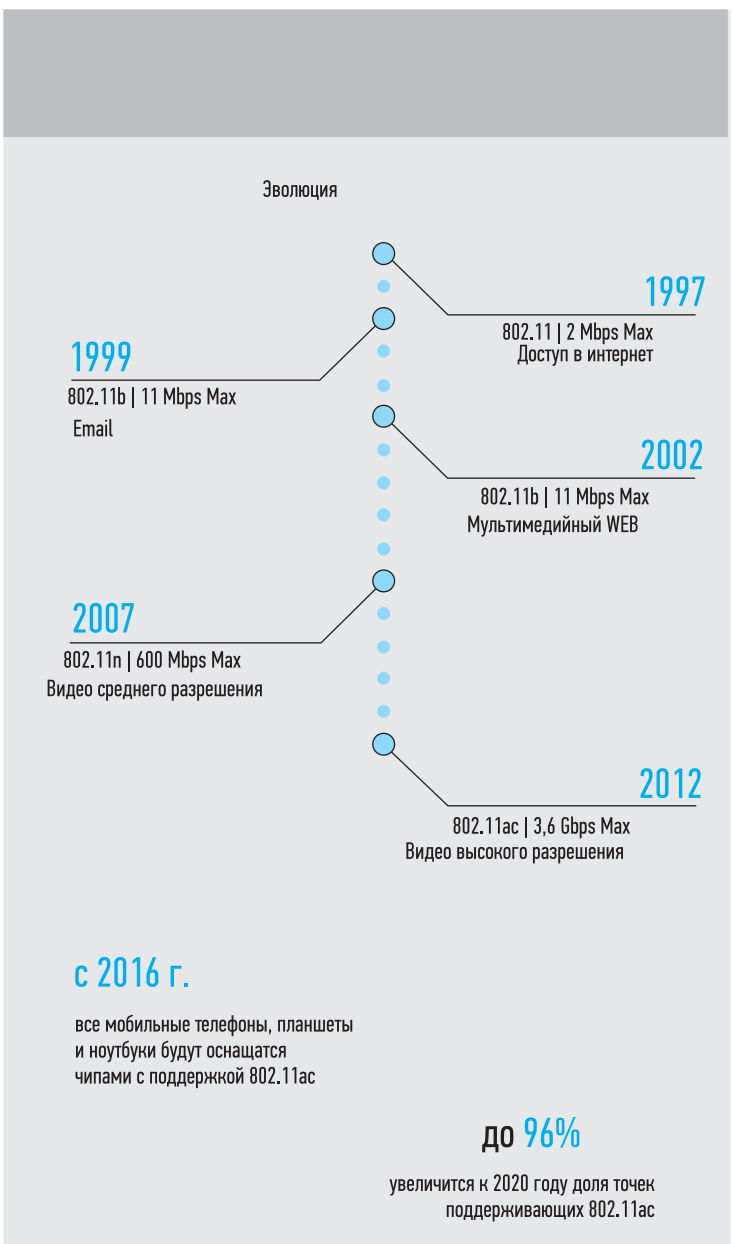


РИС. 1. ▶
Рост пропускной способности Wi-Fi

Интернет-трафик растет каждый год, и не пройдет и пяти -семи лет, как он достигнет десятков эксабайт. Трафик оконечных пользователей перераспределяется — сокращается доля проводных каналов и увеличивается доля беспроводных. Причины вполне очевидны: с одной стороны, носимые устройства (смартфоны, планшеты) становятся мощнее, а с другой — доступнее и дешевле. Мощности портативных гаджетов уже достаточно для весьма ресурсоемкого приложения — видеосвязи высокого качества. Сотовые операторы предлагают мощные смартфоны за небольшие деньги, поскольку их основной интерес лежит в продаже услуг — то есть трафика.

Пропускная способность Wi-Fi также значительно увеличилась. На рис. 1 показано, что с 1997 по 2012 год скорость выросла с 2 до 3,6 Гбит/с.

GSM и Wi-Fi не являются конкурентами, а скорее дополняют друг друга. Расчетная пропускная способность каналов GSM составляет не более 1,8–3 Гбит/с, что относительно немного для мест массового скопления людей, например большого торгового центра. Wi-Fi в этой ситуации может быть с успехом использован для разгрузки сети GSM. По этой причине наблюдается серьезный рост числа Wi-Fi-точек доступа. По оценкам экспертов, к 2020 году в мире будет работать около 433 млн подобных точек.

Как же применение сетей Wi-Fi помогает бизнесу? Какую информацию может получить бизнес от Wi-Fi? Использование Wi-Fi позволяет бизнесу собирать информацию о клиентах. Обработка данных по подключениям и запрашиваемым сведениям позволяет получить статистические

особенности клиентов — такие как демография, поведение, привычки, интересы. На основе полученной информации данных можно скорректировать предложения с ожиданиями клиента, используя для этого такие механизмы, как социальный маркетинг, персонализированные предложения, специальные предложения, SMS, e-mail-рассылки.

Все эти меры приводят к повышению лояльности клиентов и, как следствие, к повышению прибыли бизнеса.

ТЕХНИЧЕСКИЕ ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБЩЕСТВЕННЫХ WI-FI-СЕТЕЙ

Организация надежной и быстрой Wi-Fi-сети требует предварительных работ, включающих радиоразведку и радиопланирование. Wi-Fi-оборудование фирмы Wisnetworks и программа Spectrum Analyzer помогают выполнить такие работы (рис. 2). Радиоразведка позволяет провести текущий анализ радиоэфира, измерить уровни сигналов, шумов, определить наличие интерференции сигналов, скорости передачи данных, уровни потери пакетов. Радиопланирование — произвести расчет положения новых точек доступа с учетом результатов радиоразведки и особенностей помещения. Надо учесть наличие препятствий для распространения радиоволн и их материал (см. табл.) — это элементы конструкции здания, разнообразные перегородки и т. п. По результатам радиопланирования размещается новое оборудование, выполняются измерения, вносятся коррективы в проект.

ТАБЛИЦА. ЗАВИСИМОСТЬ РАСПРОСТРАНЕНИЯ РАДИОВОЛН ОТ МАТЕРИАЛА ПРЕПЯТСТВИЙ

Материал	Изменение уровня сигнала, дБ	
	2,3 ГГц	5,25 ГГц
Металлическая решетка	–20,99	–13,17
Штукатурка	–14,86	–13,24
Шлакоблок	–6,71	–10,33
Красный кирпич	–4,44	–14,62
Еловые доски	–2,79	–6,13
Плитка	–2,22	–1,42
Фанера	–1,91	–1,83
ДСП	–1,65	–1,95
Проволочная сетка	–1,21	–0,34
Стекло	–0,5	–1,69
Гипсокартон 12,8 мм	–0,49	–0,52
Оргстекло 7,1 мм	–0,36	–0,93
Рубероид	–0,1	–0,13
Потолочная плитка	–0,09	–0,18
Ковер	–0,03	–0,01
Линолеум	–0,02	–0,13
Жалюзи закрытые	–0,002	0,002
Жалюзи открытые	0,01	0,03
Ткань	0,02	0,01
Стеклопластик	–0,02	–0,03

При планировании размещения точек доступа и выборе их типа (одно- или двухдиапазонные) надо учитывать, что зона покрытия точек на 5 ГГц меньше, чем на 2,4 ГГц, поскольку чем выше несущая частота, тем больше поглощение в окружающих материалах. На частоте 5 ГГц каналов больше. Эти факторы дают возможность размещать точки доступа на 5 ГГц ближе друг к другу. К сожалению, пока не все пользовательские устройства могут работать на 5 ГГц, что ограничивает использование двухдиапазонных точек доступа.

Для торговых центров, с одной стороны, характерна высокая плотность клиентов, с другой — отсутствие необходимости в 100%-ном покрытии. Такое «пятнистое» расположение посетителей требует

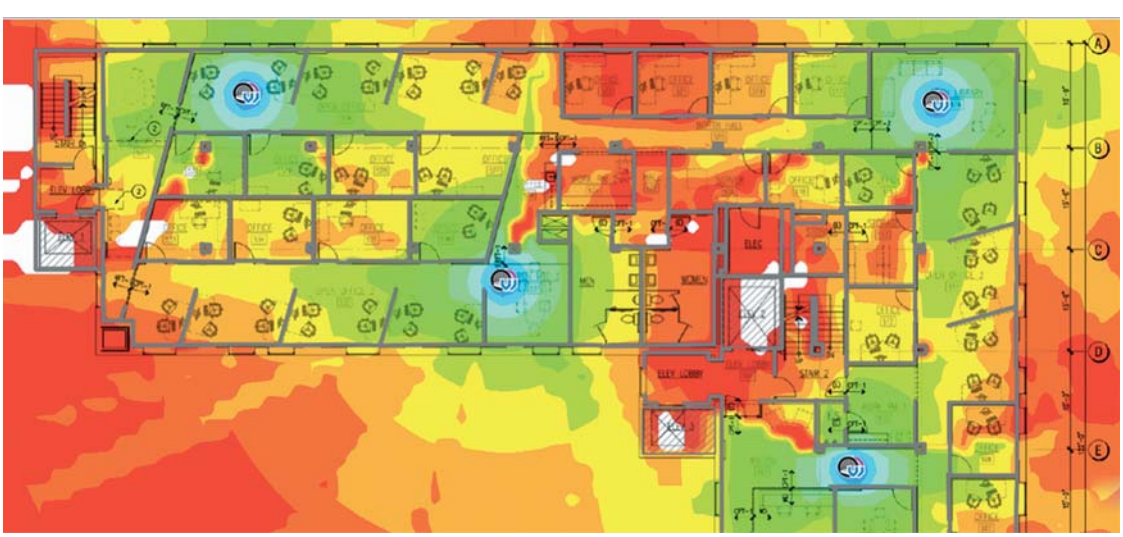


РИС. 2. ◄
Радиоразведка с помощью оборудования Wisnetworks

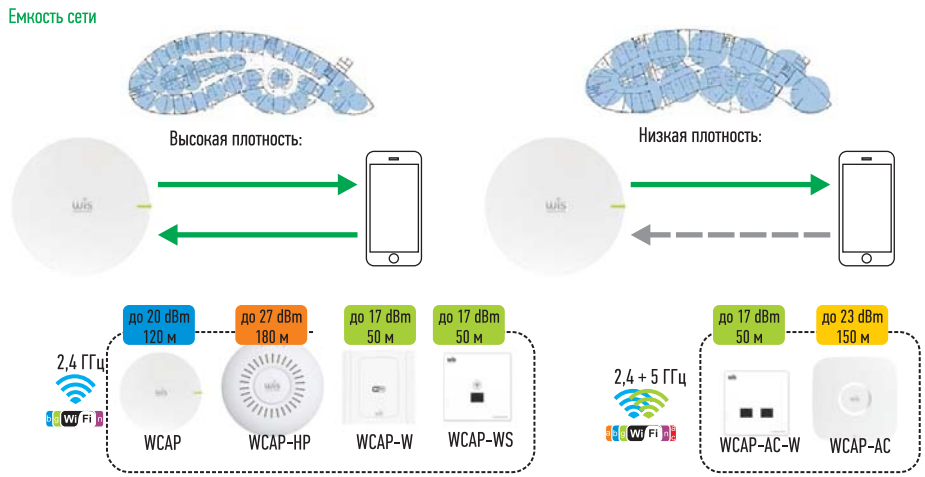


РИС. 3. ▲ Критерии выбора точек доступа

точек доступа с большим возможным числом подключений, но малой мощности. Большая мощность точки доступа вредна: во-первых, точки доступа будут мешать друг другу, а во-вторых, даже если клиент «услышит» точку доступа, сам до нее «докричаться» не сможет. Возникнет парадоксальная ситуация — уровень сигнала на клиенте 100%, а связи нет. Описанные вводные требуют производить многокритериальную оптимизацию при выборе характеристик точек доступа и мест их установки. Нужен разумный баланс между количеством точек доступа, их производительностью и ценой проекта. К примеру, для точек доступа Wisnetworks число ассоциированных клиентов составляет максимально 124. При равномерном распределении полосы пропускания по клиентам на каждого придется 1 Мбит/с. На рис. 3 показаны оптимальный и неоптимальный выбор расположения точек доступа и приведены примеры конкретных моделей точек доступа с указанием мощности. Мощность точки может регулироваться программно. В линейку моделей входят одно- и двухдиапазонные модели с различными видами монтажа: на потолок, на стену и в стандартные монтажные коробки.

Рассмотрим вопросы защиты обмена шифрованием. На рис. 4 показаны четыре вида шифрования трафика и их сравнительное быстродействие. Защита WPA/WPA2(PSK)-AES представляется наиболее сложной для взлома и обеспечивает максимальную производительность. Также следует отметить, что необходимость шифрования для общедоступной сети неочевидна. Ведь всегда имеется явное указание, что «данные, передаваемые по общедоступным сетям, могут быть перехвачены», хотя обычно на эти предупреждения пользователи внимания не обращают.

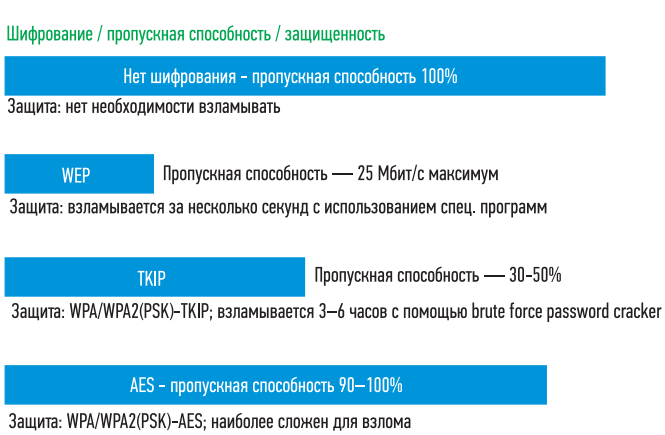


РИС. 4. ▶ Сравнение быстродействия различных способов шифрования обмена

ТОПОЛОГИЯ СЕТИ

Рассмотрим возможное построение сети с большим количеством (свыше нескольких десятков) точек доступа. Для таких сетей оптимально использование контроллера сети (в данном примере — это WisCloud controller), выполняющего функции централизованного управления сетью, мониторинга и оптимизации. В схеме также имеется шлюз, включающий функцию агрегации и балансировки каналов, что может быть полезно как для повышения общей пропускной способности, так и для резервирования каналов. К этому шлюзу можно подключать Radius-сервер. Контроллер аппаратный, он устанавливается как локально на объекте, так и через облако. Число поддерживаемых точек доступа достигает 1000. Существуют решения и для большего числа ТД (до 10 000). Пример организации сети показан на рис. 5.

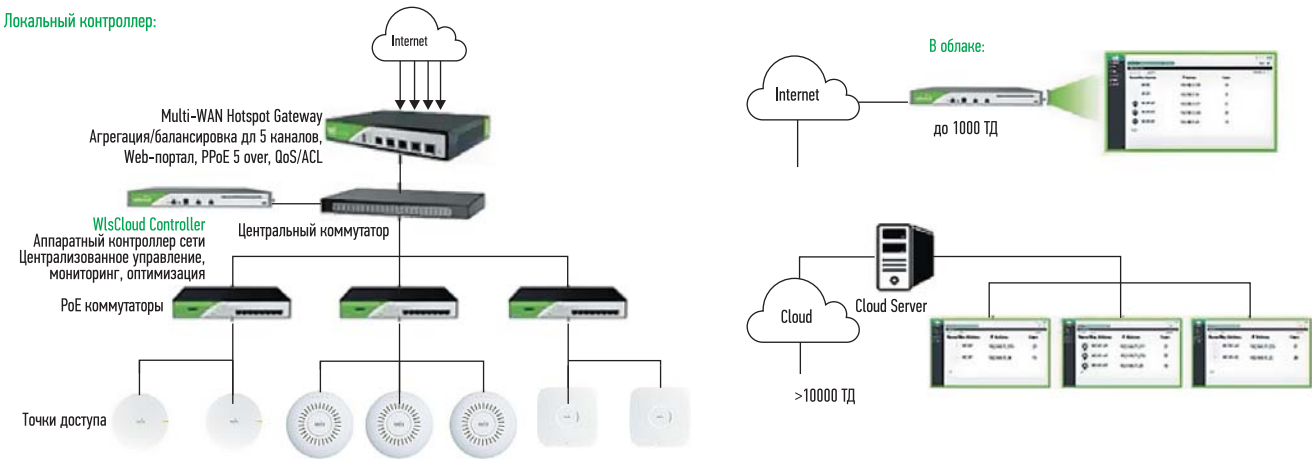
Из основного функционала следует отметить распределение нагрузки между соседними точками, оптимизацию каналов, автоматическое обнаружение в режиме L2 и L3 новых ТД, централизованную настройку и мониторинг. Также частично реализован бесшовный роуминг. «Частично» означает небольшую задержку при переключении. Например, при работе в программе видеосвязи пользователь ощутит незначительную задержку в передаче речи. Доработка этой функции приоритетна и в ближайшее время уже должна быть доступна. В первоочередных планах — функции балансировки мощности и так называемый band steering — принудительный перевод клиентов, способных работать в диапазоне 5 ГГц, в данный диапазон.

РАСЧЕТ СТОИМОСТИ ОРГАНИЗАЦИИ СЕТИ НА ОБОРУДОВАНИИ WISNETWORKS

Для расчета используем статистику, согласно которой средняя посещаемость российского ТЦ составляет 35 тысяч человек в выходной день. Примем, что нагрузка вырастает вдвое в утренние и послеобеденные пики, среднее время, проводимое в ТЦ, составляет 40–60 мин. Из расчета получится, что надо обслужить примерно 6000 клиентов в час. Известно, что одно-

Организация сети

С централизованным управлением



временно пользуются сетью 15% (900 чел.) и минимальная скорость составляет 3 Мбит/с. После учета пропускной способности каждой ТД в 94 Мбит/с получим, что необходимое число точек доступа составит 30 штук с нагрузкой в 31 клиента на каждую. Общая стоимость ТД в данном случае — $1600. Тот же расчет, но для двухдиапазонных ТД с большей пропускной способностью, даст общую сумму в $3000.

Определим теперь стоимость всего комплекта оборудования. На рис. 6 показан расчет общей стоимости оборудования, предназначенного для оснащения ТЦ сетью Wi-Fi.

В этом предложении использованы POE-коммутаторы, но не учтена стоимость центрального коммутатора.

Для однодиапазонных ТД на 2,4 ГГц общая стоимость оборудования достигает примерно $3300. Для двухдиапазонных — $4700. В реальном проекте следует дополнительно учесть стоимость центрального коммутатора и монтажных элементов.

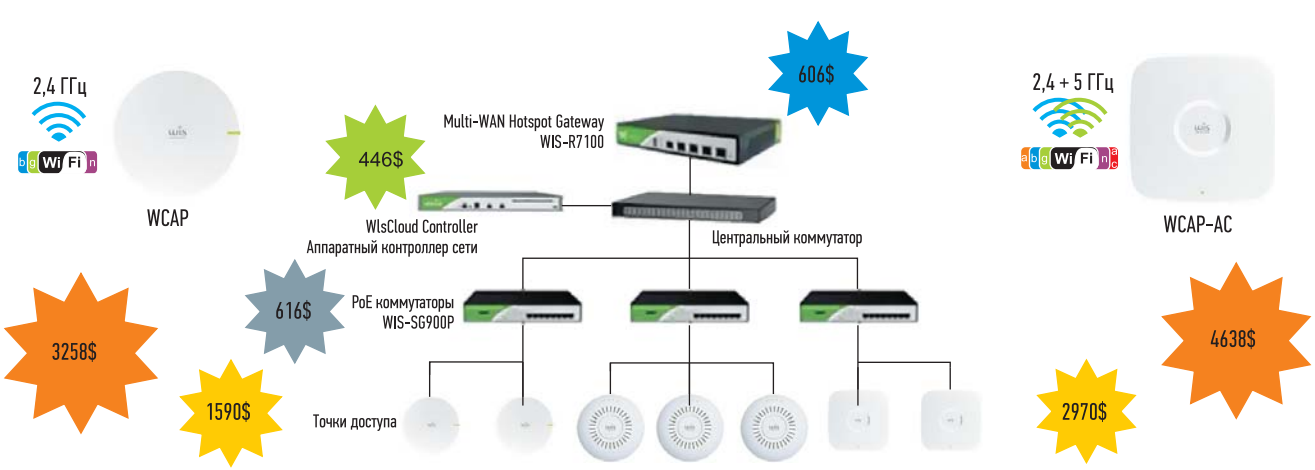
Таким образом, без сомнения, наличие Wi-Fi-доступа в Интернет является уже не дополнительной, а обязательной функцией общественных мест. Но быстрое и сравнительно экономичное развертывание, возможность настройки различных уровней доступа в сеть (общественный, защищенный, индивидуальный), идентификация и простота в обслуживании — все это позволило оборудованию Wisnetworks завоевать популярность среди провайдеров и интеграторов. ⬣

РИС. 5. ▲
Пример организации сети с централизованным управлением и аппаратным контроллером

РИС. 6. ▼
Общая стоимость оборудования на примере Wisnetworks

По пропускной способности:

Минимум 3 Мбит/с на абонента
15% пользуются одновременно (900 чел.)
31 клиент на точку
30 точек доступа



ТРИ ВАЖНЫХ ВОПРОСА НА ПУТИ СОЗДАНИЯ ИНТЕЛЛЕКТУАЛЬНОГО НЕФТЯНОГО МЕСТОРОЖДЕНИЯ

ИВАН ЛОПУХОВ
ivan.lopukhov@moxa.com

Цены на нефть падают, а цены на обслуживание добывающего сектора, наоборот, растут, из-за чего страдает экономика нефтедобывающих стран, в значительной степени зависящих от добычи нефти. Однако существует возможность повысить эффективность разработки нефтяных месторождений, используя уже существующие сети на устье скважины, — благодаря интеллектуальным системам.

ВВЕДЕНИЕ

По сравнению с 2014 г. цены на нефть упали на 50%, поэтому нефтяным компаниями приходится сокращать заработные платы, чтобы внедрить современные технологии. На площадках нефтедобычи очень важно, помимо вопросов безопасности и устойчивости системы, учитывать преимущества обработки информации с полевых устройств, а также с Ethernet- и беспроводных сетей. Компании, работающие в сфере нефтедобычи, постоянно ищут способы сокращения затрат на автоматизацию устья скважины, стараясь при этом соблюсти меры безопасности, которые так важны для нефтегазовой отрасли.

Существует три основных фактора, влияющих на реализацию интеллектуальных сетей на нефтяных месторождениях:

- безопасность;

- модернизация устаревших систем;
- обработка данных в режиме реального времени.

За исключением некоторых аспектов безопасности, данные факторы направлены на достижение сокращения издержек производства и увеличение эффективности работы компании.

На сегодня в интеллектуальных системах нефтяных месторождений все больше внедряются промышленные сети и беспроводные преобразователи.

Из-за низких цен на нефть для большей части промышленности необходимы новые способы получения максимального результата от уже существующих сетей на устье скважины. Достичь этого стало возможным благодаря беспроводным и Ethernet-сетям в интеллектуальных системах оповещения, внедрению более совершенных средств управления ресурсами и возможности анализа работы основных устройств в режиме реального времени. Ethernet- и беспроводные устройства помогают установить логическую связь между SCADA-системой и датчиками, что обеспечивает максимально расширенное решение по сравнению с устаревшими последовательными сетями.

БЕЗОПАСНОСТЬ

Очень важным фактором при создании интеллектуальной сети на нефтяном месторождении является вопрос безопасности. Широко распространенные Ethernet- и беспроводные технологии, обеспечивающие процессы автоматизации сети, вызывают сомнения в надежности, кибербезопасности и соответствии новым технологиям. Операторы сети понимают, что усовершенствование сети и соединения между устройствами на местах и центром управления способно обеспечить значительную экономию средств и повысить эффективность, но вопрос остается открытым: безопасно ли это?

Благодаря промышленным маршрутизаторам, беспроводным и периферийным системам контроля и резервирования, управление основными средствами сети значительно улучшилось, что обеспечивает максимальную степень надежности сети, являющейся важным условием для большинства операций на нефтяных месторождениях.

Резкое падение цен на нефть заставило компании сократить все малоэффективные части систем. Это стало толчком для перехода от простых последовательных сетей к интеллектуальным расширяемым сетевым технологиям. В связи с чем многие нефтяные компании осознали, что промышленные сетевые технологии, такие как промышленные маршрутизаторы и беспроводные преобразователи, не просто предлагают больше инструментов для повышения эффективности производства, но и обеспечивают максимальную безопасность в эксплуатации. Кроме того, поставщики промышленного оборудования предлагают готовый или почти готовый функционал для внедрения в существующие распределенные системы управления (DCS) или SCADA-системы. Промышленные беспроводные технологии и преобразователи позволяют осуществлять удаленное управление и контролировать состояние всех устройств на периферии сети. Сигналы аварийной сигнализации и не соответствующие норме данные со скважины могут быть отображены в режиме реального времени, что значительно снизит риски выхода системы из строя. Технология промышленной маршрутизации связывает между собой операции от центра к центру, поддерживая надежную защиту межсетевого экрана в сочетании с расширенной полосой пропускания для потенциального подключения вспомогательных средств.

Для предотвращения человеческих ошибок и облегчения интеграции новых устройств в существующую SCADA-систему должны быть обеспечены создание развернутой интеллектуальной сети периферийных устройств и готовая для эксплуатации система. Кроме того, необходимо найти поставщика, который сможет предложить промышленный маршрутизатор с пропускной способностью до 500 Мбит/с, чтобы сеть поддерживала увеличение количества устройств в будущем и работу сети с высокой пропускной способностью — например, сети видеонаблюдения на удаленных объектах устья скважины. Сочетание простоты использования и поддержки VPN/Firewall/NAT обеспечит надежность интеллектуальной сети на нефтяных месторождениях. Компания Moxa предлагает серию универсальных защищенных промышленных маршрутизаторов (рис. 1).

МОДЕРНИЗАЦИЯ УСТАРЕВШИХ СИСТЕМ

Если бы после падения цен на нефтяном рынке в 2015 году появился бы хоть один положительный результат, было бы интересно посмотреть, как он повлиял бы на отрасль в вопросе улучшения эффективности существующих процессов. Это привело к появлению и увеличению использования Ethernet-сетей и беспроводных технологий для модернизации устаревших DCS-сетей, что позволило улучшить управление ресурсами и расширить применение основного оборудования. Согласно исследованию, проведенному в 2015 году компанией Cisco Consulting Services, «80% компаний нефтегазового сектора увидели, что большая часть роста инвестиций происходит за счет улучшения операционной эффективности существующих проектов и резервов с исполь-

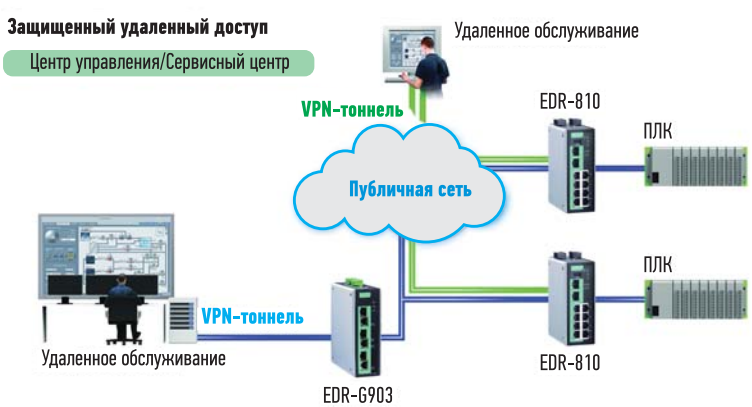


РИС. 1. Обеспечение надежности интеллектуальной сети с помощью защищенных промышленных маршрутизаторов Moxa

РИС. 2. Преобразователь протоколов Моха

зованием интеллектуальных сетевых технологий как центрального средства максимальной рентабельности инвестиций в автоматизацию устья скважин в данный момент»[1].

Управление ресурсами и модернизация устаревшей системы являются одними из самых важных факторов, отличающих успешные компании от неуспешных. Промышленные беспроводные и Ethernet-сети создают возможность управления и контроля ресурсов на периферийных участках устья скважины с учетом ограниченных средств на развертывание и небольшого штата сотрудников. Более того, внедрение и увеличение числа беспроводных и Ethernet-устройств обеспечивают совместимость с различными сетевыми протоколами, таким образом максимально расширяя параллельную разработку сенсорных технологий и IP SCADA. Доступ к протоколам периферийных устройств может быть увеличен благодаря преобразователю протоколов компании Моха (рис. 2).

В современных нефтяных системах устаревшие устройства используют различные интерфейсы, в том числе цифровые входы/выходы (DIO), RS-232/422/485, Ethernet и USB. Если поставщик сетевых решений предлагает сетевое подключение, учитывающее подобные интерфейсы, гораздо проще расширить уже существующую инфраструктуру DCS-сети.

Например, связь между полевым управлением и датчиком уровня часто теряется, прерывая передачу данных между диспетчерской и всеми счетчиками на каждой скважине, насосе и нефтепроводе. Важная информация со счетчиков на устье скважины часто бывает полезна только на месте, поэтому можно с помощью удаленного доступа ограничить анализ в режиме реального времени и управление операциями на устье скважины. Этот сценарий объясняется тем, что большинство ведущих производителей средств автоматизации вложили значительные средства в развитие SCADA и сенсорных технологий, игнорируя связь между ними. Данные в огромных количествах получаются и генерируются на уровне периферийных устройств и на каждом устье скважины. Технологии SCADA на уровне центра управления становятся более эффективными, аналитическими и прогрессивными. Однако из-за невозможности с минимальными затратами развернуть линию связи с уже существующими между SCADA-системой и датчиками сетевыми протоколами в условиях ограниченного пространства, главной задачей, существовавшей еще до появления промышленных сетей, является альтернативный путь модернизации устаревших DCS-систем.

Сегодня на чрезвычайно активном рынке нефти, как правило, невозможно найти способ обновления всей сети целиком. На площадках старых нефтяных месторождений изменения системы DCS должны происходить постепенно и продуманно, с использованием промышленных беспроводных устройств и интеллектуальных Ethernet-преобразователей. Уделив пристальное внимание инвестициям в промышленные сети, можно помочь операторам подключить все устаревшие устройства друг к другу и к центру управления. В частности, установка дополнительных ретрансляторов на устье скважины позволит максимально быстро разместить устройства сети в местах, еще не подключенных к сети, что значительно сэкономит время и расходы на ввод в эксплуатацию и дальнейшее обслуживание.

ОБРАБОТКА ДАННЫХ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ

В отличие от линейных систем связи, предназначенных для передачи данных и измерения электроэнергии, системы нефтегазовой области перегружены информацией. В условиях высоких нагрузок, экстремальных температур, необходимости защиты очистных сооружений и высоких темпов производства большое значение на стадии добычи нефти имеет объем данных, генерируемых ежеминутно. Поэтому было очень важно найти способ и средства для подключения источника этих данных, датчика, к управляющей SCADA-системе.

В системах нефтяных месторождений сведения генерируются на уровне датчиков с ограниченными режимами передачи от самого устройства к центру управления. Режимы передачи данных варьируются от ограниченной передачи до отчета на месте, написанного от руки. Аналогичным образом передача данных в морских системах зависит от сигнала спутниковой связи, порой процесс передачи, сбора и обработки информации может занимать несколько дней. Словом, интеллектуальные нефтяные системы — это не слишком новая концепция, использующая созданные и протестированные способы подключения.

В проведенном в 2015 году опросе ведущих нефтегазовых компаний 48% респондентов обозначили понятие «данные» как основную область, требующую улучшений, для эффективного использования технологий связи[2].

Для продуктивного управления постоянно увеличивающейся нагрузкой данных, производимых интеллектуальными датчиками на нефтяных месторождениях, необходимо применять эти сведения для создания команд в режиме реального времени. Только промышленная сеть может поддерживать обработку данных в реальном времени. Компания Моха и другие компании, работающие в промышленном секторе коммуникационного оборудования, создают для интеллектуальных месторождений нефти устройства, которые позволяют соединить решения прикладного уровня с большим количеством датчиков, распределенных по всей территории нефтяного месторождения.

ИНТЕЛЛЕКТУАЛЬНАЯ МОДЕЛЬ ЗАВЕРШЕННОСТИ НЕФТЯНОГО МЕСТОРОЖДЕНИЯ

Концепция интеллектуального нефтяного месторождения — это технология, которая, как правило, гораздо более эффективна и безопасна, чем обычные системы, опирающиеся исключительно на последовательную связь и соединение по полевой шине.

[1] Новая действительность нефтегазовой отрасли. Cisco, апрель 2015 г.
[2] Новая действительность нефтегазовой отрасли. Cisco, апрель 2015 г.

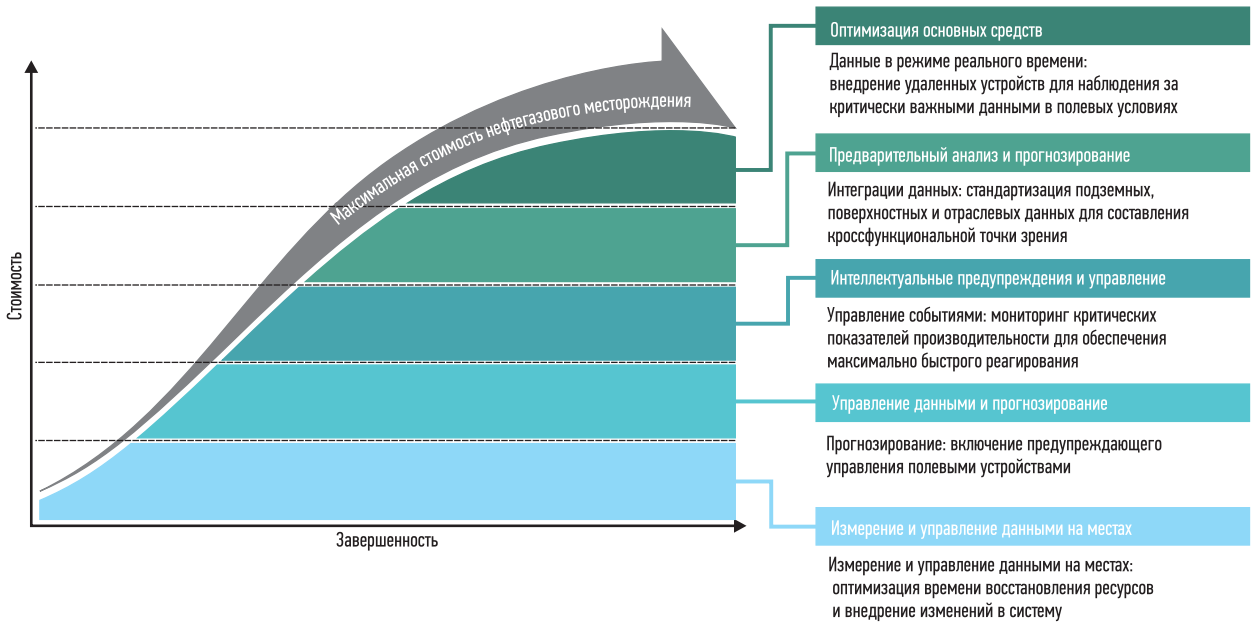


РИС. 3. ▲ Модель завершенности приборного обеспечения процесса (IBM Center for Applied Insights)

Традиционное нефтяное месторождение, будь оно маленькое, среднее или большое, изобилует датчиками системы и клапанами управления, производящими огромные потоки данных каждую минуту.

Лидеры отрасли и системные операторы месторождения задаются вопросом, как безопасно и надежно можно использовать эту информацию для снижения себестоимости добычи и увеличения объемов:

- Если бы эти данные могли быть безопасно получены, объединены и проанализированы в режиме реального времени, могли бы они надежно связать мою SCADA-систему с полевыми устройствами?
- Если я создам беспроводную и Ethernet-сеть в рамках существующей DCS-системы, смогу ли я продлить срок службы удаленных устройств?
- Сможет ли это помочь мне повысить производительность при более низких эксплуатационных расходах и сократить время восстановления системы после сбоев?
- И наконец, оправдает ли это вложенные средства?

Ответы на все вопросы — да. Тем не менее проблемы внедрения интеллектуальных систем связи в сфере нефтедобычи заслуживают нашего внимания.

IBM Center for Applied Insights наглядно демонстрирует этот момент в своей модели завершенности приборного обеспечения процесса, в которой отражена максимальная окупаемость инвестиций для получения средств, расширения и оптимизации основного оборудования[3] (рис. 3).

Инвестиции в современные контрольно-измерительные технологии и сенсоры не обеспечат ожидаемой рентабельности, если данные не будут доступны в приложении или на уровне управления операциями. Постепенно увеличивая способность собирать информацию с месторождения, интеллектуальная система должна научиться ее интегрировать, а также переводить в события и оповещения. Также должна быть возможность на описанном уровне запросить и зарегистрировать данные для анализа и составления модели на контрольном уровне. Только на этом этапе может быть достигнута максимальная оптимизация основных средств.

БОЛЬШЕ ИНТЕЛЛЕКТА — БОЛЬШЕ РЕЗУЛЬТАТ

Лидеры нефтедобывающей отрасти, как крупные, так и мелкие, прекрасно осознают преимущества интеллектуальных систем на месторождениях и инвестиций в технологии промышленного «Интернета вещей» (IIoT) в данной отрасли. Например, по сведениям компании Shell oil, в период с 2002 по 2009 год, благодаря внедрению интеллектуальных технологий на 50 нефтяных месторождениях, прибыль достигла $5 млрд. В 2010-м компания Chevron внедрила в свою систему собственную интеллектуальную технологию iField, что привело к экономии на эксплуатационных затратах на 2–8%[4].

Согласно Oxford Economics, «внедрение технологии IoT в нефтегазовую промышленность может увеличить глобальный ВВП на 0,8% ($816 млрд) к 2025 году[5].

Одновременно с понижением цен на нефть и дальнейшим развитием беспроводных и Ethernet-сетей такие компании, как Moxa Inc., расширяют возможности нефтедобывающего сектора, предлагая устройства для преобразования существующих последовательных сетей, в частности Modbus TCP, в сети PROFINET, 3G, 4G Wi-Fi и Ethernet. Расширение сетей нефтяных скважин с применением периферийных устройств стало более доступным и быстрым, чем когда-либо раньше, благодаря надежным промышленным беспроводным технологиям. Интеллектуальная система нефтяного месторождения сейчас становится осознанной необходимостью, ведущие нефтяные и газовые компании рассматривают переход на интеллектуальные системы как средство сокращения операционных расходов. ⬣

[3] Производительность наиболее интеллектуальных месторождений нефти и газа. IBM Center for Applied Insights, 2015.

[4] Специальный отчет на конференции Intelligent Energy. Digital Energy Journal, 23–25 марта 2010 года.

[5] Новая действительность нефтегазовой отрасли. Cisco, апрель 2015 г.

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ НА НЕФТЯНЫХ МЕСТОРОЖДЕНИЯХ: ПРИМЕРЫ

ИВАН ЛОПУХОВ
ivan.lopukhov@moxa.com

Для управления процессами операторы буровых установок используют панельные компьютеры с уровнем защиты IP66, что обеспечивает интеллектуальную автоматизацию и мониторинг системы на нефтяных месторождениях даже в суровых условиях тундры провинции Альберта (Канада). Две сотни морских платформ в Аравийском море отправляют данные на центральный сервер на материке, чтобы из офисов, находящихся за много миль, вести наблюдения, диагностику и контроль за полевыми устройствами. На удаленных нефтяных скважинах, расположенных высоко в Скалистых горах Колорадо (США), сотовая связь и информационные технологии, предназначенные для автоматической передачи сведений операторам и менеджерам, оповещают об изменениях в процессах и чрезвычайных ситуациях, позволяя вести дистанционное управление с помощью смартфонов, планшетов и ноутбуков.

Во всех трех случаях данные о силе напора насоса, уровне жидкости в резервуаре, а также информация с датчиков трубопровода, с датчиков давления и температуры и устройств ввода/вывода передается на центральный сервер и в диспетчерский пункт на расстоянии в несколько миль. Сведения с локальных и удаленных систем сопоставляются и анализируются для того, чтобы обеспечить всестороннее видение ситуации в режиме реального времени. Доступ к каждому отдельному устройству осуществляется через сотовую сеть.

Удаленные данные и команды управления могут быть собраны и переданы с помощью мобильных транспортных средств управления, свободно перемещающихся по всему региону в центральный офис, который может быть расположен далеко от континента. Инициируемые событиями видеопотоки обеспечивают в режиме реального времени оперативную оценку произошедших событий, в то время как полные хронологические отчеты по данным всех датчиков сохраняются и анализируются. Инженеры на местах и руководители подразделений получают уведомления о критических событиях с помощью SMS или электронной почты, и каждый может иметь доступ к удаленным видеотрансляциям и показаниям датчиков посредством любого устройства, подключенного к Интернету, — смартфона, ноутбука или планшета (рис. 1).

В ЧЕМ ЗАКЛЮЧАЕТСЯ «ИНТЕЛЛЕКТУАЛЬНОСТЬ» МЕСТОРОЖДЕНИЯ?

Основной задачей интеллектуальной сети нефтяного месторождения является сбор и передача огромных объемов данных от десятков тысяч устройств, поэтому очень важно обеспечить надежную беспроводную связь, сохранить целостность информации и безопасность передачи. Решить подобную проблему удалось благодаря недавним достижениям в широко распределенной, высокопроизводительной, резервированной системе сбора данных и управления процессами. Распределение вычислительной мощности по всей сети позволяет передавать сведения гораздо быстрее, безопасно их сопоставлять и обрабатывать, территория сбора данных стала более обширной, чем это допустимо в централизованной архитектуре сети. Распределение упрощает коммуникации, повышает скорость, чувствительность сети и надежность за счет резервирования в случае аварии на каждой станции. Увеличиваются масштабы применения и мобильность: выгода буквально неизмерима.

БУДУЩЕЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ НА НЕФТЯНЫХ МЕСТОРОЖДЕНИЯХ

Движущей силой интеллектуальных систем на нефтяных месторождениях является стремление производителя интегрировать систему контроля над распределенной системой управления (DCS), состоящей, как правило, из множества несовместимых устройств от разных поставщиков. Такая система автоматизации содержит сенсоры и приводные устройства, подключенные к магистральным коммутаторам и операторским панелям (HMI), расположенным и на периферии, и в центре сети. Если создать такую сеть с использованием технологии Ethernet, можно контролировать основную систему дистанционного управления, одновременно увеличив возможность подключения множества устройств и скорость самой системы.

Например, бесчисленные счетчики, установленные в постоянно расширяемой береговой сети скважин, отвечают за предоставление данных, необходимых для принятия решений по управлению сетью. С распространением высокоскоростных Ethernet-сетей (HSE) в системах нефтяных месторождений типичные для нефтегазовой отрасли DCS-системы стали еще более автоматизированными и интеллектуальными, но что если можно добиться гораздо большего? Что если полевые датчики смогут предсказывать отказ устройств и способы улучшения и прогнозирования качества и состава нефти? Что если каждый конечный датчик, привод, счетчик или двигатель были бы доступны для центрального сервера по отдельности, предоставляя данные в режиме реального времени, принимая оперативные решения на каждом уровне — от производства до управления основными средствами?

Благодаря информации с датчиков, которая автоматически обрабатывается непосредственно на месте, мы можем получить наиболее точные данные о запасах нефти, требованиях к производительности и ресурсах оборудования. Следовательно, возможность установить неисправность в процессе работы устройств значительно возрастает, управление и использование основных средств увеличены до максимума, благодаря чему реализована совместимость DCS-систем, к которой так долго стремились нефтегазовые компании. Все это позволит избежать критических отказов системы.

ПРИМЕР 1. КОНСОЛЬ УПРАВЛЕНИЯ В РЕЖИМЕ РЕАЛЬНОГО ВРЕМЕНИ НА БУРОВОЙ УСТАНОВКЕ

В интеллектуальных системах на нефтяных месторождениях все коммуникации должны быть настроены параллельно друг другу для того, чтобы гарантировать возможность не только резервирования и надежной передачи данных от периферии к центру, но и резервирования устройств (или станции) внутри системы. Устройства ввода/вывода, расположенные как на периферии сети, так и в центре, должны быть устойчивы к одиночным отказам терминалов

РИС. 1. ◄ Интеллектуальные системы нефтяных месторождений: данные передаются между устройствами и в центр управления, что позволяет достичь ощутимых результатов производителям нефти и газа по всему миру

ТАБЛИЦА. УРОВНИ СИСТЕМЫ УПРАВЛЕНИЯ БУРОВОЙ УСТАНОВКОЙ

Периферийный уровень	Связанные между собой программируемые контроллеры поддерживают возможность отправки сигнала тревоги, push-уведомлений, автоматической обработки данных и другие режимы работы для раннего анализа, интеллектуального предупреждения и быстрого реагирования на изменения физической целостности устройств и в окружающей среде.
Уровень преобразования данных	Информация преобразовывается для передачи с помощью SCADA-системы, локального компьютера, HMI-интерфейсов или Ethernet-сети к удаленному центру управления.
Уровень основной базы данных	Здесь данные с удаленных устройств ввода/вывода и HMI-интерфейсов хранятся, анализируются и оцениваются.
Уровень HMI	Команды оператора передаются на буровые устройства, а подпрограммы контролируются и подвергаются оценке.

(RTU). Поскольку буровая установка всегда находится на периферии, она послужит хорошим примером того, как системы должны взаимодействовать и усиливать друг друга. Уровни системы представлены в таблице.

Описание системы

Система на буровой установке (рис. 2) должна информировать операторов обо всех данных, необходимых для правильного, эффективного и непрерывного процесса. Центральная операторская HMI-панель в системе буровой установки — это место, в котором объединены и отображены все системы, источники энергии, центр управления двигателем, буровой насос, скважина и опора башенного типа. Отказ любой из этих систем приведет к остановке всего процесса, сбой в любой из них — к ошибкам в других или к серьезной потере производительности.

Силовые приводы и сенсоры в подсистемах могут быть стационарными, передвижными или временными, могут контролировать среду на местах и для каждого отдельного устройства и, как правило, входят в состав SCADA-систем. Впоследствии данные возвращаются к оператору и либо сопоставляются, сохраняются и передаются, либо преобразовываются для отправки на другие устройства сети. По мере продвижения данных от устройств сети к центру управления по региональной сети будет происходить их поэтапный анализ. Между тем все сведения, обработанные на местах, должны отобразиться на операторской панели, что позволит мастеру на буровой установке быстро оценить общую ситуацию в сети.

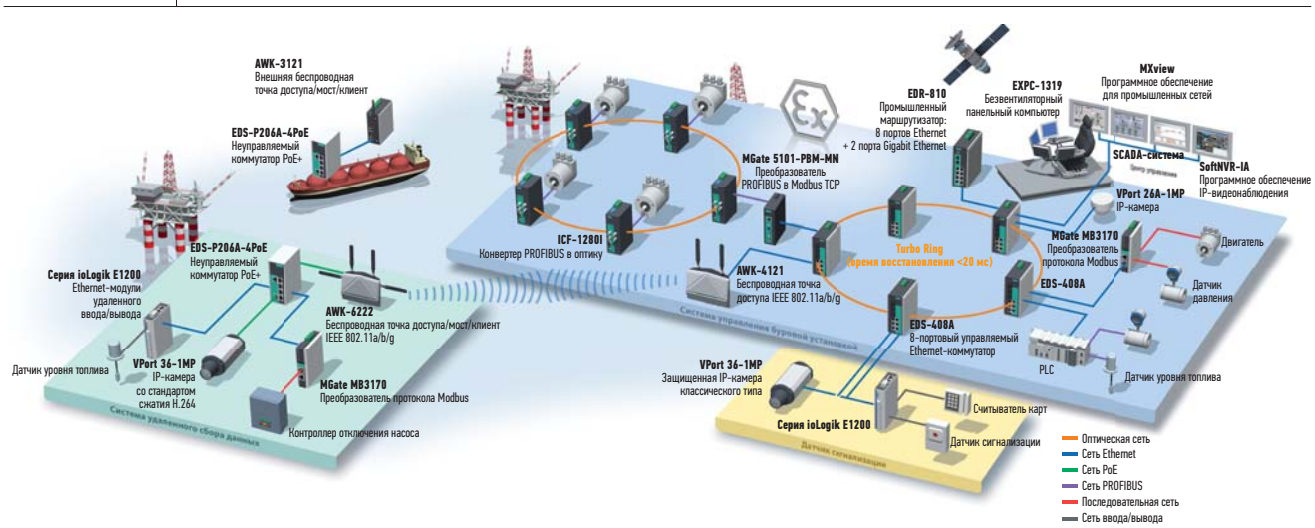
Особенности системы

В системах управления буровыми установками должны быть предусмотрены комплексные сетевые и вычислительные устройства с возможностью резервирования, высокой производительностью и функциональной совместимостью. В качестве основного интерфейса, посредством которого происходит взаимодействие между оператором и сетью, должны использоваться надежные, проверенные решения HMI, поддерживающие различные промышленные коммуникационные интерфейсы.

Разнообразие интерфейсов необходимо для интегрирования различных устаревших устройств и протоколов в HMI-систему. Вполне вероятно, это будут датчики и устройства RTU, обменивающиеся данными по последовательным, RS-422/482/485- и Modbus-протоколам (возможно, потребуются Ethernet-преобразователи); беспроводные устройства сотовой связи или Wi-Fi; IP-камеры для записи процессов на скважинах и установках; программируемые контроллеры для подключения приводов и датчиков. Большинство из этих устройств отправляет информацию по коммутируемым каналам связи, по крайней мере в два места: основному компьютеру и резервному устройству, которое используется в качестве основного сервера для долговременного хранения базы данных.

Приоритетной задачей является создание SCADA-системы с портами для подключения устройств RS-232/482/485, цифрового ввода/вывода и Ethernet, подходящих для реализации приложений промышленной автоматизации и IT с протоколами Modbus, PROFIBUS, SNMP, ONVIF и другими. Преобразователи и программируемые контроллеры

РИС. 2. ▼ Консоль управления в режиме реального времени на буровой установке



нужно настроить с помощью OPC-сервера для работы в Ethernet-сети. Кроме того, современная OPC-система должна поддерживать связь с удаленными устройствами сети, устраняя излишние затраты и задержки, к которым приводит опрос сети.

Все решения, размещенные на буровых установках, должны соответствовать стандарту C1D2/ATEX Zone 2, а если они находятся в морских системах (например, на подводных и морских платформах), то также должны быть сертифицированы по стандарту DNV и ABS. Еще одним требованием к устройствам является расширенный температурный диапазон, чем он больше, тем лучше: промышленный диапазон –40...+75 °C надежен в любых климатических условиях, за исключением самых экстремальных.

ПРИМЕР 2. МОНИТОРИНГ МОРСКИХ СКВАЖИН — ПРОЦЕСС ПЕРЕДАЧИ ДАННЫХ ОТ ПЕРИФЕРИИ К ЦЕНТРУ

Большая часть данных в традиционных сетях отсортировывается, поскольку они часто находятся в дискретных распределенных сетях, в отличие от которых интеллектуальные системы на нефтяных месторождениях созданы для того, чтобы гарантировать передачу и хранение данных. В примере 1, представленном выше, мы описали ключевые элементы достаточно ограниченной автономной подсистемы нефтяного месторождения. Сбор сведений на местах обеспечивает более высокую общую надежность и контроль с помощью обработки всех полученных данных в режиме реального времени. Скорость и эффективность передачи, а также распределенный анализ и обработка данных со всей WAN-сети являются двумя самыми важными задачами. Для иллюстрации подобных задач рассмотрим морскую сеть мониторинга в Аравийском море.

Введение в систему

Эта интеллектуальная система на нефтяном месторождении представляет собой обширную сеть и содержит множество платформ, расположенных на большой территории. Задача состоит в обработке большого количества данных, собираемых с каждой платформы. Оптоволоконная линия связи, используемая для передачи информации на большие расстояния, формирует магистральный канал от морской платформы к береговому центру управления. Беспроводная сеть применяется только для локального сбора данных на морских платформах и вокруг них, после сбора с удаленных устройств ввода/вывода сведения передаются по оптоволокну к центру. Оптоволоконные линии связи проходят от устья скважины через морские и присоединенные к ним платформы, на которых предусмотрено резервное копирование данных. Такие промежуточные платформы помогают собирать и обрабатывать большие объемы данных с различных платформ, включающих несколько видеопотоков с каждой станции.

Особенности системы

Связующие платформы поддерживают передачу аварийных и других сигналов и способны запускать противопожарную систему (FAS), резервную, аварийную (ESD) и систему остановки технологического процесса (PSD) для всего участка месторождения. Данные платформы дополнительно сортируют, обрабатывают вновь поступившие сведения, которые они получают от нескольких платформ устьев скважины, и пересылают их дальше по сети, например на компрессорную станцию или в центр управления (рис. 3).

Для реализации такой задачи обработка удаленных устройств ввода/вывода осуществляется с помощью программируемых контроллеров, управляющих большим количеством датчиков, расположенных в различных точках сети. Преобразователи протокола Modbus передают данные от удаленных устройств как на локальные, так и на связующие платформы HMI. Видеокамеры обеспечивают круглосуточное наблюдение за станциями на устьях скважины и связующими платформами в режиме реального времени 24×7. Все эти устройства должны быть сертифицированы по стандарту ATEX Zone 2 и эффективно защищены надежным межсетевым экраном.

В случае чрезвычайных ситуаций удаленные программируемые контроллеры отвечают за запуск последовательных событий, которые приведут к аварийному отключению или остановке процесса, что делает эти контроллеры главными устройствами защиты от сбоев в сети. Кроме того, от подобных устройств зависят анализ и хранение данных, поскольку концепция удаленных устройств и программируемых контроллеров давно выходит за рамки их традиционных ролей.

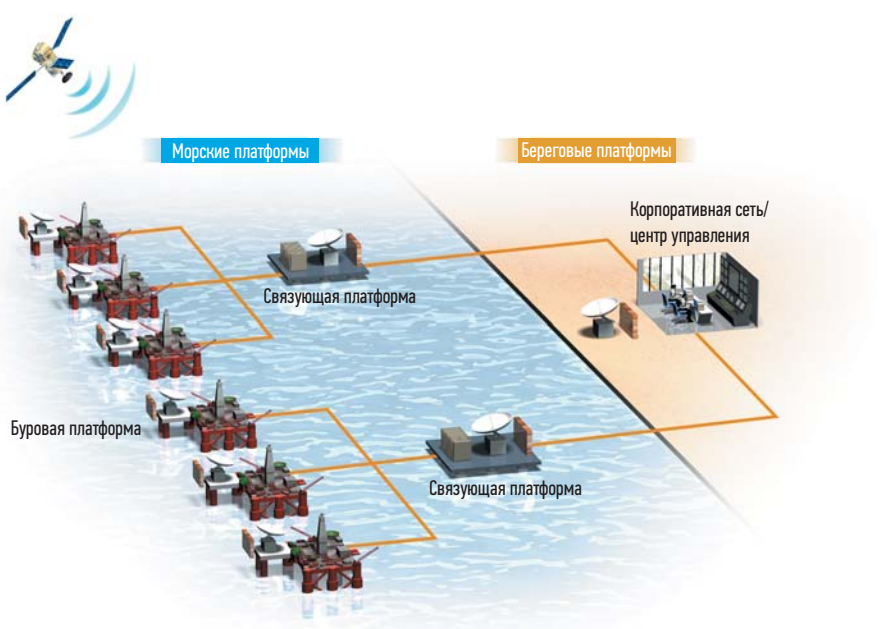


РИС. 3. Морская сеть мониторинга

Аварийные системы и остановка технологического процесса дублируются на связующих платформах, выполняющих тройную функцию: управление сбором данных с нескольких платформ устья скважины, управление платформой и предоставление резервных каналов связи. Решение об аварийном отключении принимается за миллисекунды в режиме реального времени, система будет работать 24×7, 365 дней в году, причем на первом месте стоит целостность данных, их быстрая обработка и передача. Таким образом, все связующие платформы должны быть резервированными, с высоким уровнем безопасности и несколькими маршрутами для передачи данных.

ПРИМЕР 3. УДАЛЕННЫЙ КОНТРОЛЬ И СБОР ДАННЫХ С НЕФТЯНЫХ СКВАЖИН

Введение в систему

Компания Terra Ferma — системный интегратор, осуществляющий дистанционное видеонаблюдение и сбор данных на устьях скважины, расположенных на территории Скалистых гор штата Колорадо. Каждая система устья скважины состоит из устройств автоматической регистрации, мониторинга и управления данными, связанных сотовыми каналами с центральным сервером и центром управления на расстоянии в несколько миль (рис. 4). Сенсоры и IP-камеры на станции контролируют солнечные и ветряные генераторы, условия на устье скважины, оборудование и температуру окружающей среды. Журналы данных, видео в режиме live, инициируемые событиями, и полные отчеты должны быть доступны с помощью проводной и беспроводной Ethernet-сети, доступ к которой осуществляется со смартфонов, планшетов и ноутбуков, что позволит операторам иметь доступ к данным центра управления, где бы они ни находились.

Особенности системы

Программируемые контроллеры, установленные на устье скважины, служат интеллектуальными удаленными устройствами, они регистрируют в режиме реального времени и сохраняют данные о давлении, скорости потока и температуре, а затем отправляют их на пульт дистанционного управления для принятия мер или анализа. Эти устройства способны передавать операторам сети аварийные сигналы по SMS или email, используя сотовые сети, в тот момент, когда происходит отклонение в производственном процессе. Центр управления получает сведения от защищенных IP-камер (UL Class 1, Division 2) с помощью сотового модема, автоматически сохраняет изображения и видео на сетевом сервере и отправляет их в диспетчерский центр HMI, когда происходят определенные типы событий. Наконец, используя оборудование одного производителя для объединения устаревшей SCADA-системы и системы удаленного мониторинга и управления, заказчик избегает лишних затрат на приобретение дополнительного сетевого оборудования и на значительное время простоя системы.

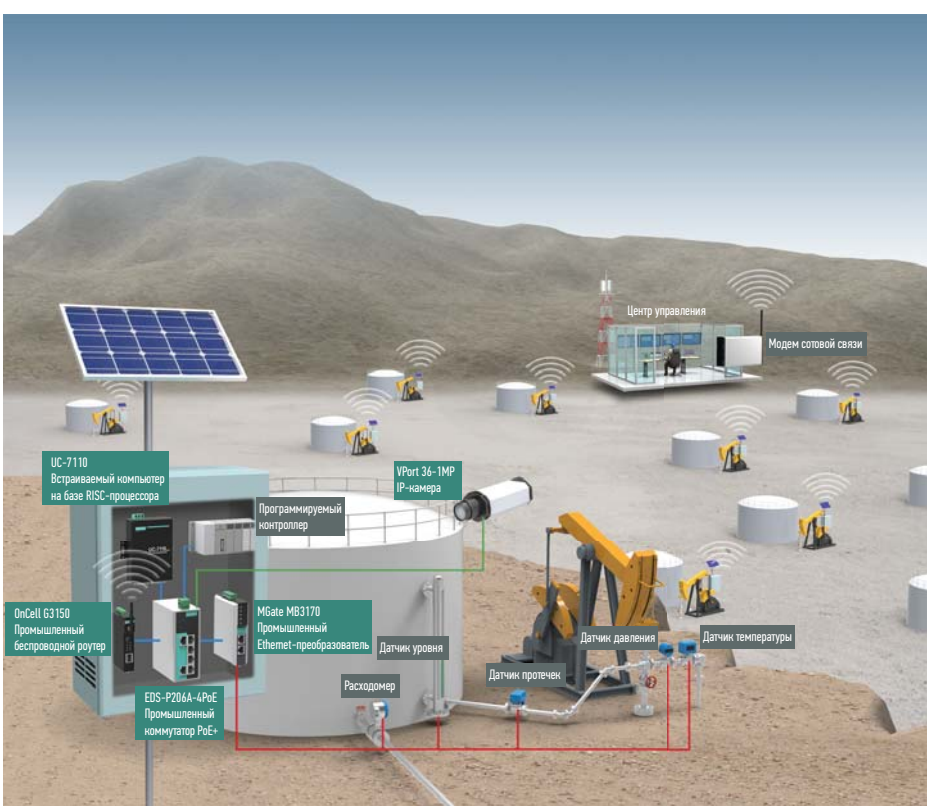


РИС. 4. ▼ Сбор данных на устьях скважины

ВАЖНОСТЬ ВЕРТИКАЛЬНОЙ ИНТЕГРАЦИИ

Технология интеграции, разработанная для специфичных рынков с вертикальной структурой, — это отличный помощник для разработчиков системы и конечных пользователей. При проектировании интеллектуальной системы нефтяного месторождения оборудование, приобретенное у одного поставщика, дает значительное преимущество в плане разработки сети. Сосредоточив внимание на создании широкого спектра устройств для использования на нефтяных и газовых месторождениях, производители могут гарантировать аппаратную безопасность и надежность за счет дополнительных функций и программного обеспечения для управления сетью.

В настоящий момент компания Моха предлагает широкий спектр устройств, соответствующих стандарту ATEX Zone 2/C1D2, обеспечивающих высокую производительность интеллектуальной системы на нефтяном месторождении. Благодаря последним моделям панельных компьютеров и одобренным для применения в морских системах сетевым и компьютерным решениям, компания Моха может предоставить комплексное решение практически для любой системы на нефтяных месторождениях. ⬣

Wonderware Russia

ИНТЕГРАЦИЯ **БИЗНЕС-ОПЕРАЦИЙ И ПРОИЗВОДСТВЕННЫХ СИСТЕМ В ЕДИНУЮ** ИНФОРМАЦИОННУЮ СИСТЕМУ

HMI/SCADA · Управление производственной информацией · MES/MOM · Промышленный интернет вещей

НЕФТЯНАЯ И ГАЗОВАЯ ПРОМЫШЛЕННОСТЬ

ПИЩЕВАЯ ПРОМЫШЛЕННОСТЬ

МЕТАЛЛУРГИЯ И ГОРНОДОБЫВАЮЩАЯ ПРОМЫШЛЕННОСТЬ

ЭНЕРГЕТИКА

ФАРМАЦЕВТИКА

ХИМИЧЕСКАЯ ПРОМЫШЛЕННОСТЬ

Реклама

Wonderware Russia

САНКТ-ПЕТЕРБУРГ
тел. +7 812 327 3752
info@wonderware.ru

МОСКВА
тел. +7 495 641 1616
info@wonderware.ru

ЕКАТЕРИНБУРГ
тел. +7 343 287 1919
info@wonderware.ru

САМАРА
тел. +7 846 273 95 85
info@wonderware.ru

КИЇВ
тел. +38 044 495 33 40
info@wonderware.com.ua

МИНСК
тел. +375 17 2000 876
info@wonderware.ru

КАЗАХСТАН
тел. +77779994825
sales@wonderware.kz

Klinkmann имеет статус Wonderware Russia и является официальным авторизованным дистрибьютором и центром компетенций Wonderware by Schneider Electric в России

Wonderware Russia

СИСТЕМА ДИСПЕТЧЕРИЗАЦИИ ПРОИЗВОДСТВЕННЫХ ОБЪЕКТОВ ТПП «РИТЭК-УРАЛОЙЛ»

ДМИТРИЙ ЕПИМАХОВ

Статья посвящена описанию проекта по внедрению системы диспетчеризации от компании Wonderware на ТПП «РИТЭК-Уралойл».

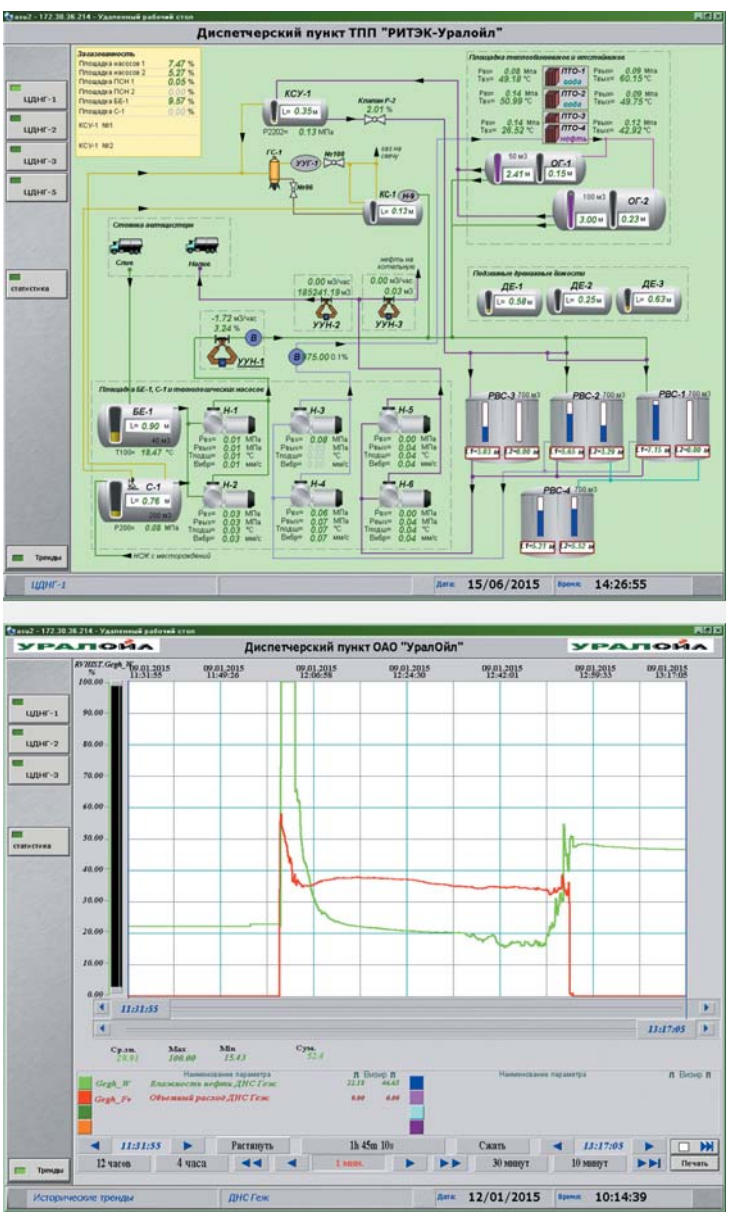


РИС. 1. ▶
Диспетчерский пункт ТПП «РИТЭК-Уралойл»

Акционерное общество «Российская инновационная топливно-энергетическая компания» — АО «РИТЭК» (входит в Группу «ЛУКОЙЛ») создано в 1992 г. В настоящее время «РИТЭК» владеет лицензиями на право пользования недрами с целью поиска, разведки и добычи углеводородного сырья на территории 10 субъектов Российской Федерации.

Причины, которые привели руководство компании к решению о внедрении новой системы диспетчеризации, были следующие:

1. Необходимость существенного расширения системы и хранения большого количества данных. Первоначально система диспетчеризации включала в свой состав два производственных объекта ТПП «РИТЭК-Уралойл», но в дальнейшем количество объектов увеличилось до десятка. Требовались архивы с глубиной хранения не менее года и с количеством хранимых параметров по одному объекту не менее 20 штук.
2. Обеспечение стабильной работы системы диспетчеризации с минимальными вложениями в сопровождение (минимизация операционных расходов).
3. Возможность существенного расширения и развития функционала системы в будущем.

ПОЧЕМУ ВЫБОР ОСТАНОВИЛСЯ НА ПРОДУКЦИИ WONDERWARE?

Проведенный перед выбором анализ программных продуктов для системы диспетчеризации показал, что при использовании программного

обеспечения (ПО) Wonderware System Platform все локальные АРМ на объектах (InTouch классический, т. е. локальный) легко в нее интегрируются.

В итоге получилась система на основе Wonderware System Platform, включающая клиентские интерфейсы на InTouch для System Platform и InTouch классический на местах (рис. 1). Некоторые объекты, которые работали под управлением стороннего ПО, интегрировались в систему посредством применения системы серверов ввода/вывода Device Integration Server.

На данный момент в системе используются:

- System Platform 2014R2, 25K IO/12K History;
- Wonderware InTouch;
- Wonderware InTouch for System Platform with Historian Client.

ОБЛАСТЬ ПРИМЕНЕНИЯ

Система производит сбор информации для архивирования и отображения с объектов:

- сдачи нефти и газа (нефтеперекачивающие станции, коммерческие узлы учета газа);
- крупных установок подготовки нефти;
- ключевых дожимных насосных станций (в основном реконструируемых или перестраивающихся);
- газокомпрессорных станций, осуществляющих сдачу нефтепродуктов в трубопроводы данного и смежных предприятий;
- газотурбинных электростанций.

Основными типами источников данных являются контроллеры FLOBOSS, SCADA PACK, регистраторы «Базис», приборы коммерческого учета ИМ2300, контроллеры ГКС и ГТС, а также программные решения на базе скриптов SQL, применяемые для выгрузок из сторонних систем смежных предприятий (система «Телескоп»).

Не менее важен функционал предоставления точек передачи информации для систем смежных предприятий, например отчетов по сданным нефтепродуктам для предприятий, осуществляющих их транспортировку и переработку. Точки предоставления информации в основном реализованы на стандартных серверах ввода-вывода из пакета Wonderware Device Integration Server.

КОНЦЕПЦИЯ СИСТЕМЫ

Система была разработана для контроля производственных объектов и организации единого защищенного архива с предоставлением отчетности.

В дальнейшем предполагается развертывание системы, которое позволит иметь АРМ в основных производственных отделах (рис. 2): единой диспетчерской службы, производственной службы, службы безопасности, отделах технологов, энергетиков, метрологов.

Также в каждом цехе добычи нефти и газа (ЦДНГ) планируется поставить АРМ оператора пульта управления ЦДНГ с целью координации и контроля работы системы в целом в пределах структуры цеха (рис. 3).

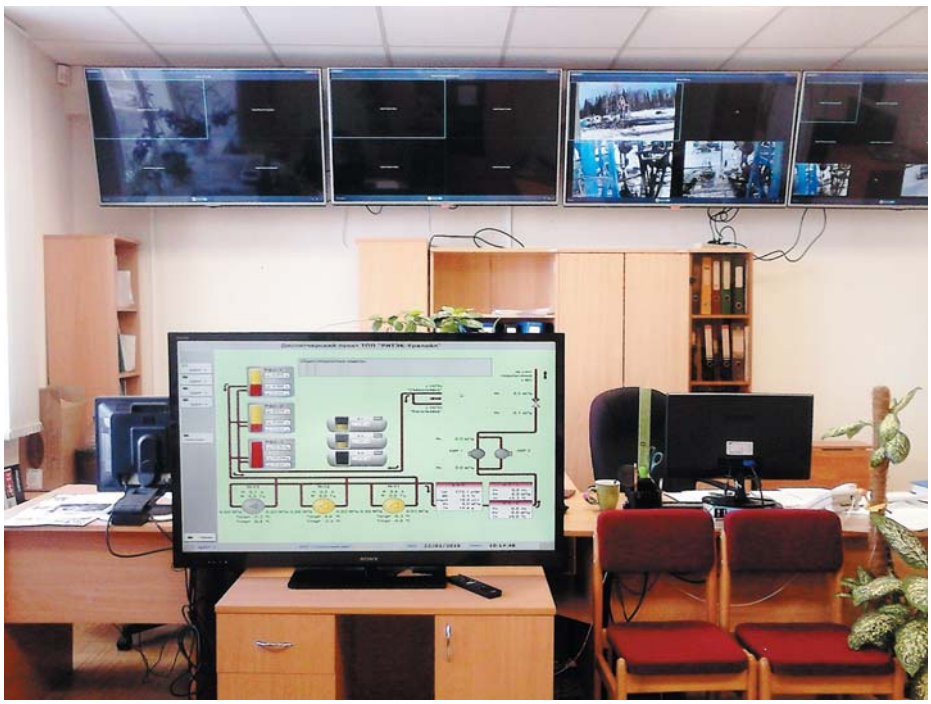


РИС. 2. ▲ Рабочее место диспетчера ЦИТС (единая диспетчерская служба)

РИС. 3. ▼ АРМ оператора пульта управления ЦДНГ

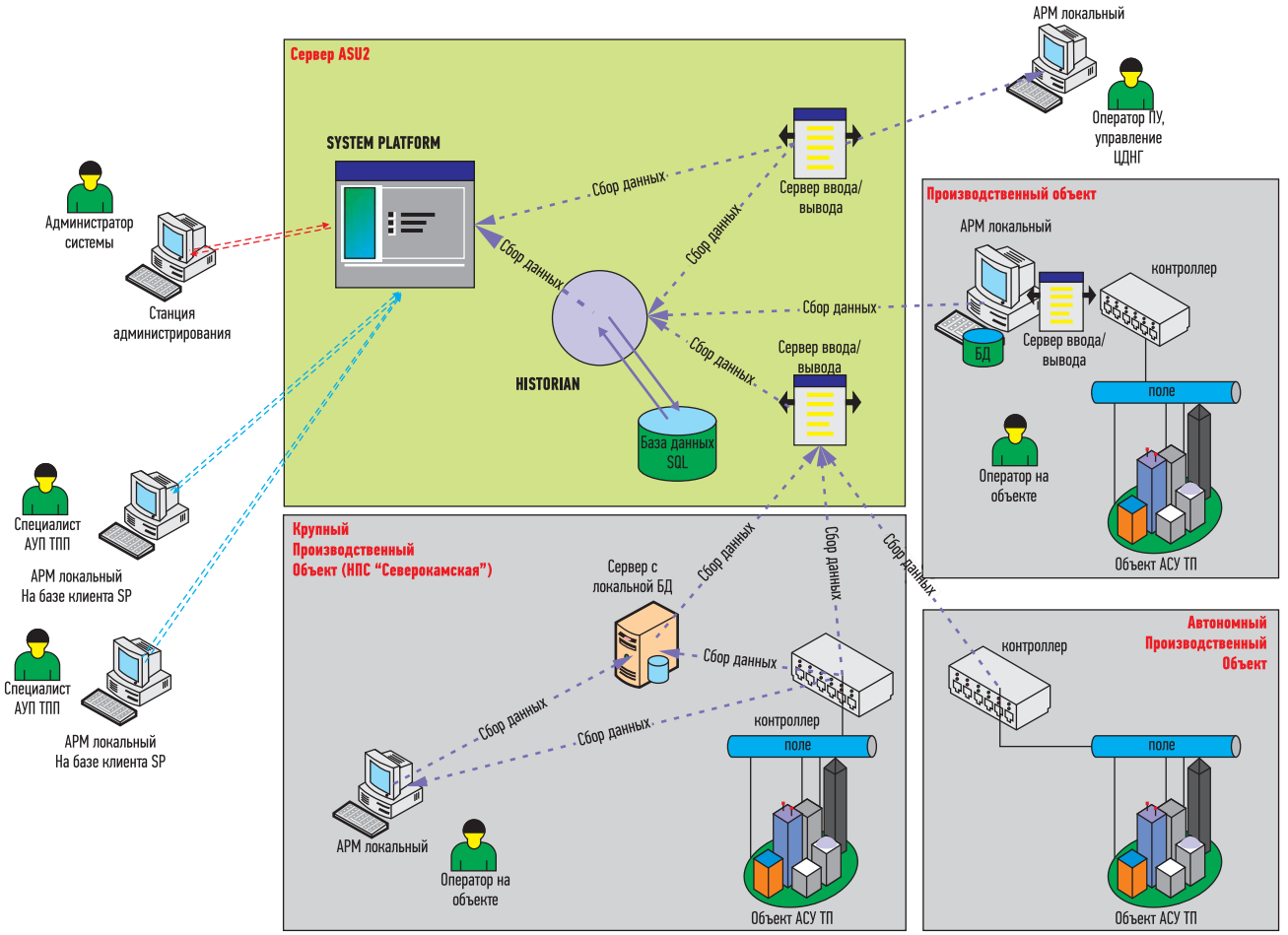


РИС. 4. Схема системы Wonderware с рабочими станциями

Концепция системы включает в себя (рис. 4):

- установку InTouch на каждом объекте, подключаемом к системе (разновидность InTouch — классический или предназначенный для System Platform — определяется наличием и характеристиками канала передачи данных с серверами System Platform);
- установку System Platform (включая сервер архива, Historian) на центральном узле для сбора и отображения информации;
- установку клиентских мест для отображения данных;
- стыковку со смежными системами;
- создание системы отчетности.

ОПЕРАЦИОННАЯ ТЕХНОЛОГИЯ И ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ В ПРОЕКТЕ

Спецификация проекта была составлена совместно с системным интегратором, компанией «Систем-нефтеавтоматика». Исполнители проекта прошли курсы обучения, которые проводят специалисты отдела технической поддержки компании Klinkmann (авторизированного дистрибьютора Wonderware в России).

Первоначально система была реализована на базе интернет-портала и отображала параметры с двух основных объектов, осуществляющих сдачу нефтепродуктов потребителю. В ходе эксплуатации выявилась необходимость соответствия повышенным требованиям по оперативности отображения информации и надежности работы системы, и это послужило основной причиной перехода на Wonderware System Platform с использованием клиентских мест на InTouch/InTouch for SP. В дальнейшем, при реализации новых автоматизированных систем управления (АСУ) или реконструкции существующих они просто интегрировались в общую систему.

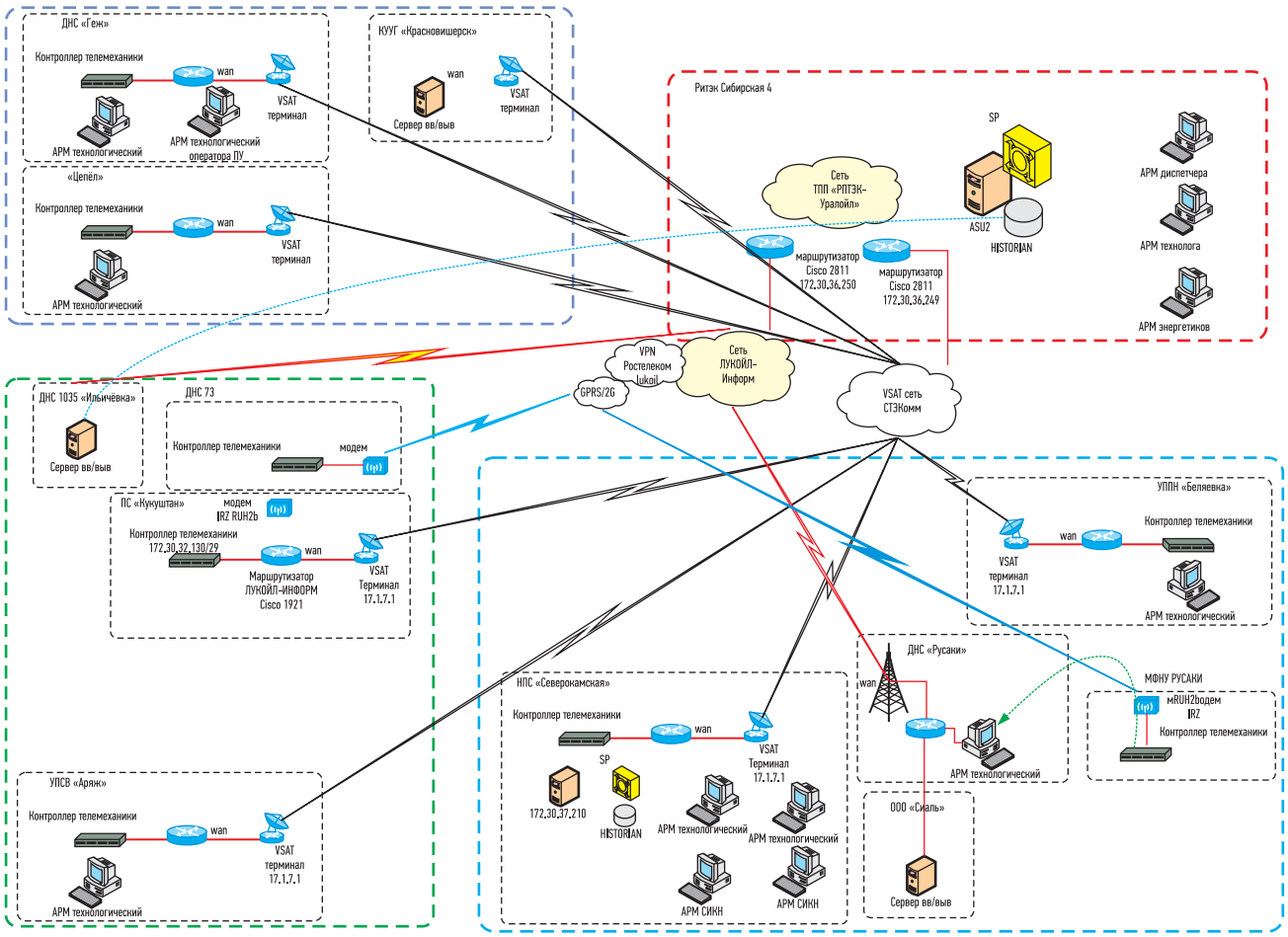
В ходе реализации непрофильного объекта (электрической подстанции 110/35/6 кВ) подрядчиком «АТОЛЛ-М» была выполнена интеграция не только в систему диспетчеризации, но и в АСУ предприятия — поставщика электроэнергии (МРСК Урала). Также в систему диспетчеризации была выполнена интеграция АСУ стороннего предприятия, сдающего нефтепродукт на объект СИАЛЬ.

Еще одним из ключевых моментов проекта было внедрение системы мониторинга удаленных объектов, таких как кусты добычи, через каналы GPRS по сети VPN.

В настоящий момент система включает в себя тринадцать производственных объектов (рис. 5).

РЕЗУЛЬТАТЫ ПРОЕКТА

Применение данной архитектуры позволило вносить изменения и масштабировать систему без существенных затрат. Благодаря обеспечению хранения данных в едином защищенном хранилище



была создана централизованная защищенная система отчетности.

У заказчика также появилась возможность интегрироваться практически в любую АСУ, применяя широкий спектр серверов ввода/вывода и систему запросов SQL. Если перейти к коммерческим преимуществам, то в результате проекта существенно снизился риск нештатных ситуаций на удаленных автономных объектах, что позволило оптимизировать штат обслуживающего персонала, снизить транспортные расходы и объемы по подрядным организациям. Также уменьшилась вероятность экономических потерь от ликвидации внештатных ситуаций.

В качестве примера можно привести ДНС «Геж»: в результате проведенных работ вместо круглосуточно дежурящих оператора пульта управления и двух операторов ООУ остался дневной оператор пульта управления и один круглосуточный оператор ООУ. В целом, если судить по реализованным проектам компании «Клинкманн», применение подобных комплексов позволяет сократить численность персонала на местах на 20–40%.

Кроме того, применение централизованного архива позволяет отслеживать техпроцесс в режиме реального времени, полностью исключая необходимость выезда на объект, а любая нештатная ситуация фиксируется в защищенном архиве без возможности изменения. ⬢

По материалам компании «Клинкманн», официального дистрибьютора Wonderware в России.
Контактный телефон:
(812) 327-37-52
www.klinkmann.ru
www.wonderware.ru

РИС. 5. Схема системы диспетчеризации Wonderware для производственных объектов ТПП «РИТЭК-Уралойл»

WONDERWARE ОТМЕЧАЕТ 30 ЛЕТ ИННОВАЦИЙ

В этом году Wonderware исполнилось 30 лет. Для компании это более 800 000 установленных лицензий на более чем 120 000 промышленных объектах в 130 с лишним странах мира.

Цель Wonderware — создание инновационного и надежного промышленного программного обеспечения, заключающего в себе множество возможностей как для отдельных специалистов, так и компаний любого масштаба.

Обладая широкой базой установленных решений в самых различных отраслях и портфелем продукции с богатым функционалом, компания Wonderware на протяжении десятилетий является одним из лидеров на рынке HMI, SCADA и программного обеспечения для управления операциями в режиме реального времени.

www.wonderware.ru

НПФ «КРУГ»: ОПЫТ АВТОМАТИЗАЦИИ НЕФТЕПАРКОВ И СКЛАДОВ ГСМ

АЛЕКСАНДР ПРОШИН
МИХАИЛ ШЕХТМАН
krug@krug2000.ru

В данной статье рассматриваются вопросы автоматизации нефтехранилищ и складов горюче-смазочных материалов. Приводится опыт использования в подобных системах программных продуктов и программно-технических средств НПФ «КРУГ».

Многие современные технологии основаны на потреблении и производстве горюче-смазочных материалов (ГСМ) и нефтепродуктов. Для обеспечения непрерывности производственной деятельности, создания запасов сырья, топлива и готовой продукции, а также по некоторым технологическим причинам существует потребность в хранении нефтепродуктов. Решение данной задачи обеспечивается созданием складов ГСМ, которые являются частью инфраструктуры предприятий. Несмотря на множество возможных вариантов использования и применения складов ГСМ, их вместимости, типов хранимых нефтепродуктов, все они выполняют несколько основных функций: прием нефтепродуктов на склад, их хранение и отгрузку. Выполнение этих функций с соблюдением современных требований по безопасности, точным и своевременным учетом и минимизацией количества оперативного персонала невозможно без применения автоматизированных систем управления технологическими процессами (АСУ ТП).

В настоящей статье рассматривается опыт создания АСУ ТП складов ГСМ и нефтепродуктов научно-производственной фирмой «КРУГ» (НПФ «КРУГ»), которой в этом году исполнилось уже 25 лет. Фирма «КРУГ» является многопрофильной компанией, которая занимается разработкой, производством и внедрением АСУ ТП для различных отраслей промышленности, включая нефтегазовую отрасль, энергетику, химическую промышленность, теплосети, водоканалы, пищевую промышленность, стройиндустрию и т. д. Со своими партнерами «КРУГ» осуществил более 600 внедрений систем автоматизации. Наряду с созданием АСУ ТП, «КРУГ» является разработчиком программно-технического комплекса (ПТК) КРУГ-2000, который активно применяет в своих работах и проектах партнеров. Помимо программно-технических средств собственной разработки, инжиниринговые подразделения НПФ «КРУГ» используют продукцию таких брендов, как Siemens, Yokogawa, Schneider Electric, Mitsubishi и т. д.

РИС. 1. ▼ Помещение операторной ОАО «Киришинефтеоргсинтез»

Одним из показательных и значимых внедрений АСУ ТП парков нефтезаводов фирмой «КРУГ» является АСУ парком смешения топлив (ПСТ) ПО «Киришинефтеоргсинтез», входящего в ОАО «Сургутнефтегаз». Данный проект выбран в качестве примера не только из-за своей масштабности, но и в связи с большим разнообразием функций, структур, приборов и методов управления, имеющих место в этой системе.

Внедрение АСУ ТП ПСТ началось в 1999 г. с автоматизации узла смешения дизельных топлив. На рис. 1 показано помещение операторной ПО «Киришинефтеоргсинтез». На тот момент АСУ ТП представляла собой шкаф управления (ШУ) с промышленным контроллером и двумя станциями оператора, совмещенными по функциям с серверами базы данных. Проект был выполнен с использованием программно-технических средств КРУГ-2000. Работа данной системы в течение нескольких последующих лет сформировала положительное мнение у заказчика о качестве и надежности применяемых программно-технических средств, и уже в 2001 г. было принято решение

о расширении данной системы подсистемой автоматизации узла смешения бензинов в составе трех ШУ с контроллерами, где впервые на данном заводе была применена технология смешения топлив в потоке. В 2005 г. система дополнилась еще одним ШУ насосами узлов приготовления керосина и мазута. В 2006 г. был введен в эксплуатацию узел ввода присадок в дизельное топливо (ДТ) с еще четырьмя ШУ. В 2010 г. были внедрены очередные два ШУ с контроллерами в связи с началом работы комплекса глубокой переработки нефти на базе гидрокрекинга вакуумного газойля. Данная установка позволяет работать в трех режимах: с целью получения максимального объема дизельного топлива, наибольшего выпуска керосина либо максимальных объемов производства и того, и другого вида продукции. В 2011 г. произошло расширение (до четырех ШУ) узла смешения дизельных топлив в связи с модернизацией парка смешения светлых нефтепродуктов для обеспечения производства топлива с ультранизким содержанием серы и выполнения требований технического регламента РФ на соответствие стандарту ЕВРО-4. В 2013 г. были введены в эксплуатацию три ШУ узлом ввода присадок в топливо ТС (авиакеросин). Таким образом, к настоящему моменту, в результате вышеперечисленных модернизаций и ряда менее крупных работ, система имеет информационную мощность порядка 11 000 сигналов и представленную на рис. 2 структуру.

АСУ ТП ПСТ ОАО «Киришинефтеоргсинтез» имеет ряд особенностей. Одна из наиболее важных — непрерывный цикл работы оборудования, что подразумевает полное отсутствие за все время эксплуатации АСУ ТП остановов ПСТ на ремонты, модернизации и т. д. Прекращение работы парка смешения означает фактически остановку всего предприятия, что влечет за собой значительные финансовые потери. Вследствие этой особенности все модернизации и расширения проводились при работающем оборудовании АСУ ТП. Добавление параметров в систему, незначительные изменения алгоритмов и т. п. выполнял непосредственно обслуживающий персонал АСУ ТП, который прошел соответствующие курсы в Центре обучения НПФ «КРУГ». Более масштабные изменения требовали непосредственного участия специалистов НПФ «КРУГ». Одной из интересных работ, связанных с этой особенностью объекта автоматизации, стала замена контроллеров, управляющих оборудованием парка смешения дизельных топлив, на более современные. Обновление было выполнено после того, как старые контроллеры безотказно отработали более десяти лет, и было обусловлено необходимостью изменения схемы резервирования контроллеров. Работы осуществлялись после предварительной подготовки в течение нескольких часов, что позволило узлу функционировать в штатном режиме без останова и снижения мощности.

Вторая особенность ОАО «Киришинефтеоргсинтез» — практически постоянная необходимость внесения изменений в действующую систему (более и менее значительных). В связи с тем что возраст установленной АСУ ТП приближается ко второму десятку и за это время было произведено до десяти достаточно крупных расширений, то можно представить себе количество разных модификаций оборудования и программного обеспечения (ПО) даже в пределах одного ПТК КРУГ-2000, которое применяется на данном объекте. Несмотря на это, никаких проблем, связанных с поддержкой старого оборудования и ПО, за все время эксплуатации не было. Благодаря преемственности оборудования и версий ПО, входящих в состав ПТК КРУГ-2000, можно постепенно менять контроллеры и обновлять ПО. Объясняется это и модуль-

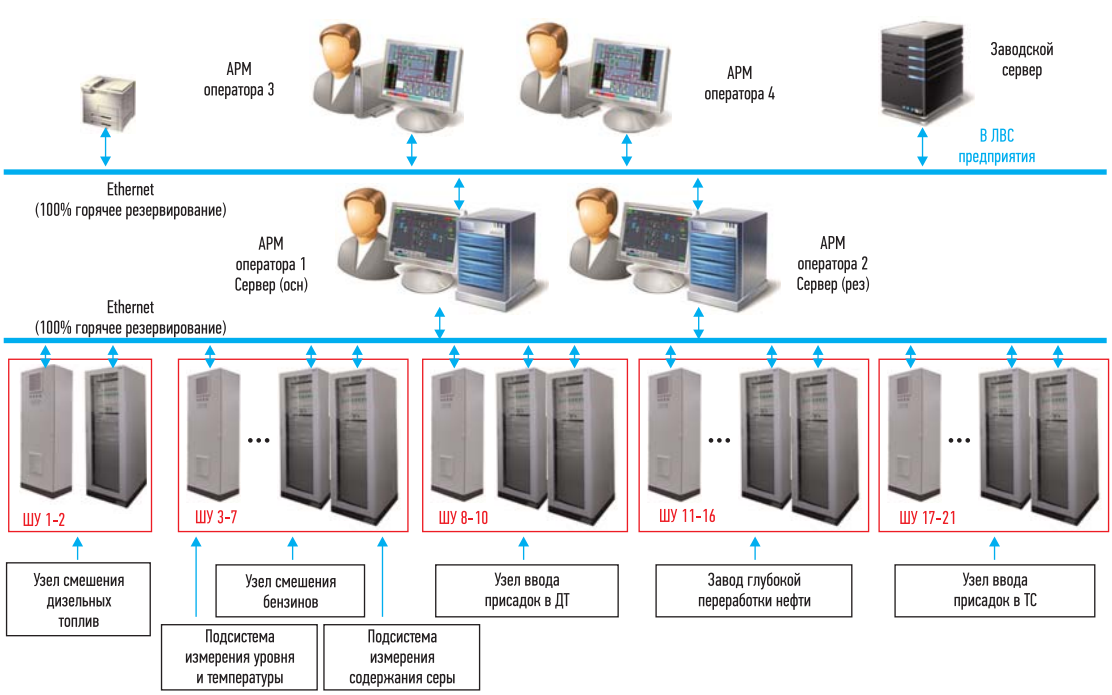


РИС. 2. ◀
Структурная схема АСУ ТП парка смешения топлив ОАО «Киришинефтеоргсинтез»

ностью ПТК, которая позволяет по мере необходимости наращивать как информационную, так и функциональную мощность системы. Таким образом, несмотря на свой солидный возраст, система является современной, активно развивается и не требует «бульдозерного» варианта модернизации, когда необходимо заменить все «сразу и сейчас», что обычно связано со значительными финансовыми и временными затратами и неприемлемо для данного объекта.

Третья особенность этого проекта — большое количество оборудования и подсистем сторонних производителей, информация от которых по различным протоколам и каналам связи передается, отображается и хранится в АСУ ТП. Например, измерение уровня и температуры выполняется приборами TGD фирмы Valcom, при этом расчет массы и объема нефтепродуктов в резервуарах осуществляется ПТК КРУГ-2000, а данные по содержанию серы принимаются от хроматографов «Кристалл 5000». С помощью ПТК также производится, например, управление вариаторами скорости дозирующих насосов. Информация, необходимая для принятия решений на общезаводском уровне, передается в АСУП завода. Обмен со сторонними системами производится как на уровне контроллеров, так и на уровне серверов баз данных интегрированной SCADA-системы КРУГ-2000 с использованием общепринятых протоколов типа Modbus и OPC или драйверов, специально разработанных под конкретные устройства, механизма файлообмена и т. д. Таким образом, ПТК выполняет функции единого интегрирующего центра для всех подсистем управления, присутствующих в АСУ ТП ПСТ.

В ближайшем будущем на данном объекте планируются работы по замене сигнализаторов загазованности на приборы фирмы Stahl, а также обновление версии ПО SCADA КРУГ-2000.

Похожие задачи решались и при автоматизации других парков нефтепродуктов: Туапсинского НПЗ, Сургутского ЗСК, Ярославского НПЗ и других нефтезаводов.

С точки зрения возможности интеграции приборов сторонних производителей в АСУ ТП заслуживает внимания проект автоматизации товарно-сырьевого парка Павлодарского НХЗ. Система была внедрена в 1994 г.: SCADA КРУГ-2000 под операционной системой MS-DOS. В 2012 г. потребовалось произвести замену персональных компьютеров в связи с их моральным и физическим старением. В связи с недостаточностью финансирования было принято решение обновить только оборудование и ПО верхнего уровня (SCADA), а полевые приборы оставить существующие. Таким образом, появилась задача интеграции с приборами, произведенными еще в начале 1990-х гг. Полноценная документация на них отсутствовала, но замена была произведена успешно. В рамках данных работ были разработаны OPC-серверы для комплексов телемеханики ТК-301, приборов Ш9329АИ и УГР-1М.

Помимо создания АСУ ТП парков нефтепродуктов на нефтезаводах, у фирмы «КРУГ» накоплен значительный опыт автоматизации нефтебаз. Примером тому могут служить нефтебазы в таких городах, как Пенза, Тихорецк, Новороссийск и др.

Как уже отмечалось выше, инжиниринговые подразделения НПФ «КРУГ» могут выполнять проекты не только на базе ПТК собственной разработки, но и на оборудовании и ПО сторонних производителей. Например, АСУ ТП приема, хранения и отпуска нефтепродуктов на нефтебазе в г. Тихорецк (ПАО «НК «Роснефть» — Кубаньнефтепродукт») реализована на устройствах и ПО Schneider Electric. По требованиям заказчика в качестве контроллеров были выбраны ПЛК Modicon Premium с ПО Unity Pro XL. В данном случае АСУ ТП решает все необходимые задачи, включая управление процессами приема нефтепродуктов с железнодорожных цистерн, их хранения в резервуарных парках и отпуска нефтепродуктов в автоцистерны.

Примером применения решений НПФ «КРУГ» на судовых терминалах является проект по созданию АСУ ТП склада нефтепродуктов в г. Новороссийск. Склад нефтепродуктов судового сервисного центра ООО «База Технического Обслуживания Флота — Терминал» — это крупнейший объект с проектным грузооборотом 540 тысяч тонн в год.

Система автоматизации данного склада позволяет управлять процессами приема, накопления и отгрузки дизтоплива и мазута на морские суда и выполняет все требуемые функции, включая противоаварийные защиты и блокировки, дистанционное управление запорно-регулирующей арматурой и насосными агрегатами, управление процессом слива/налива нефтепродуктов и т. д. Верхний уровень АСУ ТП выполнен на базе SCADA КРУГ-2000, входящей в состав ПТК КРУГ-2000. Связь между SCADA-системой и контроллерами организована с использованием протокола OPC, а модули ввода/вывода дискретных и аналоговых сигналов контроллеров объединены линией Ethernet с топологией «кольцо» и вместе с барьерами искробезопасности и коммуникационным оборудованием полевых шин смонтированы в электротехнических ШУ, которые установлены в операторной и электрощитовых.

Еще одним перспективным направлением в этой отрасли на данный момент является разработка АСУ ТП для топливозаправочных комплексов (ТЗК) аэропортов. Применение систем автоматизации на данных объектах позволяет организовать оперативно-диспетчерский контроль и управление процессами хранения, слива/налива нефтепродуктов, обеспечивает выполнение требуемых противоаварийных защит и технологических блокировок. На данный момент НПФ «КРУГ» уже выполнено семь таких проектов, и еще пять находятся на стадии проектирования и внедрения. Проработанные технические решения охватывают весь комплекс автоматизации, включая выбор полевого КИП, блок-боксов для размещения оборудования АСУ ТП, программных и аппаратных средств, организацию системы диспетчеризации, решение вопросов передачи информации в MES-систему и создание тренажерного комплекса для обучения оперативного персонала. Базой для создания АСУ ТП ТЗК в данных проектах служит ПТК КРУГ-2000.

Разработанные АСУ ТП ТЗК выполняют практически весь комплекс задач по управлению ТЗК, в том числе:

- управление процессом приема авиатоплива с авто- и железнодорожных цистерн;
- управление выдачей авиатоплива на пункты налива в аэродромные топливозаправщики (ТЗА) и центральные топливозаправщики (ЦЗТ) с дозировкой противоводокристаллизационной жидкости;
- контроль режимов работы резервуаров (прием, выдача, отстой с обратным отсчетом минимального времени);
- автоматическая сборка предопределенных маршрутов движения нефтепродуктов;
- контроль правильности собранных оператором маршрутов движения топлива;
- дистанционное управление блочными насосно-фильтровальными станциями;
- управление процессом топливоснабжения дизельной электростанции и котельной;
- дистанционное управление насосными агрегатами и запорной арматурой;
- автоматическое определение герметичности запорной арматуры;
- сбор данных о наличии пожара на складе;
- автоматическое отключение электроэнергии по секциям при пожаре;
- перевод запорной арматуры в положение, соответствующее безопасному состоянию объекта, и их обесточивание при наличии сигналов о загазованности;
- обесточивание насосного оборудования при наличии сигналов о загазованности.

С целью унификации контроллерного оборудования система управления автоматической фильтровальной станцией выполнена на оборудовании ПТК КРУГ-2000. Это позволило получить глубокую интеграцию подсистемы управления аппаратами фильтрации топлива (АФТ) в общую АСУ ТП, тем самым уменьшив время на инжиниринг и наладку системы, минимизировав количество единиц ЗИП, сократив объем знаний, требующихся для эксплуатации системы, и т. д. В этих проектах также решены вопросы по интеграции с измерительным комплексом «Струна», служащим для измерения уровня, температуры, плотности, давления, массы и вычисления объема нефтепродуктов.

Приведенные в данной статье примеры показывают, что, несмотря на большое многообразие складов ГСМ, можно выделить несколько основных выполняемых ими функций, которыми являются: хранение нефтепродуктов в резервуарах, компаундирование нефтепродуктов, прием и отгрузка нефтепродуктов по железной дороге, автомобильным, водным и трубопроводным транспортом. Среди основных задач автоматизации складов ГСМ — проведение складских операций в соответствии с установленными требованиями безопасности, минимизация ручных операций по управлению арматурой, насосным оборудованием, сборкой маршрутов, решение учетных задач, передача необходимой информации на корпоративный уровень (рис. 3).

Многочисленные внедрения в данной области позволили НПФ «КРУГ» обобщить имеющиеся наработки и создать ряд типовых решений по автоматизации складов ГСМ, парков нефтепродуктов, наливных терминалов и ТЗК. Решения предназначены для создания АСУ ТП, целями которых являются:

- организация оперативно-диспетчерского контроля и управления процессами хранения, слива/налива нефтепродуктов;
- получение данных о материальном балансе склада, ведение учета (коммерческого и технического) массы принятых и отгруженных нефтепродуктов;
- снижение уровня трудоемкости технологических операций на объекте управления, обеспечение комфортных условий труда эксплуатационного персонала;
- обеспечение необходимого уровня безопасности и надлежащего функционирования складов ГСМ во всех режимах работы, а также выполнения требуемых противоаварийных защит и технологических блокировок.

Применение типовых решений дает ряд преимуществ, таких как уменьшение времени и стоимости проектирования, снижение затрат на инжиниринговые, пусконаладочные работы и техническое обслуживание, широкие возможности по расширению и масштабированию системы. Как следствие — использование разработанных НПФ «КРУГ» типовых решений приводит к снижению совокупной стоимости владения системой автоматизации в целом. ⬣

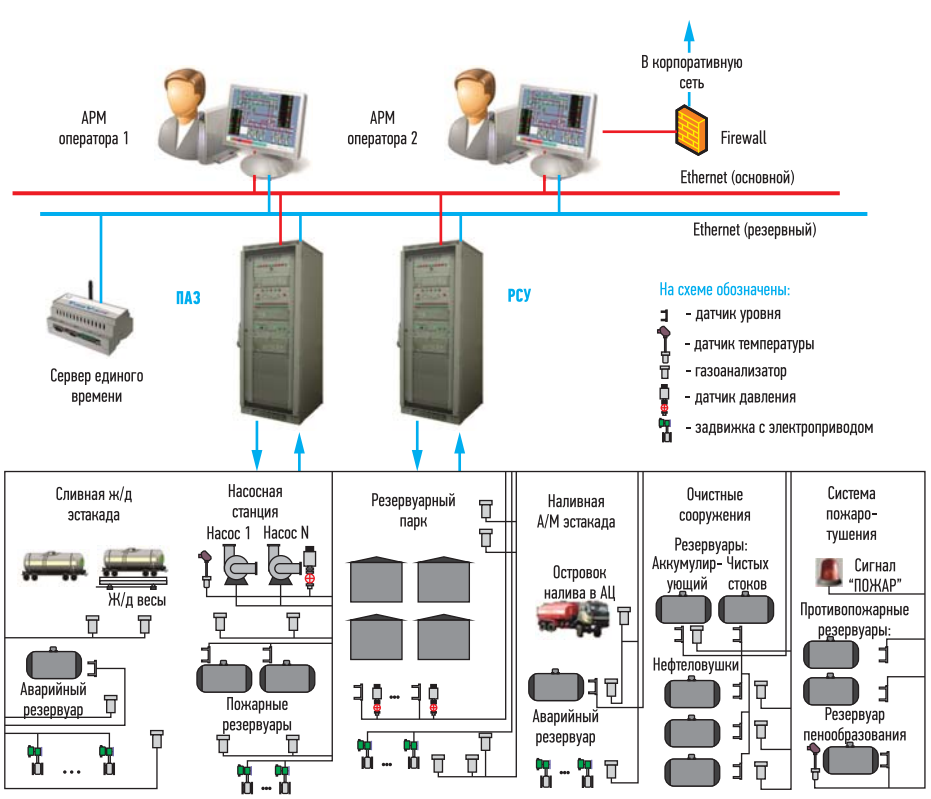


РИС. 3. ▼
Общая структура АСУ ТП складов ГСМ

ATLAS MES — ИННОВАЦИОННАЯ СИСТЕМА ДЛЯ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ ПРОИЗВОДСТВОМ

СЕРГЕЙ ВИХАРЕВ
mail@atlasbpm.com

От грамотного внедрения любой MES-системы производительность может вырасти в несколько раз. Но сегодня это уже не вопрос «выгодно или невыгодно», это вопрос способности выдержать конкуренцию с теми, кто уже автоматизировал управление производством. Данная статья посвящена обзору комплексной системы автоматизации управления производственными процессами Atlas MES.

ЗНАЧИМОСТЬ РЫНКА MES-СИСТЕМ

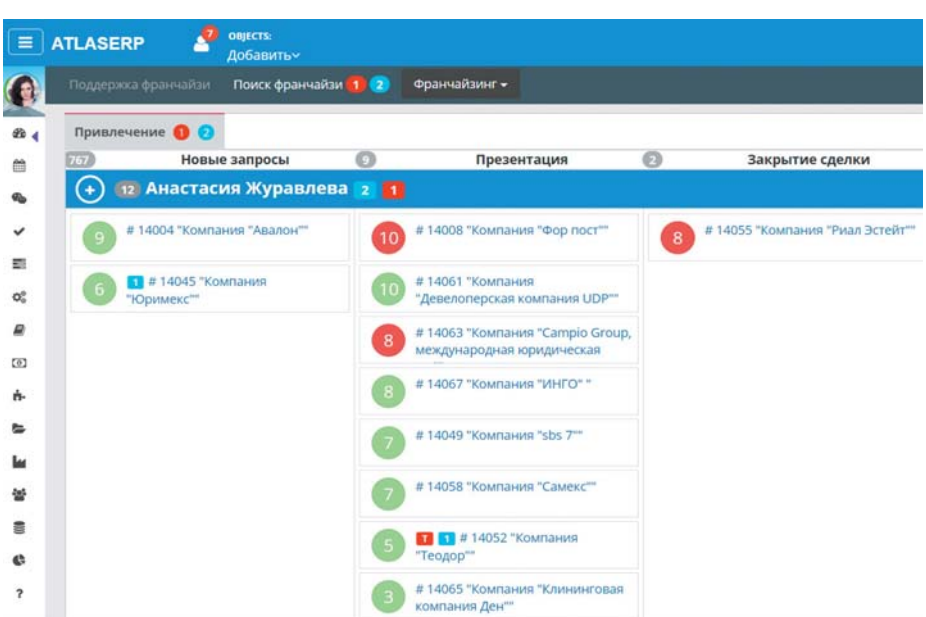
Согласно исследованию аналитической компании MarketandMarkets, мировой рынок систем автоматизации производства к 2022 г. достигнет $18,22 млрд, а среднегодовой темп роста в 2016–2022 гг. составит 13,6%. При этом в данный период рынок программного обеспечения станет крупнейшим на общем производственном рынке. MES-системы поддерживают каждый производственный процесс, планируют и совершенствуют операции, а также контролируют работу оборудования. Основными факторами, стимулирующими рост рынка, являются низкая стоимость внедрения, широкое использование автоматизации в промышленности, улучшение производств благодаря MES-системам, а также важность соблюдения нормативных требований.

НЕБОЛЬШИЕ ПРОИЗВОДСТВА

Atlas MES ориентирована в том числе на малые и средние предприятия, где при производстве изделие проходит несколько юнитов. Если товар изготавливается, например, на одном станке, то такая сложная система не нужна. Но если продукция проходит 10-–15 юнитов, причем по разным маршрутам, то подобная система способна дать ощутимый эффект.

Главная задача любого производства — это повышение производительности и рост качества продукции без увеличения затрат. Ручное управление производственными процессами и заказами снижает качество, поэтому его необходимо максимально автоматизировать. Например, MES-системы могут снять замер показателей, выполнить планирование, выдачу и распределение заданий, аналитику полученных данных, подготовку отчетности и т. д.

РИС. 1. ▼
Карта производственного процесса



КОНЦЕПЦИЯ ATLAS MES

Концепция Atlas MES состоит из пяти элементов.

1. Управление технологиями. Система улучшает процесс их создания за счет формирования процесса разработки и строгого соответствия ему в дальнейшем. Atlas MES собирает карточки технологий, документацию, описание операций и другие данные в одном месте.
2. Моделирование технологических процессов. Система может составлять карту производствен-

ного процесса (рис. 1) из отдельных операций, как конструктор. Получается, что эта информация хранится не в головах людей, а в стандартизированном виде — с ней можно работать, изменять ее, передавать, согласовывать и т. д. Кроме того, в таком производственном процессе запускаются задания, которые уже содержат в себе схему работы с изделием: кто, на каких юнитах и в какой очередности должен выполнять работу.

3. Производственное планирование. Atlas MES позволяет автоматически распланировать задания на то время и те юниты, которые оптимально подходят для повышения производительности и выравнивания производственного потока. Специальная панель планирования (рис. 2) помогает эффективно загружать юниты, минимизировать простои и очереди, оптимизировать узкие места и тем самым повышать производительность участков и цехов. Этот модуль Atlas MES является ключевым.
4. Работа с заданиями с точки зрения исполнителя. Atlas MES способен снабдить рабочих производственными терминалами. Разработчики создали приложение для Android, поэтому это могут быть как ноутбуки для работы из браузера, так и любые устройства с этой операционной системой. Сотрудники прямо в системе получают задания и отчитываются о ходе работы.

С другой стороны, такой подход также позволяет руководителю видеть фактическую ситуацию на производстве. В Atlas MES встроены элементы искусственного интеллекта и «умные» алгоритмы, которые автоматически пересчитывают плановое время готовности изделия в зависимости от того, что происходит в течение производственного процесса. Этой информацией можно делиться с другими сотрудниками, партнерами и даже клиентами, которые меньше отвлекают персонал и спокойнее себя чувствуют, наблюдая за заказом в прямом эфире.

5. Сбор аналитики по производственным процессам. Atlas MES собирает всю информацию о производстве: когда, кем и какие задания были сделаны. Это позволяет анализировать производственные процессы и видеть, как, например, меняется длина операции и как она зависит от того, на каком юните и у какого рабочего было выполнено задание. Даже по прошествии года можно поднять данные и увидеть, как было произведено изделие, поминутно. Это может быть очень важно при работе с претензиями по качеству и появлением брака, когда нужно отследить, был ли на производстве какой-либо сбой.

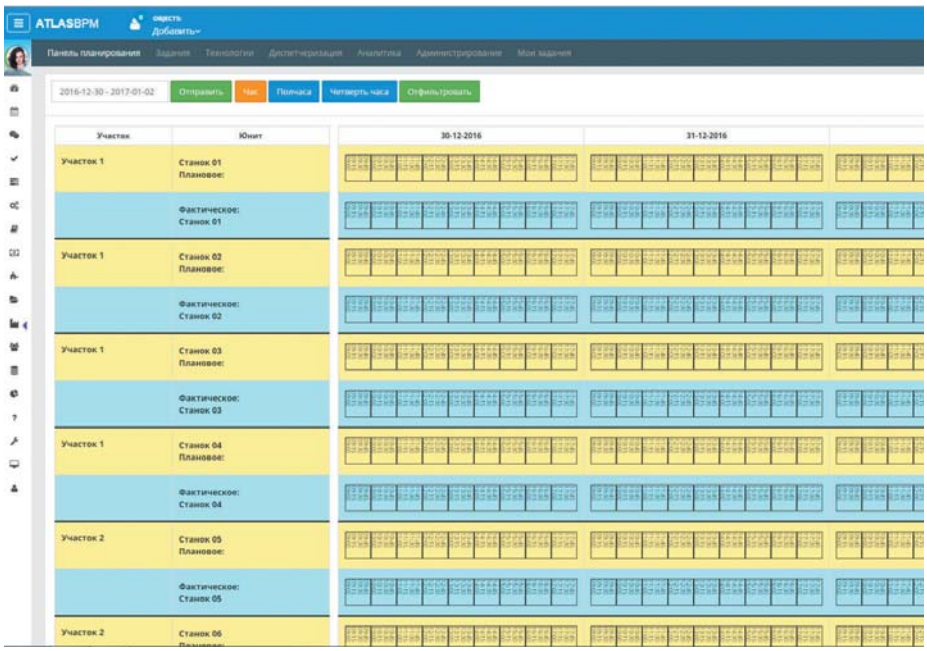
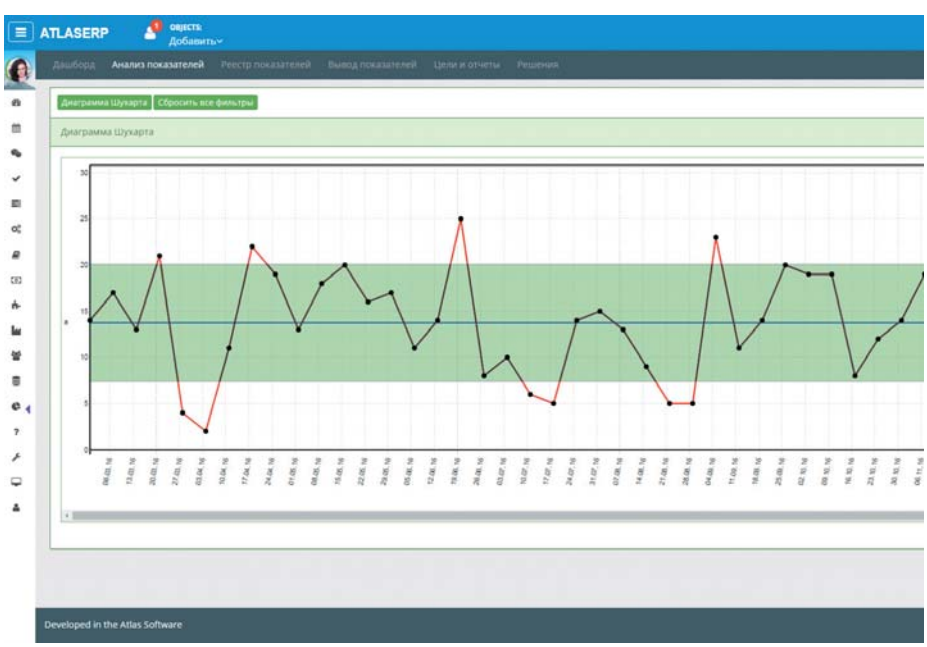


РИС. 2. ▲
Панель планирования

В Atlas MES также доступен аналитический инструмент в виде диаграммы Шухарта, которая показывает вариативность и изменения производственных параметров (рис. 3). Эта информация помогает принимать правильные управленческие решения для оптимизации производственных процессов, повы-

РИС. 3. ▼
Диаграмма Шухарта



шения качества продукции и роста производительности.

Говоря о технических аспектах, важно отметить, что Atlas MES — облачная система. Это дает возможность легко развернуть работу и организовать доступ к системе на производствах любого размера. Также благодаря этому обеспечивается гибкость: терминалом рабочего может стать любой компьютер или устройство на базе Android, за счет чего систему дешевле и проще внедрить, поскольку предприятию не нужно покупать дорогое коробочное решение и сразу же инвестировать большие деньги в его внедрение.

ВНЕДРЕНИЕ ВНЕДРЕНИЮ РОЗНЬ

Экономический эффект от внедрения Atlas MES и использования всех возможностей системы в несколько раз превышает ее стоимость. Но важно подчеркнуть, что все зависит от правильного использования сервиса. Переход на новую автоматизированную систему — непростое дело, требующее изменения управленческого мировоззрения и переобучения сотрудников. Далеко не все предприятия готовы совершить этот шаг. Многие останавливаются на полпути и ограничиваются полумерами, тем самым упрощая отдельные элементы производственного процесса и получая меньший экономический эффект.

Сейчас Atlas Software заканчивает внедрение MES-системы в компании по производству мебели. Работа еще не завершена, но уже есть первые результаты. Во-первых, руководство перешло от ручного планирования к автоматизированному. Это повысило его эффективность и уменьшило количество ошибок, из-за которых раньше на производстве регулярно случались задержки. Во-вторых, оснащение всех рабочих смартфонами с приложением позволило наладить диспетчеризацию. Теперь руководитель контролирует исполнение процессов и видит, что происходит на каждом участке. В-третьих, начат полноценный и комплексный сбор данных. Пока информация только накапливается, но уже можно сделать выводы о том, что заказы стали исполняться быстрее, а качество продукции осталось прежним.

БУДУЩЕЕ СИСТЕМЫ

Первоочередная задача для Atlas MES — это автоматизация аналитики. Сейчас система собирает данные, но анализируют их люди, которые затем принимают решения на основании своей оценки. Разработчики стремятся к тому, чтобы Atlas MES не просто систематизировала информацию, но и анализировала ее, сигнализировала о проблемах и сама предлагала готовые решения.

Также целью Atlas Software является повышение уровня автоматизации планирования. Безусловно, планирование осуществляется и сейчас. Есть список заказов, и по ним вручную создаются задания, которые затем автоматически распределяются по юнитам. Задача состоит в том, чтобы научить систему строить весь маршрут изделий самостоятельно сразу после загрузки заказов. ⬣

Реклама

С факельным газом не все так однозначно

Кажущийся правильным выбор измерения расхода может оказаться неверным, когда дело касается факельного газа.

Поскольку факельный газ может быть низкого давления и низкого расхода, термодифференциальный массовый расходомер TA2 производства компании Magnetrol - единственный прибор, способный предоставить Вам точную информацию о газовых сбросах при минимальных экономических затратах.

Для более подробной информации пройдите по ссылке:
flow.magnetrol.com

Реклама

Magnetrol®

magnetrol.com • +7-812.320.70.87 • info@magnetrol.ru

НОВЫЙ ТРЕНД В БИЗНЕСЕ: «УМНЫЕ КОНТРАКТЫ»

КАРИНА КРУПЕНЧЕНКОВА
kkrupenchenkova@redenex.com

Smart contracts, или «умные контракты», — актуальная тема в мире бизнеса, которую активно обсуждают последние несколько лет не только в России, но и в мире. Почему этот инструмент появился только сейчас и чем он интересен для энергетики?

Автоматизация бизнес-задач, как и любой другой вид автоматизации, — это область, которая активно развивается уже несколько десятилетий. Выгоды от внедрения таких технологий очевидны как владельцам бизнеса, так и простым обывателям. Самой элементарной и такой необходимой в современном мире является возможность автоматического платежа с банковской карты — например, провайдеру или интернет-магазину, в котором были совершены покупки. По сути, «умные контракты» — это развитие столь же простых идей автоматизации бизнес-задач, но построенных на новых технологических платформах и использующих современные средства, которые позволяют легче справиться с необходимыми процедурами и обеспечивают высокий уровень защиты.

ПРЕДПОСЫЛКИ ДЛЯ ПОЯВЛЕНИЯ «УМНЫХ КОНТРАКТОВ»

Многие крупные промышленные предприятия давно и весьма успешно интегрируют свои ERP-системы с такими же решениями своих партнеров. Разумеется, это требует серьезной кастомизации, но зато они существенно упрощают контроль и сопровождение бизнес-процессов, что приводит к снижению накладных расходов. В таких системах можно реализовать автоматизированные действия, похожие на «умные контракты», но ERP по определению закрытые, поэтому их возможности ограничены.

«Умные контракты» поднимают функциональность подобной автоматизации на принципиально новый уровень. В частности, smart contracts позволяют взаимодействовать как с уже известными партнерами, с которыми налажены отношения, так и с неизвестными — т. е. обеспечивают доверительное взаимодействие сторон автоматически. Нет необходимости прибегать для этого к услугам третьей стороны и, соответственно, оплачивать эти услуги. Остановимся подробнее на некоторых новейших направлениях, связанных с этой областью индустрии, — блокчейне и «Интернете всего».

ПОЧЕМУ НЕОБХОДИМ БЛОКЧЕЙН

«Умные контракты» основаны на блокчейне (его называют и по-другому, например «децентрализованной бухгалтерской книгой»), технологии, которая практически исключает шансы подделки записей и, соответственно, минимизирует возможности мошенничества.

Блокчейн получил широкую известность благодаря буму криптовалюты биткойн. Нельзя ставить знак равенства между блокчейном и криптовалютами, но для понимания сути технологии нам придется поговорить о некоторых ее важных особенностях, которые наиболее выразительно проявились именно в ситуации с биткойном.

ОТКРЫТОСТЬ КАК ЗАЩИТА

Биткойн — это просто последовательность цифр, которая может быть передана от одного пользователя

другому в качестве платежа. Конечно, за системой биткойна стоит сложнейшая математика, которая во многом и предопределила популярность этой криптовалюты. Но при ее создании нужно было предусмотреть некоторые важные моменты, которые позволяли бы использовать биткойны в качестве платежного инструмента. В частности, как доказать, что данная последовательность в качестве оплаты передана из одного «электронного кошелька» в другой, и как сделать так, чтобы эту последовательность невозможно было скопировать и использовать любое количество раз?

Для автоматизации этих задач был создан блокчейн, и на нем построили решение, которое позволяет системе «кошельков» отслеживать каждый биткойн, автоматически фиксируя все его перемещения. Для фиксации факта передачи средств уже не нужны никакие другие структуры — ни банки, ни нотариусы, ни какие-либо иные институты.

Важно, что эта система распределенная. В ней участвует каждый «кошелек», поэтому взломать ее практически невозможно. Взлом отдельного «кошелька» в данном случае бесполезен, уничтожение части системы тоже ничего не даст потенциальным «фальшивобиткойнщикам». Подделку возможно реализовать математическими методами, но для этого потребуется контролировать более половины «кошельков» на планете, что сделать нереально.

ОТ КРИПТОВАЛЮТЫ К ИНДУСТРИИ

Блокчейн, как технологию для создания единой «блочной» базы данных, содержимое которой практически невозможно подделать, можно использовать не только для «кошельков» криптовалют, но и для других задач — например, фиксации прав собственности и их передачи. Таким образом, наличие такого средства позволяет автоматизировать многие бизнес-задачи. Эта автоматизация экономически оправдана, хотя бы за счет исключения затрат на транзакции: напомним, в данном случае оказываются необязательными банки, нотариальные конторы, кадастровые системы и другие посреднические структуры, к услугам которых договаривающиеся стороны обычно прибегают при оформлении сделок.

Существует достаточное количество блокчейн-платформ — как открытых, так и созданных отдельными структурами, например банками или консорциумами. Платформы могут и зафиксировать необходимые условия, и обеспечить работу нужных алгоритмов в «умных контрактах».

«УМНЫЕ КОНТРАКТЫ» = АЛГОРИТМЫ

Пункты большинства контрактов в бизнесе могут без проблем получить математическое описание. По сути, smart contract — это алгоритм, однозначно и полно описывающий взаимодействие сторон.

Появление платформ обеспечит простоту создания «умных контрактов» и, что очень важно, практически исключит возможность мошенничества. Заметим, что, кроме блокчейн-платформ, для работы потребуются и другие криптоинструменты, но они, по счастью, уже есть и даже стали привычными. В качестве примера приведем электронные подписи, использование которых давно стало привычным делом: они как раз необходимы для фиксации факта приема условий сторонами и, соответственно, для активации «умного контракта».

ИНФРАСТРУКТУРА УЖЕ ГОТОВА

Итак, блокчейн-системы, созданные за пределами биткойна, к обеспечению работы «умных контрактов» готовы. Но некоторые технические сложности на пути smart contracts все же еще есть.

Основная проблема состоит в том, что система, обеспечивающая работу «умного контракта», должна иметь беспрепятственный и прямой доступ к предмету договора, а для этого должен быть соблюден ряд условий. Например, предмет договора, как минимум, должен быть или изначально цифровым (как, например, криптовалюта), или иметь достоверное «цифровое отражение». С последним связаны очевидные сложности, которые сейчас уходят в результате распространения «Интернета всего» (Internet of Everything, IoE).

«ИНТЕРНЕТ ВСЕГО» ДЛЯ SMART CONTRACTS

Термин «Интернет всего» стирает грань между миром физическим и миром цифровым. На примере «умных контрактов» это особенно хорошо видно. Причем наиболее выразительно — в решениях из области энергетики.

Если проверенные датчики способны предоставить «умному контракту» по защищенному каналу достоверную информацию о факте соблюдения условий договора, то с его заключением проблем нет. Технически вполне возможна и обратная ситуация: «умный контракт» определяет выполнение условий договора и, соответственно, дает команду IoE-системе на выполнение действий в физическом мире, например на перевод денежных средств, манипуляции с вентилями, подключение или отключение энергосистемы и т. д.

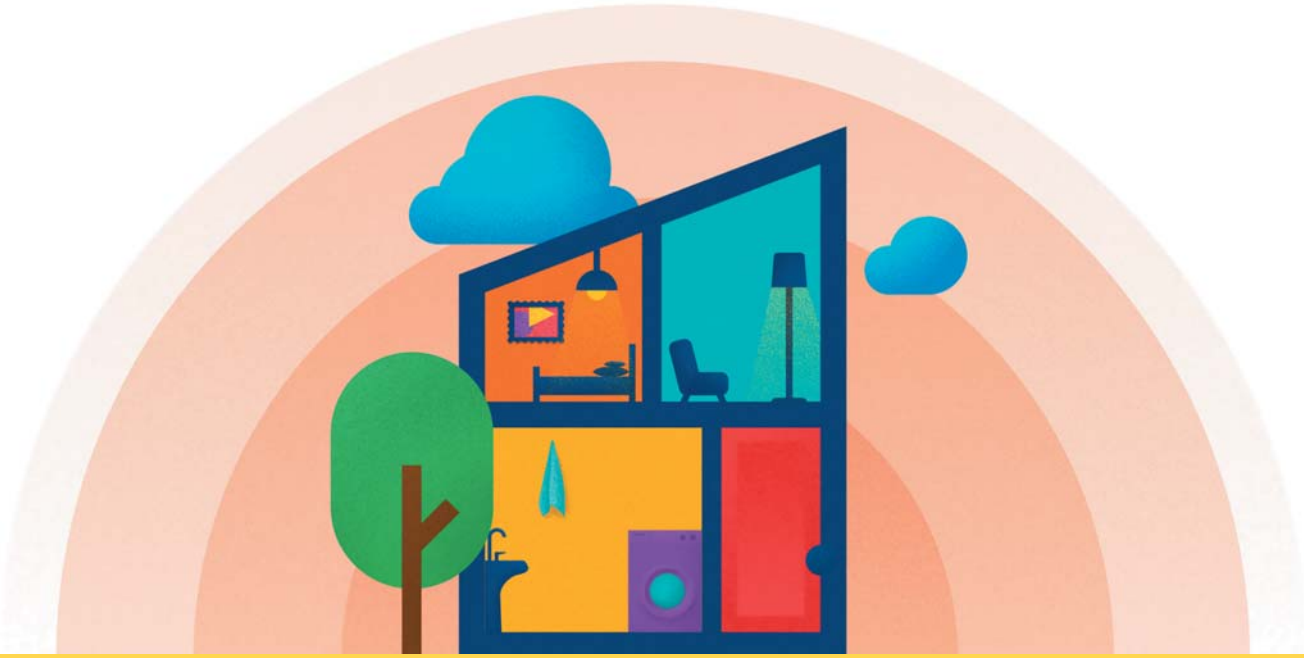
Пример с энергосистемами в настоящее время наиболее реалистичен, так как энергетика сегодня является отраслью, наиболее насыщенной IoE-решениями, и «умные контракты» для бизнес-процессов в этой области использовать проще всего.

ПРАКТИЧЕСКОЕ ВНЕДРЕНИЕ

Несмотря на простоту, сегодня системы, построенные на основе «умных контрактов», все еще находятся на стадии внутреннего тестирования в ряде как российских, так и глобальных компаний — приведем лишь примеры IBM и «Сбербанка». Причина проста: нужное количество упомянутых нами блокчейн-платформ, необходимых для функционирования «умных контрактов», было создано только летом прошлого года. За несколько месяцев полноценные решения для промышленности создать невозможно, тем более на основе современных технологий, которые проходят «обкатку» в новых условиях. Но за это время компании успели провести R&D и убедились в актуальности доступных инструментов и, что важно, в степени защищенности всей процедуры.

В ближайшее время, уже в этом году, мы увидим разворачиваемые пилотные проекты на основе «умных контрактов», причем в самых разных областях экономики — от энергетики и промышленности до страховой сферы и банков. ⬣

Материал подготовлен на основе докладов со Smart Energy Summit.



«ИНТЕРНЕТ ВЕЩЕЙ» В РОССИЙСКОМ ДОМЕ

КИРИЛЛ КОВАЛЕНКО
kirill.kovalenko@rubetek.com

Российский рынок беспроводных систем «умный дом» растет высокими темпами, и в 2017 г., по информации газеты «Ведомости», составит $73 млн. В 2017–2021 гг. рынок будет расти в среднем на 78% в год и к 2021 г. увеличится до $735 млн.

Сначала в России работали только инсталляторы, использующие импортное оборудование, но сейчас ситуация меняется, появляются готовые решения и производители таких устройств. Сегодня на российском рынке представлен ряд решений »умный дом» различных брендов: Rubetek, Nest, Samsung SmartThings, Fibaro, МГТС, Мегафон (Life Control), EnOcean, Xiaomi. «Доля умных домов в общем объеме российского жилья вырастет с 0,9% в 2017 г. до 4,7% в 2021 г.», — сообщает газета «Ведомости»[1].

При этом компаний полного цикла, аналогичных Rubetek, которые бы являлись и разработчиком, и производителем, и имели бы собственную инсталляционную службу, на рынке немного. Кроме того, система Rubetek является максимально «открытым» решением, поскольку работает одновременно с четырьмя протоколами беспроводной связи (Z-Wave, Wireless RF, Wi-Fi и Bluetooth), что позволяет подключать широкий спектр устройств и техники.

Интерес массового сегмента к беспроводному «Интернету вещей» для дома вызван тем, что такая система позволяет достичь значительной экономии средств. Например, в обычном режиме теряется огромное количество энергии при отоплении неиспользуемых помещений. Благодаря автономной регулировке температуры в каждой комнате можно сэкономить более 30% энергии: ведь температура может быть пониженной в тех комнатах, которые редко используются (только когда человек дома или только в выходные). Кроме того, обычно 34% электроэнергии расходуется на освещение и бытовую технику, и 25% из счета составляют расходы на освещение. Можно снизить потребление энергии, просто выключая свет, когда он не нужен, с помощью автоматических таймеров и датчиков движения. Также, используя диммеры, можно экономить энергию, уменьшив яркость освещения.

Широкому распространению беспроводных систем способствует и привлекательная цена в сравнении с проводными решениями. Например, экосистема Rubetek, включающая видеонаблюдение, управление электроприборами, освещением и климатом, а также комплекс сигнальных датчиков (открытия, движения, дыма, протечки воды, утечки газа), обойдется пользователю в сумму от 30 тыс. рублей для квартиры в 100 кв. м. Базовый набор стоит примерно в два раза меньше. Если говорить о зарубежных аналогах, то стоимость решения в этом случае составит от 70 тыс. рублей. Большим преимуществом беспроводных систем является и то, что дополнять экосистему можно постепенно, по очереди покупая новые устройства, которые обеспечат дополнительную функциональность. Проводные системы, которые требуют прокладки кабеля и ремонта в помещении, это сделать не позволяют.

Большой интерес к «Интернету вещей» отмечается и со стороны собственников жилой и коммерческой недвижимости. Застройщикам интересна возможность позиционировать свой объект как элитное жилье. По оценкам экспертов, применение «умных» устройств увеличивает стоимость 1 кв. м жилья на 30–40%, а конечную стоимость объекта — более чем на 20%. ⬢

[1] Как преподаватель вуза построил бизнес на умных домах // Ведомости. 2017. №4287.

Компания PT AIR предлагает крейты, соответствующие стандарту ICE 60297 (ГОСТ Р МЭК 60297)

POLY RACK
TECH-GROUP

Крейты 19"

Все крейты (каркасы) могут быть дополнительно оснащены различными аксессуарами:

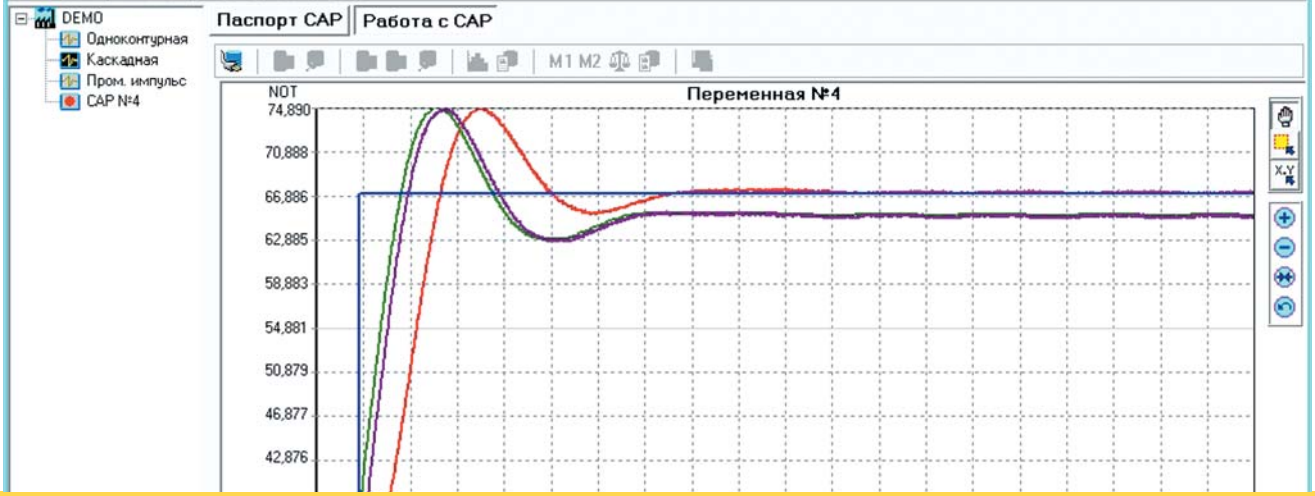
- направляющими для печатных плат
- верхними и нижними крышками (с перфорацией и без)
- защитными задними кожухами
- различной фурнитурой
- компонентами для обеспечения ЭМС

pt AIR
Innovations & Technologies

Единый телефон: 8-800-333-63-50
info@pt-air.ru
www.pt-air.ru

Офисы компании: Санкт-Петербург, Москва, Чебоксары, Нижний Новгород, Екатеринбург, Новосибирск, Ижевск, Таганрог, Пермь, Киев

Реклама



PID-EXPERT — АВТОМАТИЗАЦИЯ АВТОМАТИЗАЦИИ

ИЛЬЯ ВАРЛАМОВ
info@insat.ru
ПАВЕЛ ЗУБОВ
zubovpa@zsk.gpp.gazprom.ru

Когда говорят об автоматизации, обычно имеют в виду системы автоматического управления различными производственными процессами, включающие в себя множество составляющих: мониторы, серверы, контроллеры, датчики и исполнительные устройства. Эффективность такой системы всегда стремятся повысить — и этот процесс на самом деле тоже можно автоматизировать. Об успешном опыте повышения эффективности работы системы автоматического управления на Заводе по стабилизации конденсата им. В. С. Черномырдина (Сургутский ЗСК) пойдет речь в данной статье.

Сургутский ЗСК — крупнейший завод в России по переработке газового конденсата. Предприятие предлагает широкую номенклатуру продукции на основе углеводородов (в том числе автомобильные бензины, дизельное топливо, авиационный керосин), а также является единственным в структурах ПАО «Газпром» производителем топлива для реактивных двигателей марки ТС-1. Это относительно молодое предприятие (вся его история составляет немногим более тридцати лет) оснащено самым современным оборудованием и является предприятием высокой культуры производства.

В рамках стратегии ООО «Газпром переработка», направленной на повышение эффективности производственно-хозяйственной деятельности, руководство предприятия задалось целью найти способы повышения эффективности работы действующего оборудования без привлечения капитальных затрат. В поисках путей решения данной задачи был изучен мировой опыт, демонстрирующий улучшение показателей эффективности за счет оптимизации работы систем автоматического регулирования. В результате анализа стало понятно, что необходимо пересмотреть подход к вопросу настройки регуляторов и привлечь инновационные технологии для оптимизации их работы. Более того, это может послужить основой оптимизации всего технологического процесса.

Несмотря на то, что предприятие располагает собственными квалифицированными кадрами, владеющими навыком настройки регуляторов, для совершенствования имеющихся компетенций и внедрения новых технологий настройки было решено привлечь к сотрудничеству компанию «ИнСАТ», специалисты которой имеют богатый опыт в области оптимизации работы систем ПИД-регулирования.

Компания «ИнСАТ», основанная в 1988 г., занимается производством различного программного обеспечения (ПО) для автоматизации, среди которого SCADA-системы, OPC-серверы, средства программирования контроллеров, а также программный пакет PID-expert, предназначенный для настройки ПИД-регуляторов и оптимизации работы систем автоматического регулирования (САР).

Для осуществления пилотного проекта по оптимизации контуров регулирования на Сургутском ЗСК была выбрана установка по производству моторных топлив (УМТ). Это было продиктовано требованием времени: в последние годы сильно ужесточились технические требования к качеству моторных топлив.

Данная установка достаточно сложная. Основная колонна имеет дополнительное циркуляционное орошение и две стриппинг-колонны. Кроме этого, в состав установки входят испаритель, три печи и мно-

го другого технологического оборудования с большим количеством рециркуляционных связей, что обусловливает сильное взаимовлияние процессов друг на друга и существенно осложняет как процесс настройки регуляторов, так и эксплуатацию установки.

Для осуществления работ в рамках проекта по оптимизации была создана команда, состоящая из опытного технолога, инженера АСУ ТП и специалиста по регулированию. Они тщательно продумали план последовательности настройки. В ходе настройки регуляторов в большинстве случаев требуется нанесение тех или иных возмущений, что на действующей установке может повлечь негативные последствия в виде раскачивания зависимых контуров или даже вывода процесса за границы регламента. Поэтому в первую очередь была запланирована настройка на вспомогательных и второстепенных контурах. По мере перехода к основным контурам работы проводились по ходу технологической цепочки — начиная от первичной подготовки сырья.

Настройка регуляторов проводилась с помощью программного пакета PID-expert — специализированного ПО, предназначенного для проведения комплекса работ по повышению эффективности систем автоматического регулирования. Программа подключается к действующей АСУ ТП в качестве OPC-клиента, получает от нее текущие значения технологических параметров и ведет собственный архив. PID-expert содержит инструменты визуального анализа, идентификации параметров объекта, расчета настроек регуляторов, имитационного моделирования, статистического анализа и другие средства, необходимые для качественного сопровождения САР (рис. 1).

ЧТО ДАЕТ ИСПОЛЬЗОВАНИЕ СПЕЦИАЛИЗИРОВАННОГО ПО?

Рассчитать настройки регулятора можно и без применения программных средств. Существует множество академических методик настройки, но на практике эти способы трудно применимы и используются редко. Чаще всего настройка ведется интуитивно: инженеры изменяют коэффициенты регулятора в ту или иную сторону и затем наблюдают за процессом. Обычно такой подход требует немало времени. Особенные затруднения при интуитивной настройке вызывают регуляторы уровня, где по внешнему виду процесса невозможно сделать выводы о том, как нужно менять настройки. С помощью PID-expert требуемые настройки можно получить за несколько кликов — нужно лишь один раз «качнуть» процесс, изменив задание регулятору или положение клапана, и выделить на тренде переходный процесс (рис. 2).

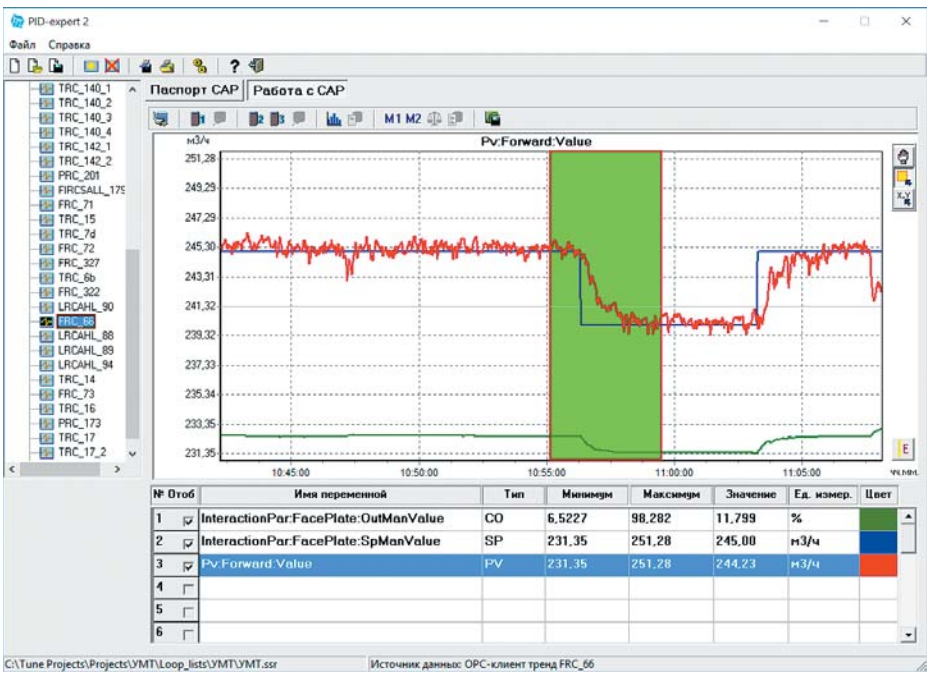


РИС. 1. ▲ Интерфейс программы PID-expert: выделен переходный процесс для расчета

«Мы и раньше настраивали регуляторы», — говорит начальник цеха АСУ ТП Игорь Болдырев. — Но этот процесс занимал достаточно длительное время. На настройку некоторых контуров уходили недели, а то и месяцы. Теперь мы увидели, что с помощью PID-expert можно настраивать по нескольку контуров в день. Производительность усилий по настройке контуров регулирования на порядок выросла, что позволило вывести работу регуляторов на качественно новый уровень».

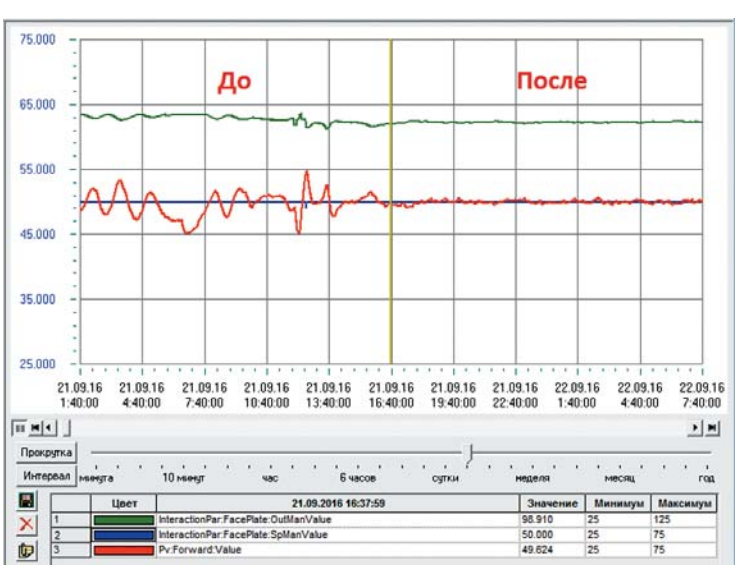


РИС. 2. ◀ Уровень в испарителе до и после настройки

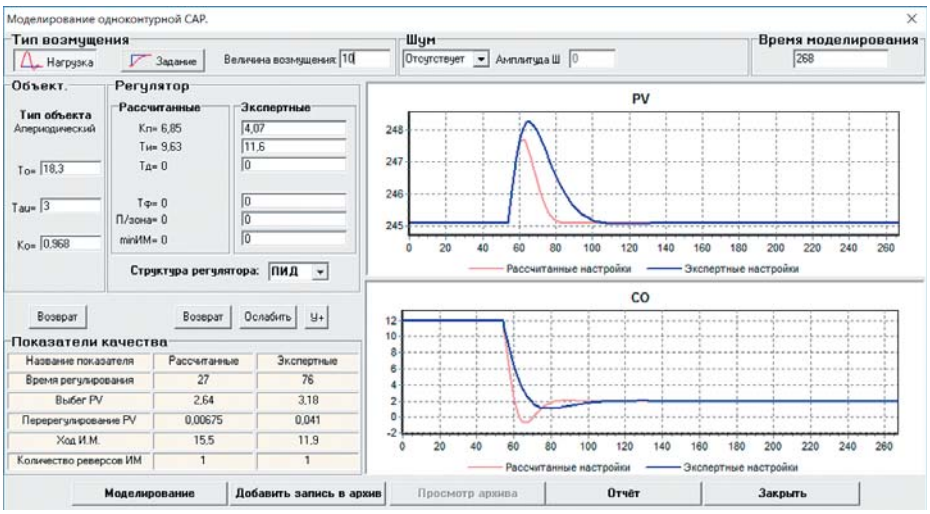


РИС. 3. ▲ Имитационное моделирование

Важным инструментом PID-expert является имитационное моделирование (рис. 3). Дело даже не в том, что оно дает возможность «поиграть» с настройками еще до их установки на реально действующую систему регулирования — хотя это тоже важно. Те, кому приходилось сталкиваться с настройкой регуляторов на реальных технологических объектах, наверняка знают, что основной проблемой поиска оптимальных настроек является постоянное изменение свойств объекта. Параметры объекта меняются от состава сырья, нагрузки, технологического режима, да и просто от погодных условий. Это приводит к тому, что еще вчера хорошо настроенный регулятор сегодня уже работает неудовлетворительно. PID-expert запоминает результаты идентифицированных параметров объекта и дает возможность смоделировать поведение контура регулирования с рассчитанными настройками при различных параметрах объекта, полученных в разное время и при разных условиях. Это позволяет подобрать настройки, подходящие для разных режимов работы установки.

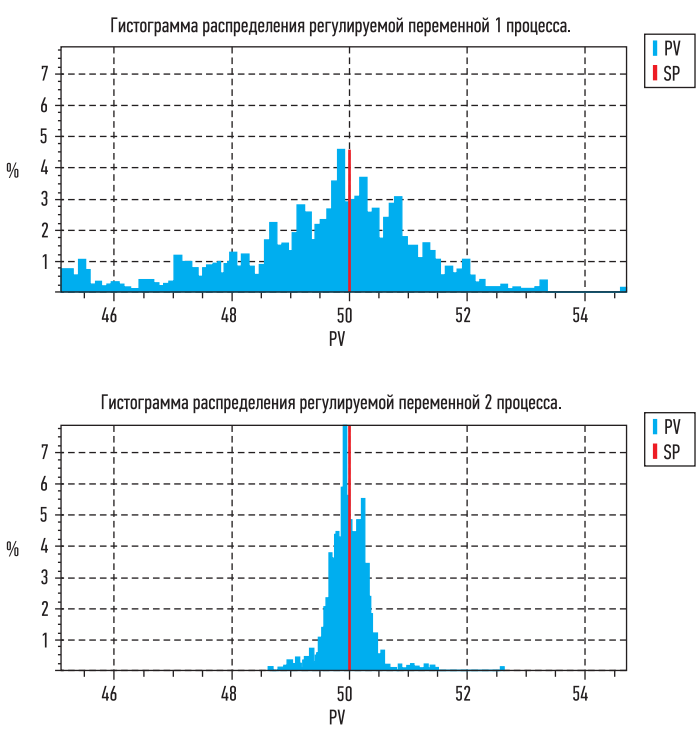


РИС. 4. ▶ Гистограмма распределения наглядно демонстрирует разброс значений переменной «до» (сверху) и «после» (снизу)

Полученные улучшения не всегда видны невооруженным глазом: случается, что отклонения в абсолютной величине малы или скрыты в обычных флуктуациях регулируемой переменной или шуме. Для оценки изменения качества стабилизации в арсенале PID-expert имеются средства статистического анализа, вычисляющие среднемодульное отклонение, распределение значений регулируемой переменной (рис. 4), суммарный ход клапана и другие параметры.

В качестве примера можно привести следующий эпизод. В рамках данного проекта внимание специалистов привлекло практически синхронное изменение всех температур, подобное реакции на какое-то возмущение, но анализ трендов не выявил источник данного возмущения внутри установки. В результате более широкого исследования удалось найти зависимость между отклонениями температур и возмущениями по давлению со стороны заводской линии топочного газа. Сначала это вызвало недоумение ввиду того, что на линии топочного газа на входе в установку стоял клапан с ПИД-регулятором, стабилизирующий давление газа после себя, и его работа никаких нареканий не вызывала — даже кратковременные пиковые отклонения не превышали 0,05 кг/см^2. Тем не менее после перенастройки регулятора средства статистического анализа показали сокращение среднемодульного отклонения с 0,01 до 0,001 кг/см^2. Это оказало самое непосредственное влияние на другие технологические параметры: возмущения со стороны давления топочного газа перестали оказывать влияние на поведение температур. Таким образом, это наглядный пример того, что можно улучшить работу даже там, где, казалось бы, и так все налажено.

Шаг за шагом команда двигалась от второстепенных контуров к более важным. В ежедневном режиме проводились оперативные совещания для быстрого решения возникающих вопросов. Например, если в ходе обследования контура обнаруживались механические проблемы клапана, препятствующие настройке регулятора или его нормальной работе, то соответствую-

щей службе давалось поручение устранить неисправность. Так были перенастроены почти все контуры, и команда вплотную подошла к основным контурам, самым непосредственным образом влияющим на качественные и количественные показатели работы установки — регулирование температурных режимов на тарелках и в стриппинговых отборах.

Поскольку имелись определенные сомнения в правильной работе этих контуров, сначала были исследованы динамические зависимости влияния различных управляющих воздействий в обвязке стриппинг-колонн на температуры как самих отборов, так и близлежащих тарелок. Основываясь на полученных динамических характеристиках, специалисты компании «ИнСАТ» предложили изменить схему регулирования температур с целью уменьшения запаздывания в канале управления и улучшения управляемости. Рекомендация была принята, и после изменения схем регуляторы были настроены заново. Для определения параметров объекта и расчета настроек, как и для большинства других контуров, потребовалось проведение эксперимента с преднамеренным нанесением возмущения. Ранее на такой эксперимент никто бы не решился, но сейчас, когда все смежные и зависимые контуры уже были настроены оптимальным образом, они без проблем отработали нанесенное возмущение и оно не вызвало никаких негативных последствий: все параметры остались стабильны, что и стало значительным результатом всей предшествующей кропотливой работы по оптимизации процессов на установке моторных топлив.

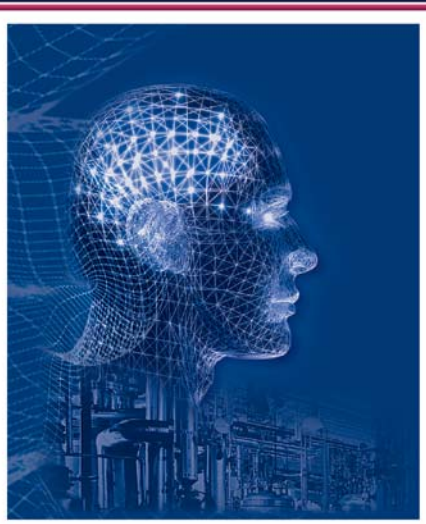
«Произошли существенные изменения, — говорит начальник смены Константин Фролов. — Раньше при сильных возмущениях, вызванных изменением состава сырья или другими факторами, операторам приходилось буквально вылавливать технологический процесс, что держало в напряжении весь персонал. Теперь заданный температурный профиль и обусловленные им точки выкипания стоят как вкопанные».

Итогом всего комплекса проведенных работ стало не только стабильное поведение всей установки и ее ключевых параметров. За счет стабильного поддержания температур на тарелках технологи получили возможность более точно управлять процессом разделения сырья, что позволило получить увеличение выхода высоколиквидных фракций на несколько процентов.

Этот результат был получен благодаря применению современных технологий автоматизации в области настройки регуляторов, тесного сотрудничества специалистов разного профиля и четкой организации работ.

«Когда мы начинали этот проект, то не могли точно знать, какие именно улучшения получим в итоге, — говорит главный технолог Антон Стуков. — Но у нас было твердое убеждение, что в оптимизации работы контуров регулирования заложен потенциал по повышению эффективности всего технологического процесса. Теперь, когда мы получили хороший результат, можно с уверенностью сказать, что мы будем и дальше совершенствовать наш подход к оптимизации процессов и переносить полученный опыт на другие установки». ●

В РАМКАХ МЕЖДУНАРОДНОГО ПРОМЫШЛЕННОГО ФОРУМА «РАДИОЭЛЕКТРОНИКА. ПРИБОРОСТРОЕНИЕ. АВТОМАТИЗАЦИЯ»



АВТОМАТИЗАЦИЯ

XVIII международная специализированная выставка

- ИКТ в промышленности • Системная интеграция
- Автоматизация производства • АСУ ТП
- Технические и программные средства автоматизации
- Измерение, контроль, испытание, диагностика
- Встраиваемые системы • Техническое зрение
- Мехатроника и робототехника
- Автоматизация зданий и ЖКХ
- САПР • Готовые отраслевые решения

21 – 23 ноября 2017

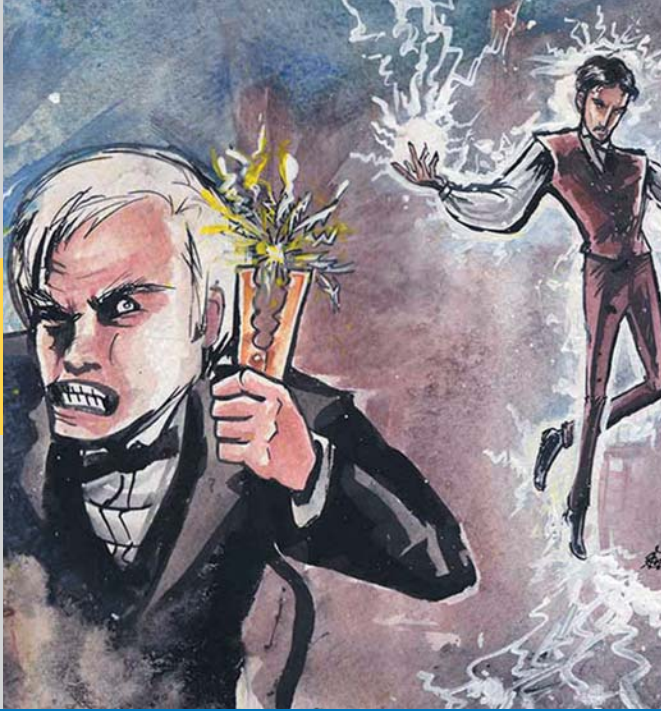
Санкт-Петербург, Петербургский СКК

Организатор выставки: FarEXPO IFE

Место проведения: Санкт-Петербург, ПСКК, пр. Ю. Гагарина, 8, м. "Парк Победы"
ais@farexpo.ru, www.farexpo.ru/ais, тел.: +7 (812) 777-04-07, 718-35-37

Реклама

АЛЕКСАНДР МИКЕРОВ,
д. т. н., проф. каф.
систем автоматического управления
СПбГЭТУ «ЛЭТИ»
a.mikerov@gmail.com



Переход в конце XIX века от первоначальной системы освещения с лампами накаливания Эдисона к современной трехфазной системе генерации, передачи и потребления электроэнергии сопровождался ярким публичным противостоянием компаний, ученых и общества.

ВОЙНА ТОКОВ И ПОБЕДА ПЕРЕМЕННОГО ТОКА

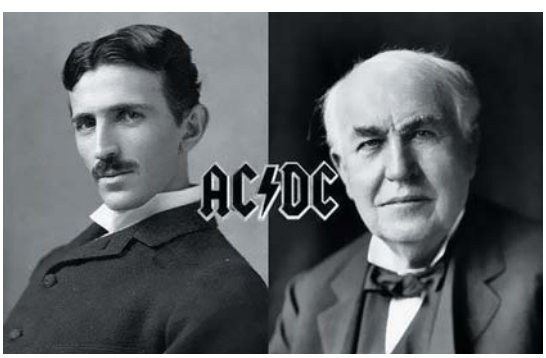


РИС. 1. ▲
Война токов

Под «войной токов» обычно понимают вражду двух крупнейших электротехнических компаний — Эдисона и Вестингауза, внедрявших различные системы электроснабжения. Также это словосочетание отражает идейное соперничество двух великих изобретателей — Томаса Эдисона и Николы Теслы, эти системы предложивших (рис. 1).

Однако картина будет неполной, если не упомянуть и о другой «войне», называемой иногда «битвой славянинов», в которой Михаил Осипович Доливо-Добровольский противопоставил двухфазной системе Тесла свою трехфазную, послужившую основой для современной структуры генерации, передачи и использования электроэнергии.

Война разгорелась в связи с появлением электрического освещения лампами накаливания Эдисона, запатентованными в 1880 г. и ставшими всемирно известными благодаря электротехнической выставке в Париже в 1881 г. [1]. Эта система предполагала, по существу, освещение целого квартала потребителей (П) от одной тепловой электростанции с генератором (Г) постоянного тока, первая из которых была пущена на Перл-стрит в Нью-Йорке в 1882 г. (рис. 2а). Поскольку длина линии электропередачи (ЛН) низкого напряжения 110 В составляла не более 1,5 км, то, очевидно, такие локальные электростанции не могли обеспечить электроснабжение целого города, а тем более удаленных районов страны.

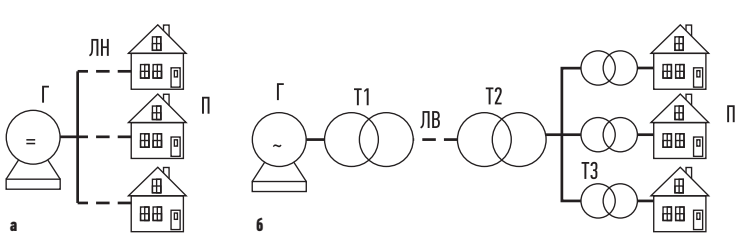


РИС. 2. ▶
Системы постоянного (а) и переменного (б) тока

Сразу же появились конкурирующие компании, которые, опираясь на европейский опыт (в частности, компании «Гейнц и Ко»), предложили централизованное (называемое тогда трансформаторным) электроснабжение однофазным переменным током от крупных электростанций любого типа (например, гидравлических) с генератором (Г) переменного тока через высоковольтные линии передачи (ЛВ) с повышающим (Т1) и понижающим (Т2) трансформаторами, а также дополнительными понижающими трансформаторами (Т3) потребителей (П) (рис. 2б) [2]. Одним из таких серьезных конкурентов Эдисона стала компания Вестингауза, вошедшая в электротехнический бизнес в 1884 г., закупив европейские патенты на трансформаторы. Почувствовав угрозу, Эдисон попытался нащупать слабые места конкурентов и увидел их в опасности поражения электрическим током высокого напряжения, без которого дальняя передача электроэнергии в те времена была практически невозможна.

К концу 1880-х гг. крупные города покрылись густой сетью телеграфных, телефонных и осветительных линий на столбах (включая линии дугового освещения в 3000 В), до сих пор портящих вид американских городов (рис. 3).

Газеты действительно были наполнены описаниями порой душераздирающих случаев поражения электрическим током ремонтников генераторов и линий и обычных пешеходов от упавших проводов. Общественную панику вызвала гибель в 1889 г. монтера телеграфной компании, замкнувшего высоковольтные провода и заживо сгоревшего на столбе в деловой части Манхэттена на глазах многочисленной, охваченной ужасом публики и работников муниципалитета [3]. Хотя несчастные случаи были связаны как с переменным, так и с постоянным током, Эдисон сознательно выбрал своей мишенью переменный ток (рис. 1). По современным представлениям, при напряжении до 500 В опаснее переменный ток, а более 500 В — постоянный [4]. Важно отметить, что по системе Эдисона напряжение подавалось большей частью по подземным кабелям.

Непосредственным поводом к началу войны послужили дебаты о высшей мере наказания — электрическом стуле [3]. История введения этого способа казни началась в 1882 г., когда американский дантист Альфред Саутвик (Alfred Southwick), проведя опыты на собаках, предложил заменить повешение более гуманной, по его мнению, казнью электрическим током. Эту тему подхватил электротехник Гарольд Браун (Harold Brown), который при поддержке Эдисона, предоставившего ему свою лабораторию, организовал серию публичных умерщвлений собак, лошадей и даже слона, показав, например, что собаки погибали уже при напряжении в 300 В переменного тока, тогда как при постоянном токе для этого требовалось в три раза большее напряжение. Желая связать ужасы убийства электрическим током с именем своего основного конкурента, Эдисон настоял на использовании в опытах высоковольтных генераторов Вестингауза, которые были приобретены через постороннюю компанию, поскольку сам Вестингауз был категорически против всякой смертной казни. Эдисон предпочитал называть эти процедуры «Westinghoused», т. е. умерщвлением токами Вестингауза.

В результате в 1888 г. штатом Нью-Йорк был принят закон об электрическом стуле с рекомендуемым напряжением 750–1500 В переменного тока. Стул, конструкция которого была создана тюремным ведомством совместно с лабораторией Эдисона, впервые был применен в 1890 г. для публичной казни некоего Вильяма Кеммлера (William Kemmler), убившего свою жену топором (рис. 4). Она произвела весьма тягостное впечатление, поскольку мучительная смерть наступила только со второй попытки. Вестингауз прокомментировал происшедшее словами: «Лучше бы они сделали это топором» [3].

На волне последовавшего общественного возмущения сторонники Эдисона предлагали законодательно разрешить только подземные сети с напряжением не более 300 В, что лишало бы системы переменного тока всякого экономического смысла. Однако первая же попытка введения подобных мер зимой 1889 г. погрузила все улицы Нью-Йорка в полную темноту, после чего было решено ограничиться только ужесточением требований электробезопасности.

Война токов не обошла и Россию, где электрическое освещение изначально строилось на постоянном токе [2]. Когда же в 1889 г. компания «Гейнц и Ко», опираясь на свой успешный опыт освещения одесской оперы, предложила создать систему переменного тока и для Москвы, в печати началась шумная кампания противников такой трансформаторной системы, доказывавших ее еретичность, опасность и безусловную гибельность для России [5].

Вернемся в США. Несмотря на мнимое преимущество, сторонники Эдисона ничего не могли противопоставить основному достоинству систем переменного тока — передаче энергии на любые расстояния. В 1893 г. компания Вестингауза выиграла заказ на электрификацию Чикагской выставки, а в 1895 г. завершила строительство самой большой по тем временам Ниагарской электростанции [2, 3, 6]. Однако постепенно у двухфазной системы Теслы стали выявляться недостатки, такие как повышенный расход меди для дальних передач, невысокие характе-

РИС. 3. ▲
Уличная проводка

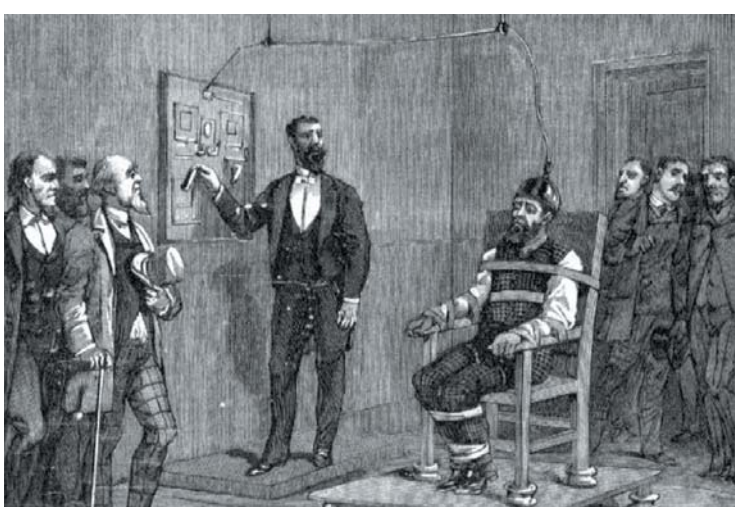


РИС. 4. ◄
Казнь Кеммлера

РИС. 5. ▶ М. О. Доливо-Добровольский (1862–1919)

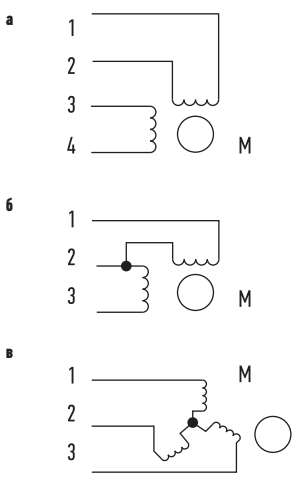


РИС. 6. ▶ Подключение двигателя к линии

ристики конструкций асинхронных двигателей и невозможность регулирования их скорости. Для формирования современного вида системы генерации, передачи и использования электроэнергии решающее значение приобрели работы выдающегося инженера-электрика М. О. Доливо-Добровольского [5–7].

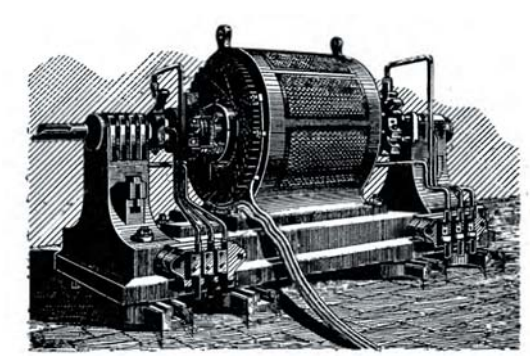


РИС. 7. ▼ Асинхронный двигатель Доливо-Добровольского

Михаил Осипович Доливо-Добровольский (рис. 5), происходивший из русско-польского дворянского рода, родился в Гатчине. Учился сначала в Рижском политехническом институте, а затем в Дармштадском высшем техническом училище (Германия). С 1887 г. и до конца жизни работал в компании AEG в Берлине, дойдя до поста технического директора. Доливо-Добровольский всегда сохранял связи с Россией, принимал активное участие в организации электромеханического отделения Петербургского политехнического института, основанного в 1902 г., и сотрудничал с ЭТИ (ЛЭТИ), по инициативе которого впоследствии ему было присвоено звание почетного инженера-электрика.

Желая найти нишу для компании AEG, Доливо-Добровольский тщательно изучил работы Теслы, начав с многофазных систем электропередачи. На рис. 6 приведены три самые распространенные линии электропередачи, питающие асинхронные электродвигатели (М): двухфазная четырехпроводная (а), двухфазная трехпроводная (б) и трехфазная трехпроводная (в). Все эти системы были запатентованы Теслой, однако на практике он использовал только двухфазные. Для линий передачи, достигающих порой длины во много тысяч километров, важнейшими показателями являются число и масса соединительных проводов. Поэтому имеет смысл сравнивать только трехпроводные линии (б) и (в).

При трехфазной линии (в) токи во всех проводах и фазах сдвинуты на 120°, но имеют одинаковую амплитуду. При двухфазной линии (б) с общим проводом (2) токи в проводах (1) и (3) равны:

$$i_1 = i_m \sin\omega t;\ i_3 = i_m \sin(\omega t + 90°),$$

где i_m — амплитуда тока и ω — его частота. Тогда в общем проводе (2) ток равен их сумме:

$$i_2 = i_1 + i_3 = \sqrt{2}\sin(\omega t + 45°).$$

Таким образом, провод (2) должен иметь сечение на 41% больше, нежели провода (1) и (3). И вот это обстоятельство, на которое первым обратил внимание Доливо-Добровольский в 1891 г., приводило к существенной экономии меди проводов и было решающим преимуществом трехфазных линий передачи и систем переменного тока [5].

Доливо-Добровольский не ограничился передачей электроэнергии, он создал и запатентовал такие важнейшие и общепринятые сейчас устройства многофазных систем, как:

- асинхронный двигатель с ротором типа «беличья клетка» (1889 г.);
- распределенные обмотки якоря машин переменного тока (у Теслы обмотки были сосредоточенными, катушечными);
- первый асинхронный двигатель регулируемой скорости с обмоткой ротора, подключенной через контактные кольца к пускорегулирующему реостату;
- трехфазный трансформатор (1889 г.); до него в трехфазной линии использовали три однофазных трансформатора.

Широкому внедрению трехфазных систем весьма способствовал блестящий успех Доливо-Добровольского на электротехнической выставке во Франкфурте 1891 г., для которой он построил трехфазную линию передачи на 16 кВ из города Лауфен (в 175 км от Франкфурта), от генератора с водяной турбиной на 300 л. с. [5–8]. Это позволило зажечь на выставке 1100 ламп накаливания и запустить самый мощный по тем временам трехфазный асинхронный двигатель в 100 л. с. (рис. 7) с водяным насосом, питающим эффектный девятиметровый водопад, который демонстрировал возможность передачи механической энергии на расстояние.

Так закончилась битва «двух славянинов» (Теслы и Доливо-Добровольского), положившая конец и всей войне токов. К тому же, инициатор этой войны, Эдисон, после создания в 1892 г. компании General Electric (путем слияния его компании с компанией Thomson-Houston) потерял интерес к освещению, переключившись на обогащение руд. А сама эта компания после прихода в нее выдающегося электротехника Чарльза Штейнмеца резко поменяла курс, став активной сторонницей трехфазных систем и уже при строительстве Ниагарской электростанции получив подряд на трехфазную линию электропередачи в г. Буффало напряжением 11 кВ [3, 8, 9].

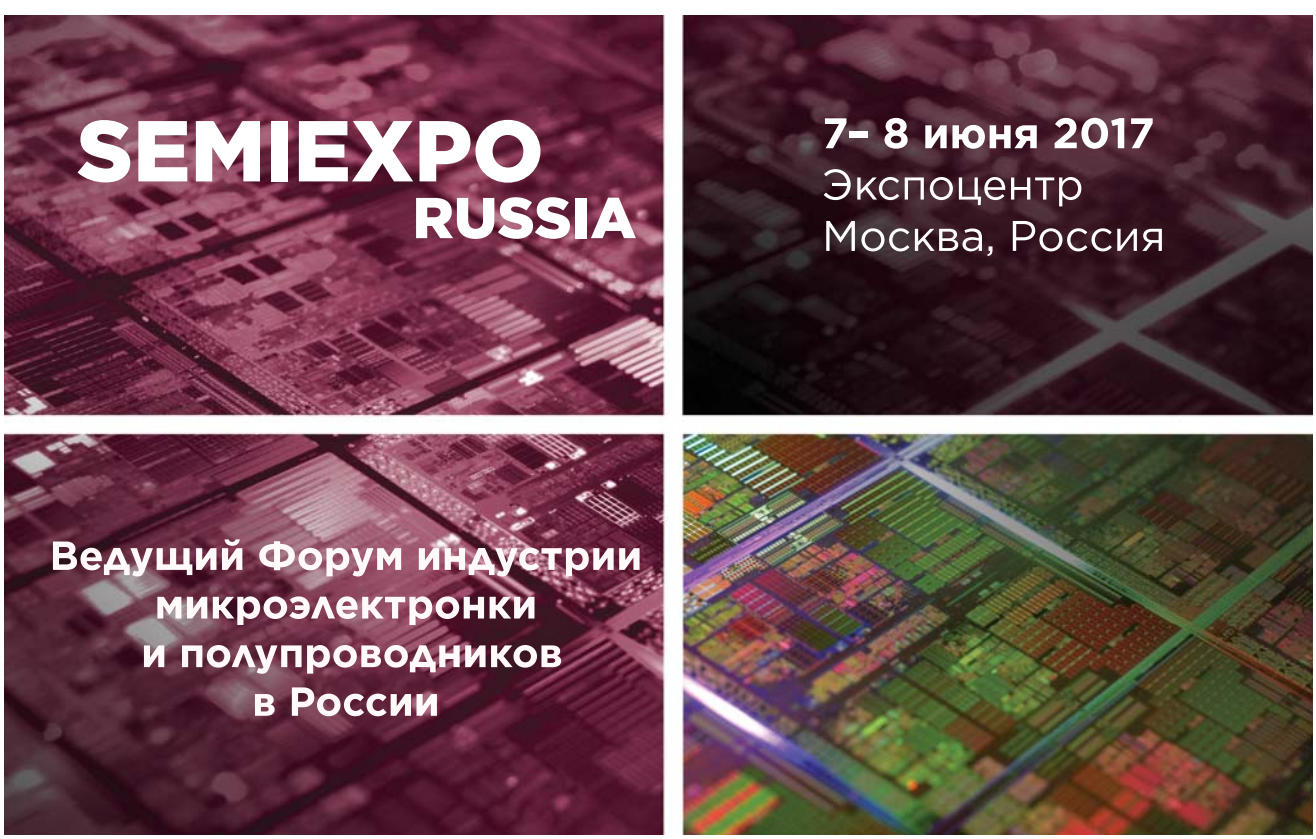
Однако датой окончательной победы переменного тока считается 2007 г., когда Нью-Йорк полностью перешел с постоянного тока на переменный [3, 9]. Тем не менее многие специалисты считают, что нас ждет

ренессанс систем постоянного тока [9]. Это связано, конечно же, с развитием электроники, которое привело к созданию мощных полупроводниковых устройств преобразования как рода тока (AC/DC), так и уровня напряжения, в результате чего на расстоянии более 1000 км линии электропередачи сверхвысокого напряжения (сотни киловольт) постоянного тока становятся экономически более выгодными. Кроме того, в системы постоянного тока легче интегрируются все возобновляемые источники электроэнергии (ветровые, солнечные и др.), а кабельные линии электропередачи также строятся преимущественно на постоянном токе. С другой стороны, все технические системы в промышленности, на транспорте и в быту становятся все более интеллектуальными на базе компьютерной техники и регулируемых электроприводов постоянного и переменного тока. Все они требуют источников питания постоянного тока. Таким образом, скорее всего война токов еще не закончена. ⬣

- Война токов — это борьба двух принципов электроснабжения: локального (Эдисона) с питанием от местной низковольтной электростанции постоянного тока и централизованного (Вестингауза) в виде сети переменного тока с высоковольтными линиями электропередачи.
- Главным аргументом сторонников Эдисона была сравнительно бóльшая опасность высоковольтного оборудования переменного тока, подтвержденная опытами Брауна на живых существах, а также первой публичной казнью на электрическом стуле.
- Но решающее преимущество системы Вестингауза — возможность электропитания множества удаленных потребителей — привело на первом этапе войны к ее победе в виде двухфазной системы, разработанной Теслой.
- Завершающий этап войны, «битва славянинов», ознаменовал переход к современной структуре мирового электроснабжения на базе трехфазной системы Доливо–Добровольского.
- Однако развитие электроники и ее широкое применение делает вероятным ренессанс в недалеком будущем систем передачи и распределения электроэнергии постоянного тока.

ЛИТЕРАТУРА

1. Микеров А. Г. Торжество постоянного тока и роль Томаса Эдисона // Control Engineering Россия. 2016. № 4 (64).
2. Микеров А. Г. Никола Тесла и передача электроэнергии переменным током // Control Engineering Россия. 2016. №5 (65).
3. Война токов. https://en.wikipedia.org/wiki/War_of_Currents
4. Пиголкин Ю.И. и др. Судебная медицина. М.:ГЭОТАР-МЕД. 2002.
5. Электротехника переходит на переменный ток. www.famhist.ru/famhist/klasson/000c6e49.htm#000e59a4.htm
6. Белькинд Л. Д. и др. История энергетической техники. М.-Л.: Госэнергоиздат. 1960.
7. Бутюгина А. А., Микеров А. Г. Выдающийся инженер-электрик Михаил Осипович Доливо-Добровольский (к 150-летию со дня рождения) // Известия СПбГЭТУ «ЛЭТИ». 2012. №7.
8. Герман-Галкин С. Г. Карл Август Штейнмец — ученый, инженер, конструктор, изобретатель, педагог// Control Engineering Россия. 2015. №6 (60).
9. Зотин О. В преддверии возрождения постоянного тока // Силовая электроника. 2013. № 3, 4, 6.



Реклама

XIII МОСКОВСКИЙ МЕЖДУНАРОДНЫЙ ИННОВАЦИОННЫЙ ФОРУМ

ТОЧНЫЕ ИЗМЕРЕНИЯ — ОСНОВА КАЧЕСТВА И БЕЗОПАСНОСТИ

проводится в соответствии с распоряжением Правительства Российской Федерации от 5 апреля 2014 г. № 541-р

17-19 мая 2017 г., Москва, ВДНХ, павильон 75, «Россия»

СПЕЦИАЛИЗИРОВАННЫЕ ВЫСТАВКИ

MetrolExpo
Control&Diagnostic
ResMetering
LabTest
PromAutomatic

ЦЕЛИ И ЗАДАЧИ

Консолидация усилий власти, науки и бизнеса в развитии отечественного приборостроения для обеспечения нужд промышленности и оборонного комплекса страны, а также повышение эффективности российской системы измерений, совершенствование нормативной базы метрологии с учетом международных тенденций в целях поддержки инноваций и их продвижения.

ДИРЕКЦИЯ ФОРУМА

129344, Москва, ул. Искры 31, корп. 1, Технопарк ВДНХ
Тел./Факс: +7 (495) 937-40-23 (многоканальный)
www.metrol.expoprom.ru
E-mail: metrol@expoprom.ru

ПРОГРАММА ФОРУМА

METROLEXPO-2017
Метрология и Измерения
13-я выставка средств измерений, испытательного оборудования и метрологического обеспечения.

CONTROL&DIAGNOSTIC-2017
Контроль и Диагностика
6-я выставка промышленного оборудования и приборов для технической диагностики и экспертизы.

RESMETERING-2017
Учёт энергоресурсов
6-я выставка технологического и коммерческого учета энергоресурсов.

LABTEST-2017
Лабораторное оборудование
5-я выставка аналитических приборов и лабораторного оборудования промышленного и научного назначения.

PROMAUTOMATIC-2017
Автоматизация
5-я выставка оборудования и программного обеспечения для производственных процессов.

WEIGHT SALON 2017
Весовой салон
Выставка весового оборудования.

Организаторы
МИНПРОМТОРГ РОССИИ
РОССТАНДАРТ

Поддержка
АППАРАТ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Стратегический партнер
РОСТ МОСКВА

Генеральный спонсор
KEYSIGHT TECHNOLOGIES

Ключевые партнеры выставки
РОСАТОМ · РОСНАНО · РЖД · КРЭТ · ТПП РФ

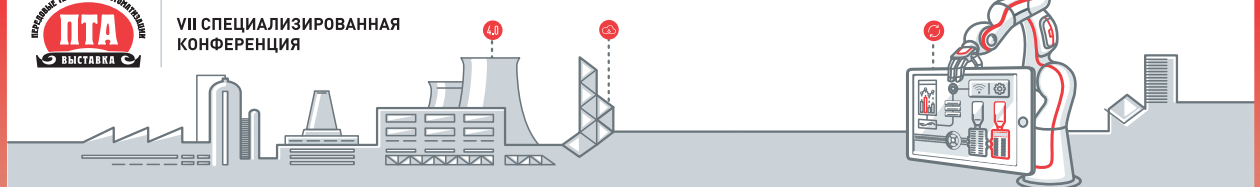
Международные партнеры
Bureau International des Poids et Mesures · OIML · COOMET

Устроитель и выставочный оператор
Экспострой

Реклама

ПТА ВЫСТАВКА
ПЕРЕДОВЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ

VII СПЕЦИАЛИЗИРОВАННАЯ КОНФЕРЕНЦИЯ



АПСС-СИБИРЬ 2017

АВТОМАТИЗАЦИЯ: ПРОЕКТЫ. СИСТЕМЫ. СРЕДСТВА

24 МАЯ 2017 / НОВОСИБИРСК, БЦ «РЕЧНОЙ ВОКЗАЛ»

ТЕМАТИЧЕСКИЕ СЕКЦИИ:

- Промышленная автоматизация: на пути к Industry 4.0
- Импортозамещение: от контроллера до облака
- Smart City: технологии и новые возможности

В деловой программе актуальные доклады, презентации,интенсивные тренинги. Сертификат по итогам тренинга

УЧАСТНИКИ ПРОШЛЫХ КОНФЕРЕНЦИЙ

BALLUFF sensors worldwide · OMRON · PHOENIX CONTACT · ProSoft · Rockwell Automation · TORNADO MODULAR SYSTEMS

Организатор Экспотроника
info@pta-expo.ru / www.pta-expo.ru

Реклама

КОЛЛЕКТИВНЫЙ СТЕНД РОССИЙСКОЙ ФЕДЕРАЦИИ НА МИРОВОМ НЕФТЯНОМ КОНГРЕССЕ

УСПЕЙТЕ ПРИНЯТЬ УЧАСТИЕ В ГЛАВНОМ МЕРОПРИЯТИИ НЕФТЕГАЗОВОЙ ОТРАСЛИ

ПРЕИМУЩЕСТВА УЧАСТИЯ

ВЫГОДНОЕ РАСПОЛОЖЕНИЕ

Расположение на центральной аллее, обеспечит дополнительное внимание представителей мировых СМИ, официальных лиц и делегатов

ПОСЕЩЕНИЕ СТЕНДА ОФИЦИАЛЬНОЙ ДЕЛЕГАЦИЕЙ

Коллективный стенд будет включен в официальный обход с представителями уровня Министров и заместителей Министров

9-13 ИЮЛЯ 2017 | СТАМБУЛ

www.wpc2017.ru

Электрификация
выставочный павильон

8 (499) 760-34-74

Реклама

СДЕЛАНО
В РОССИИ!
MasterSCADA
3.X/4D
Работает
24X7X365
с 2002
38 отраслей
12 стран
50000+ инсталляций
300+ рабочих мест в одной системе
100000+ параметров на один сервер
ИнСАТ
www.insat.ru
+7 (495) 989 22 49
scada@insat.ru

Реклама