ISSN 0206 975X

# СТА

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ

3'2018

ЭЛЕКТРОННАЯ ВЕРСИЯ НА САЙТЕ

WWW.CTA.RU

## ПОБЕЖДАЕМ ЧУЖИЕ КОМПЛЕКСЫ:
отечественные разработки для АСУ ТП

## КУБИКИ ДЛЯ ВЗРОСЛЫХ:
железнодорожные системы SIL-4 из готовых блоков

## ЗДОРОВОЕ ПИТАНИЕ:
программируемые источники для профессиональных применений

## ВСЕ НА ВОЙНУ С BOTNET:
подавить бунт вещей в зародыше

## НЕ НАСТУПИТЬ НА ГРАБЛИ:
какие стандарты в основе вашей системы?



Скачайте диск: tp.prosoft.ru/cta-3-2018

# НОВОЕ ПОКОЛЕНИЕ
## ПРОГРАММИРУЕМЫХ ИСТОЧНИКОВ ПИТАНИЯ

Серия GENESYS™+

**5 кВт** (0...600 В / 0...500 А)

LAN / USB / RS-232 / RS-485

Масштабирование до 20 кВт


TDK·Lambda

PROSOFT®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

УЗНАТЬ БОЛЬШЕ

Fastwel

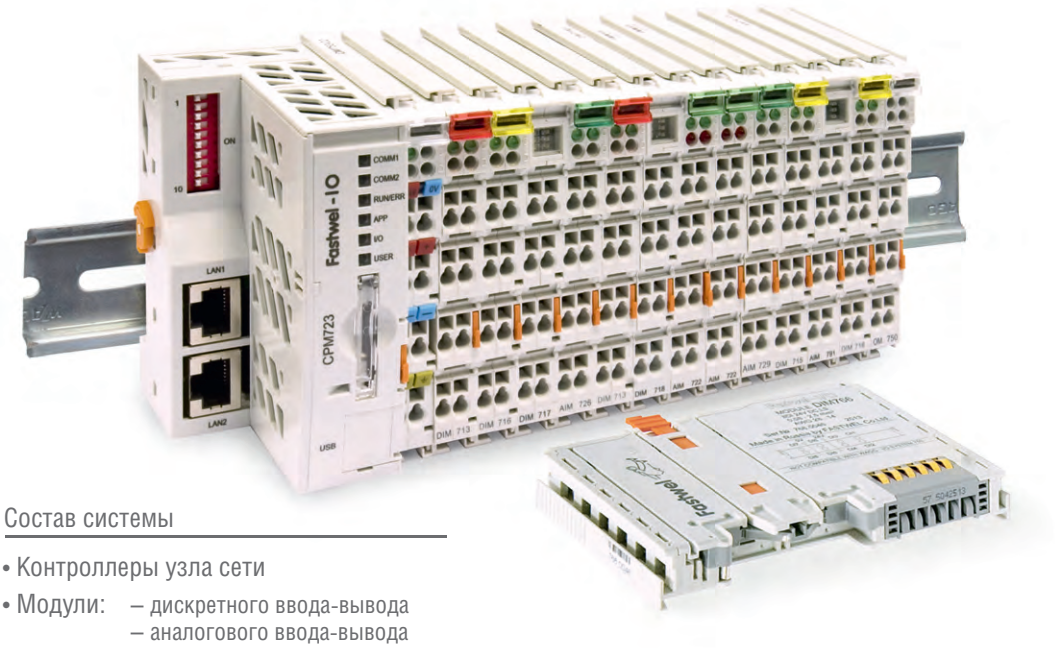
Российская электроника для ответственных применений

# Распределённая система ввода-вывода FASTWEL I/O

МОРСКОЙ РЕГИСТР
ПОЖАРНЫЙ СЕРТИФИКАТ
СЕРТИФИКАТ СООТВЕТСТВИЯ
РЕЕСТР СРЕДСТВ ИЗМЕРЕНИЙ

–40...+85°C

95%




Состав системы

- Контроллеры узла сети
- Модули:
  - дискретного ввода-вывода
  - аналогового ввода-вывода
  - измерения температуры
  - сетевых интерфейсов

## Модульный программируемый контроллер

- Процессоры 500/600 МГц
- Встроенный и внешний флэш-накопители объёмом до 32 Гбайт
- Энергонезависимая память 128 кбайт с линейным доступом
- Бесплатная адаптированная среда разработки приложений CODESYS
- Часы реального времени
- Сервис точного времени на базе GPS/GLONASS PPS
- Модули ввода-вывода с контролем целостности цепей

CPM711
- Протокол передачи данных CANopen
- Сетевой интерфейс CAN

CPM712
- Протокол передачи данных Modbus RTU, DNP3
- Сетевой интерфейс RS-485

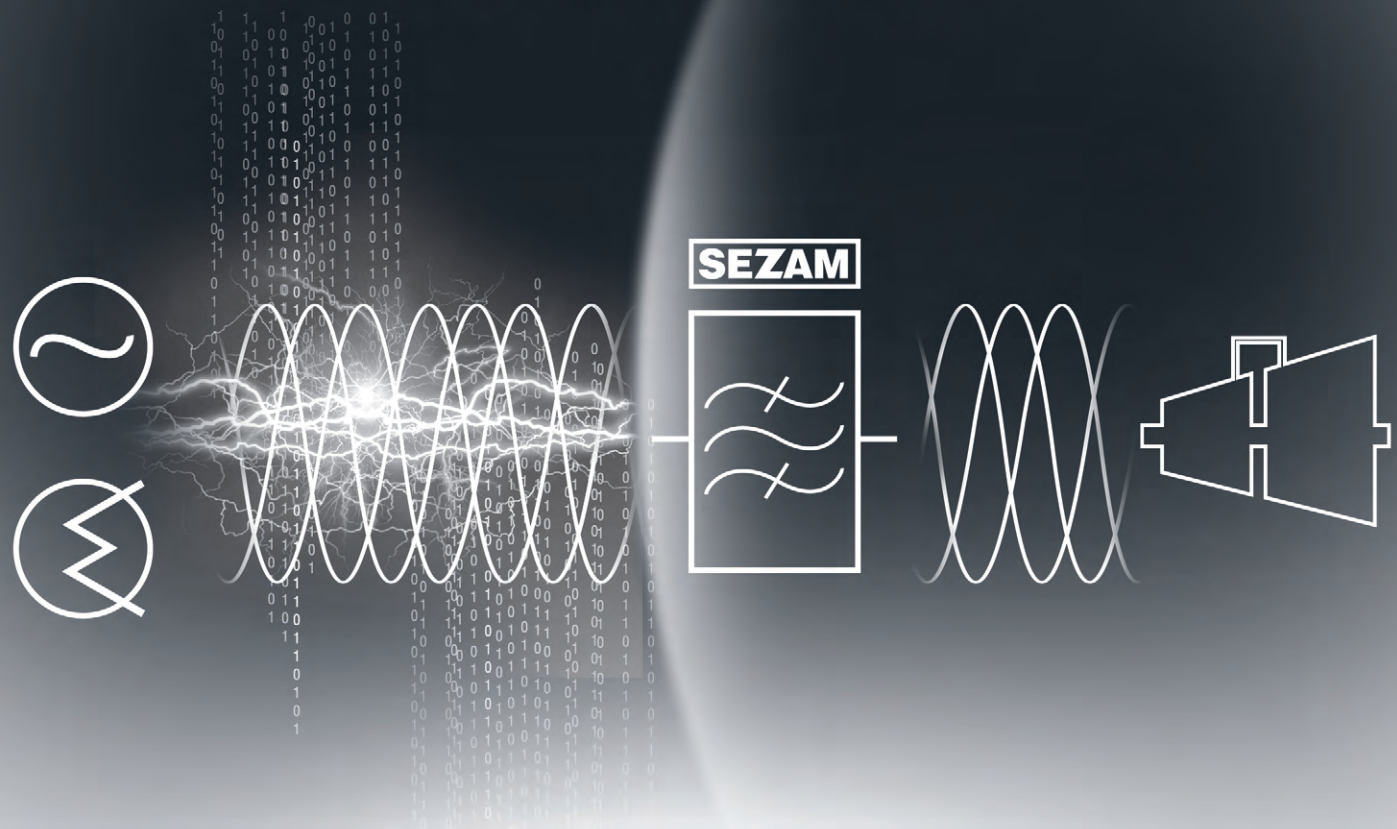
CPM713
- Протокол передачи данных Modbus TCP, DNP3
- Сетевой интерфейс Ethernet

CPM723
- Протоколы передачи данных Modbus TCP/RTU
- Сетевой интерфейс 2×Ethernet

www.fastwel.ru

SEZAM

# Там, где ИБП бессильны





## Сетевой защитный модуль SEZAM

### Параметры

- вход 220, 380 В
- мощность 3, 5, 10, 15 кВт
- рассеиваемая энергия импульсов перенапряжения до 20 кДж

### Защита от

- повышенного напряжения
- импульсов от 4,5 до 10 кВ и разрядов молнии
- последствий обрыва нулевого провода
- преднамеренных электромагнитных воздействий

ProSoft®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

СТА®
СОВРЕМЕННЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ

Производственно-практический журнал
«Современные технологии автоматизации»

Главный редактор С.А. Сорокин

Зам. главного редактора Л.И. Турок
Редактор О.И. Семёнова
Редакционная коллегия А.П. Гапоненко,
А.В. Головастов,
В.К. Жданкин,
К.В. Кругляк,
В.М. Половинкин,
Д.П. Швецов,
В.А. Яковлев

Дизайн и вёрстка А.Ю. Хортова,
К.В. Седов
Служба рекламы Н.В. Кушниренко
E-mail: knv@cta.ru

Учредитель и издатель ООО «СТА-ПРЕСС»
Генеральный директор К.В. Седов
Адрес учредителя, издателя и редакции:
ул. Чертановская, д. 50, корп. 1, г. Москва, 117534

Служба распространения И.С. Лобанова
E-mail: info@cta.ru
Почтовый адрес: 119313, Москва, а/я 26
Телефон: (495) 234-0635
Факс: (495) 232-1653
Web-сайт: www.cta.ru
E-mail: info@cta.ru

Выходит 4 раза в год
Журнал издаётся с 1996 года
№ 3'2018 (88)
Дата выхода в свет 18.06.2018
Тираж 10 000 экземпляров

Издание зарегистрировано в Комитете РФ по печати
Свидетельство о регистрации № 015020 от 25.06.1996 г.
Подписные индексы по каталогу «Роспечати» – 72419, 81872
ISSN 0206-975X
Свидетельство № 00271 000 о внесении в Реестр
надёжных партнёров Торгово-промышленной палаты
Российской Федерации

Свободная цена

Отпечатано: ООО «МЕДИАКОЛОР»
Адрес: Москва, Сигнальный проезд, 19, бизнес-центр Вэлдан
Тел. +7 (499) 903-6952



## Уважаемые друзья!

Начнём с краткого ответа на часто задаваемый вами вопрос: «Как и на каких условиях можно подписаться на журнал „СТА“?»

Если вы специалист в области автоматизации и хотели бы получать журнал регулярно, аккуратно заполните форму на нашем сайте www.cta.ru – и бесплатная подписка у вас в кармане!

Сегодня основная мировая конкуренция разворачивается не на военном, а на технологическом фронте. Технологии полностью определяют все стороны нашей жизни. Степень независимости от импорта технологий является индикатором силы и влияния любого государства в современном обществе, и выигрывает тот, у кого в запасе имеются лучшие и наиболее прогрессивные из них. Роль локомотива в этих процессах всегда играет промышленная автоматизация, поэтому мы снова и снова возвращаемся к важной для нашей страны идее импортозамещения. Отечественные компании «ИнСАТ» и «Адвантикс» представили совместную разработку – универсальный программно-технический комплекс для решения задач АСУ ТП. Он реализован на базе российских промышленных серверов AdvantiX и ПО MasterSCADA. О преимуществах применения продукции ещё одного отечественного производителя – компании «ФАСТВЕЛ» – вы прочтёте в статьях о распределённой системе управления газораспределительной станции и об управлении климатическим стендом. Кстати, вы сможете ознакомиться и с особенностями программирования контроллеров FASTWEL CPM723-01 в среде разработки CODESYS V3.

Скорее всего, вам уже известна немецкая компания MEN Mikro Elektronik. Мы расскажем об уникальной концепции создания сверхнадёжных систем автоматизации для железных дорог путём компоновки предварительно запрограммированных и сертифицированных блоков на основе модульной платформы menTCS.

Компания AU Optronics специализируется на производстве высококачественных промышленных дисплеев и решений для солнечной энергетики. Представляем вашему вниманию обзор её продукции.

В необходимости промышленных стандартов сегодня никто не сомневается, но их разработка – дело крайне непростое, а уж внедрение и подавно сопряжено с массой сложностей. Кто и как способствует современной стандартизации, читайте в нашем журнале.

В источниках питания нуждаются все электрические и электронные устройства. Это значит, что используются они практически повсеместно, а конкуренция на рынке их производства весьма высока. Но программируемые источники питания образуют отдельную специфическую нишу. Об особенностях и применении программируемых источников и электронных нагрузок мы расскажем на примере изделий компании EA Elektro-Automatik. Энергоэффективное промышленное оборудование способно экономить немалые средства и сберегать окружающую среду. Мы возвращаемся к теме энергоменеджмента и в продолжение статьи о нечётком управлении в оптимизации энергопотребления публикуем материал об основах структурно-функциональной организации встроенных и автономных нечётких систем управления технологическим оборудованием.

Продолжая цикл статей о тонкостях и секретах работы со SCADA GENESIS64, предлагаем вам примеры простой реализации задач, иллюстрирующие гибкость и универсальность этой системы.

Всего вам доброго!

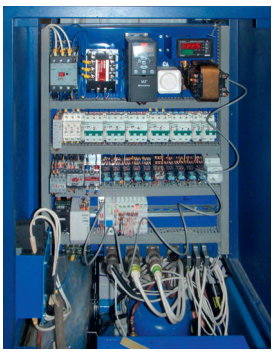
С. Сорокин

# СОДЕРЖАНИЕ 3/2018

## РАЗРАБОТКИ

### КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ СИСТЕМЫ





## АППАРАТНЫЕ СРЕДСТВА

### ОТОБРАЖЕНИЕ ИНФОРМАЦИИ

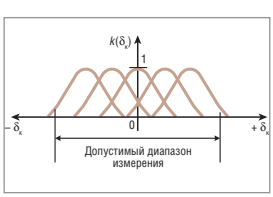


### СТАНДАРТИЗАЦИЯ И СЕРТИФИКАЦИЯ



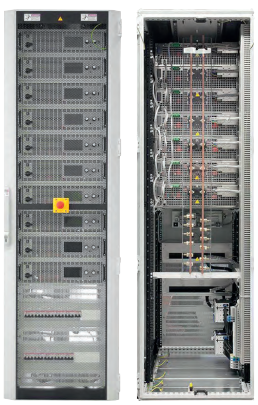
### В ЗАПИСНУЮ КНИЖКУ ИНЖЕНЕРА





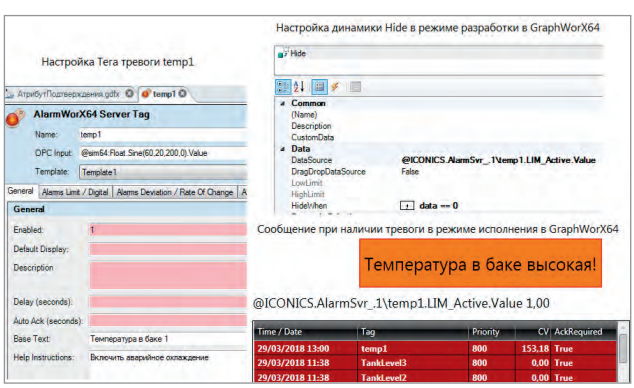


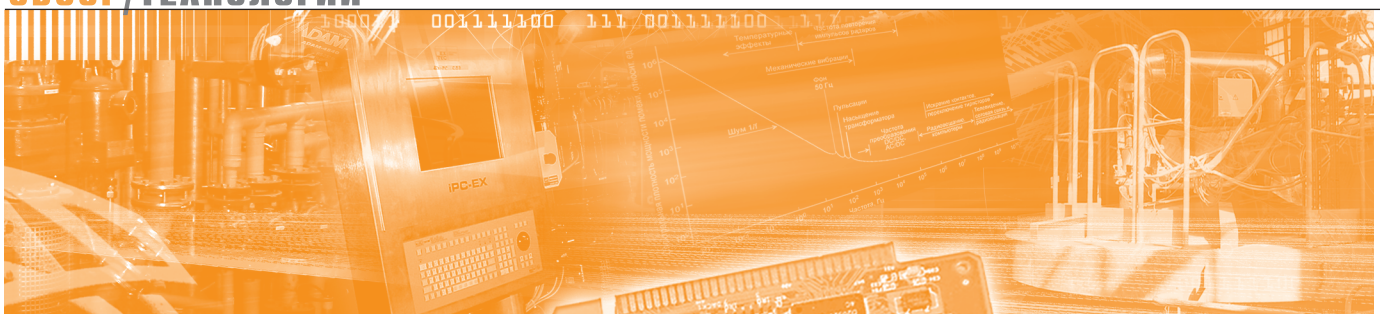


### ВОПРОСЫ–ОТВЕТЫ







*Карен Кроули, Роберт Андрес*

# Безопасность в мире IoT

**В статье рассмотрены вопросы обеспечения безопасности и противодействия киберугрозам в сетях IoT в свете бурного и бесконтрольного развития Интернета вещей. Приводятся основные требования к организации безопасных систем IoT, а также продемонстрирован комплексный подход к решению проблемы на примере концепции компании Eurotech.**

Автомобили без водителей, фитнес-трекеры, умные промышленность и сельское хозяйство, умная одежда, умные приборы и сенсоры для контроля всего на свете, медицинское оборудование, помогающее людям, где бы они ни находились, – всё это Интернет вещей.

Интернет вещей изменяет принципы ведения бизнеса, общественных связей и отношений, сам уклад нашей жизни (рис. 1). По мере лавинообразного роста подключаемых к Интернету устройств и совершенствования технологий мы приближаемся к практическим результатам, предсказываемым ведущими экспертами:

- Gartener, Inc. прогнозирует, что к 2020 году в единой сети будет уже 20,8 млрд устройств;
- По мнению IDC, рынок Интернета вещей к тому же 2020 году вырастет до $1,7 трлн;
- Business Insider считает, что порядка $6 трлн будет потрачено во всём мире только в ближайшие пять лет;
- А вот European Commission полагает, что только европейский рынок IoT в 2020 году составит около 1 трлн евро.

Одной из проблем, с которыми мы сталкиваемся в процессе внедрения технологий IoT, является ограничение скоростей связи устройств между собой, а также их слабая защищённость и вообще отсутствие единых стандартов сетевой безопасности. IoT сегодня – поистине лакомый кусочек для хакеров и террористов всех мастей. И если ситуация не изменится, то техническая революция может привести рано или поздно к техногенной катастрофе. Факты таковы, что в настоящее время около 66% сетей имеют серьёзные уязвимости, а к 2020 году до 10% хакерских атак будет нацелено именно на устройства IoT, что также немало. Далее мы постараемся показать вам, как компания **Eurotech** предлагает бороться с этими угрозами.

**Рис. 1. Интернет вещей меняет уклад нашей жизни**

## Сегодняшняя ситуация с киберугрозами

Нынешняя ситуация с киберугрозами по-настоящему серьёзна. По мере увеличения числа подключённых к сети устройств, разрастания облачных сервисов и внедрения технологий Big Data кибератаки становятся всё более масштабными и многочисленными. В результате мы наблюдаем ослабление защиты. И заметьте, речь уже не идёт о «если вас взломают» – речь идёт о «когда». Организации используют распределённые сети, которые гораздо сложнее защитить, нежели локальные. Для всех, кто пытается защитить свои активы, огромный объём незащищённых данных и устройств, который добавляется к этой проблеме безопасности благодаря IoT, весьма существенен. Кроме того, IoT привносит и новые направления кибератак, к которым мы не готовы. В рамках данной темы очень важно то, что речь идёт не об атаках на сетевую инфраструктуру, таких как DDoS-атаки, требующие глубоких знаний технологий и уязвимых мест сетевых протоколов, а об атаках на отдельные устройства, нарушающих их сетевую идентификацию и коммуникации между ними. Мы уже видели некоторые примеры атак такого рода и их плачевные результаты. Никто в настоящее время не защищён, и IoT-

ориентированные компании должны проявлять особую осторожность.

### Автомобильная промышленность

Печально известная атака Jeep, по сообщениям Wired, заставила Chrysler отозвать 1,4 млн автомобилей для исправления уязвимости ПО, позволяющей хакерам дистанционно получать доступ к автомобилям и управлять их жизненно важными функциями.

### Медицина

В Университете Южной Алабамы студенты могли попрактиковаться в «убийстве» виртуального пациента посредством получения доступа и дистанционного отключения его кардиостимулятора. Исследователь вопросов безопасности Билли Риос произвёл глубокий анализ механизма действия автоматизированной системы введения лекарственных препаратов производства фирмы Hospira и выяснил, что вполне реально дистанционно изменять дозы вводимых пациентам препаратов, что может привести к летальному исходу.

### Жильё

В дополнение к множеству историй о взломе умных лампочек мы уже имеем сведения об авариях вследствие нарушений взаимосвязей устройств, потенциально приводящих к неработоспособности систем безопасности жилища. Chamberlain Group, Inc. и Ooma Inc. зафиксировали аварии, вызванные нарушением в подключении IoT-устройств к соответствующим сервисам и приводившие к проблемам с безопасностью людей.

### Умная сетевая инфраструктура

Пока ещё не рассмотренная в этой статье умная сетевая инфраструктура, называемая также Smart Grid, также является потенциальной мишенью злоумышленников в рамках атак на IoT. Современные тенденции к распределённым системам контроля и мониторинга, глубоко внедряющиеся в нашу жизнь, также делают нас уязвимыми.

## Безопасность – основной критерий при внедрении IoT

Пока ваша сеть IoT остаётся локальной, вы не будете испытывать существенных проблем с безопасностью. Но беда в том, что в реальной жизни сети уже давно выросли до глобальных размеров, объединив инфраструктуры различных бизнесов и вобрав в себя множество устройств. Беда ещё и в том, что идея IoT эксплуатирует имеющиеся ресурсы Интернета, в силу многих причин являющиеся весьма уязвимыми и изначально не приспособленными для этих целей, поэтому безопасность IoT по своей природе является гораздо более сложной задачей, чем, например, безопасность в приложениях M2M.

Поскольку индустрия активно развивается и обновляется, мы наблюдаем бум подключения различных продуктов. Проблемой первых IoT-продуктов «из коробки» была их слабая защищённость. Такие устройства, к примеру, всегда поставляются с паролем по умолчанию вида «1234», они имеют открытые сервисы для подключения к ним извне (типа Telnet), легко взламываемое ПО, основанное на HTTP-запросах, а также миллионы других врождённых пороков. Из-за несовершенства стандартов защиты и отсутствия хороших практических примеров IoT имеет все шансы стать основной частью IT-бюджета департаментов безопасности, подрывая все остальные полезные инвестиции. Более того, проблемы безопасности IoT отвращают от этих технологий значительную часть потенциальных пользователей. Если государственные органы, владельцы бизнеса и рядовые пользователи не могут поверить в сохранность своих данных, они делают выбор в пользу более примитивных (но более надёжных в плане безопасности) технологий, а созданный прецедент существенно замедляет развитие IoT в будущем. В 2015 году на конференции IoT Security глава службы информационной безопасности ФБР Арлетт Харт предупредила, что угрозы IoT могут быть гораздо опаснее, чем это принято считать. По её словам, когда злоумышленники крадут коммерческую информацию организаций, это становится лишь новостями. Но когда они крадут персональные данные и идентификаторы, это уже угроза для жизни конкретных людей. Люди чувствуют свою незащищённость, а этого нельзя допустить.

## Botnet of Things

Один из опасных сценариев, появляющихся в последнее время, – IoT-Botnet-сети (Ботнет вещей). Они представляют собой группы взломанных компьютеров, а также умных IoT-устройств, объединённых злоумышленниками в криминальных целях. Бот, созданный из взломанного IoT-устройства, может рассылать спам или ссылки на хост с вредоносным контентом, и всё это без ведома владельца устройства. В 2013 году исследователь из компании Proofpoint, специализирующейся на вопросах секретности, обнаружил, что через шлюзы безопасности проходили сотни и тысячи спамовых писем. Proofpoint идентифицировала Botnet-атаки, в результате которых было скомпрометировано до ста тысяч устройств. Компания кибернетических исследований IID проанализировала миллионы фрагментов данных, распространяемых по сети, и сделала вывод, что огромное число IoT-устройств является частью вредоносной сети Botnet. IID предсказала, что к концу 2017 года владельцы сетей Botnet благодаря расширению границ произведут полномасштабное вторжение скомпрометированных устройств Интернета вещей, таких как носимые устройства и устройства умных домов, в нашу жизнь. Например, камеры CCTV уже сейчас идентифицируются в качестве источников DDoS-атак против банков и других целей.

Расширение возможностей устройств IoT, таких как автономные дроны, а также прочих умных приложений, тоже не добавляет уверенности в достаточности требований безопасности. Вице-президент IID по противостоянию киберугрозам Шон Тирни отмечает, что, так как эти устройства используются для первичных и ответных атак на другие сети, они могут стать родоначальниками «войны Ботнетов» за господство в среде IoT.

С появлением вредоносного кода Mirai сообщество Интернет испытало первые серьёзные последствия атак IoT-Botnet. Mirai – это программа, заражающая компьютерные системы на базе ОС Linux и превращающая их в дистанционно управляемые боты, которые затем можно было объединять и использовать для сетевых атак. После того как исходный код Mirai был открыто опубликован на одном из хакерских форумов, тут же появились его разнообразные клоны. Типичная мишень их – удалённые камеры и сетевые роутеры. Заражённые устройства непрерывно сканируют Интернет с целью поиска IP-адресов других подключённых устройств. Затем вирус пытается идентифицировать устройство и подключиться к нему, применяя стандартные заводские настройки логина и пароля. Если это удаётся сделать, устройство также заражается. Впервые Mirai был обнаружен в августе 2016 года и с тех пор стал основой самых разрушительных DDoS-атак. Примеры атак Mirai-BotNet – это и атака на DNS-

сервисы Dyn в октябре 2016 года, и атака на инфраструктуру Интернет Либерии в ноябре 2016 года, и, конечно, ситуация в том же ноябре 2016 года с выходом из строя благодаря клону Mirai миллиона роутеров Deutsche Telekom.

Ещё один пример вредоносного ПО, действующего в среде IoT, – Stuxnet. Это имя компьютерного червя, заражающего системы под управлением Windows и SCADA-системы Siemens, управляющие контроллерами этого производителя. Впервые червь проявил себя в 2010 году в компьютерной атаке, затормозившей работу ПО на иранском предприятии по обогащению урана. Это вполне могло привести к плачевным последствиям. Stuxnet атаковал систему Windows, используя как вновь обнаруженные, так и известные уязвимости этой ОС. Обычно червь распространялся посредством инфицированных съёмных USB-носителей данных, то есть «добровольными» разносчиками выступали сами сотрудники предприятия. С 2010 года выявлено уже несколько клонов червя Stuxnet. Анализируя качество написания вредоносного кода и объём требуемых для его разработки ресурсов, можно прийти к выводу, что тут дело не обошлось без государственных органов. Конечно, были разработаны соответствующие «заплатки» для ОС, препятствующие распространению Stuxnet, но ведь это лишь первая ласточка!



## Вызов IoT брошен

В одном из интервью Евгений Касперский назвал Интернет вещей Интернетом уязвимостей. И в этом высказывании, как мы уже заметили, заключён большой смысл. Чтобы обеспечить достаточный уровень доверия и исключить риски при подключении IoT-устройств, такие как кража приложений, требуется идентификация, аутентификация, авторизация, обеспечение конфиденциальности и целостности данных. Безопасность IoT – не то же самое, что безопасность Интернет-сетей и примеры новых рисков должны обострить наше отношение к проблеме. Данные должны быть защищены при обработке в системе, при передаче и хранении, а для этого требуется существенный пересмотр принципов идентификации, аутентификации и авторизации, как устройств, так и людей. Именно так считает Робин Дак-Вулли, директор компании Beecham Research. По его словам, мы должны также учитывать, что некоторые полевые устройства могут быть скомпрометированы или выйти из строя, таким образом, нам требуются эффективные процедуры восстановления – это ещё один вызов эры IoT.

Технологический директор Beecham Research профессор Джон Хаус также полагает, что нам требуется высокая степень доверия, и это ещё более критично в условиях экосистемы IoT. Доверие должно начинаться с устройств уровня сенсоров и микроконтроллеров и распространяться по всей инфраструктуре до самого верха. Это огромная головоломка, в которой каждый кусочек должен вносить свою лепту в общий положительный результат.

## Надёжность IoT: кто будет отвечать?

IoT задаёт головоломные вопросы о кибератаках и авариях систем. Кто же будет отвечать за последствия таких событий: производитель и продавец устройства, Интернет-провайдер или, может быть, сам пользователь? Должен ли и производитель ПО быть добавлен в это уравнение? В цепочке IoT весьма много чувствительных звеньев, и в случае ава-

рии удобнее, конечно, указать в качестве виновника на производителя устройства, но в целом это неоднозначный вопрос. Например, в торговле или здравоохранении потеря данных в результате применения технологий IoT может привести к последствиям для частных лиц, за которые должны будут ответить продавцы, банки или медицинские учреждения. Производители датчиков как таковые, безусловно, несут большую ответственность, особенно в случае разработки критически важных устройств типа детекторов дыма, датчиков CO или систем автомобильных подушек безопасности. Но в производстве качественных продуктов крайне важно стратегическое партнёрство производителей «железа» и ПО для устройств IoT. В качестве примера приведём случай, озвученный сенатором США Эдвардом Марки, который показал, что хакеры могут получить доступ к некоторым популярным автомобилям, управляя их внезапным ускорением, поворотами, отключением тормозов, активацией гудка, включением аварийного стоп-сигнала, перенастройкой спидометра, считыванием показаний датчиков. Таким образом, в мире IoT производители ПО также не защищены от исков и должны понимать, что они несут ответственность за продукт, а также за возможные физические повреждения и имущественный ущерб, возникающие в результате его использования. Производители подключаемых устройств финансово ответственны за небрежное проектирование кода ПО и архитектуры.

## Недостатки стандартизации

В традиционном мире IT существует огромное множество стандартов, и сегодня их пытаются адаптировать для мира IoT. Это означает, что пока мы имеем очень уязвимую экосистему, состоящую из устройств и ПО различных производителей, а также разрозненных сетевых сервисов. Чтобы добиться безопасности в этих условиях, мы должны выработать цельное решение для обеспечения идентификации устройств, их аутентификации и защищённых коммуникаций между ними.

Укажем на несколько практик, ведущих к нарушению безопасности в IoT:

- недостаточные возможности защиты, встроенные в базовые системы, такие как система на кристалле (SoC), что даёт хакеру лёгкую возможность получить права доступа администратора;
- передача незашифрованных данных позволяет любому злоумышленнику при помощи сетевого сниффинга перехватывать информацию;
- использование устройств с незакрытыми (без заплаток) уязвимостями в ПО – это приглашение для разного рода вирусов и червей, эксплуатирующих ошибки в системах;
- Web-сервисы и ОС с жёсткой логикой организации доступа позволяют хакерам легче получать доступ к данным;
- неразумная политика в сфере ПО без надлежащего контроля целостности прикладного ПО и ОС в устройствах и шлюзах;
- незашифрованные API-токены и вызовы в текстовом виде также ослабляют защищённость коммуникаций;
- низкая защищённость мобильных устройств в среде IoT усугубляет проблему растущего числа открытых беспроводных точек доступа;
- отсутствие должной аутентификации – путь к потенциально опасному доступу для хакерских атак.

Нарушение безопасности всего лишь на одном устройстве может привести к ситуации, когда множество других устройств, составляющих единую с ним сеть, окажутся под угрозой, поэтому для успешного обеспечения безопасности необходим контроль сверху донизу. Чтобы обеспечить пользователя целостной и надёжной платформой, производители устройств и ПО для них, в свою очередь, должны иметь единую концепцию, базирующуюся на испытанных открытых промышленных стандартах. Хорошая новость состоит в том, что пути реализации такого подхода по примеру мира IT найдены. Но они требуют понимания производителями разницы между классическими IT и IoT. Только тогда они смогут эффективно применить свои лучшие наработки в области IT к миру IoT.

## Основы безопасности IoT и передовая практика

Итак, по сравнению с бурным ростом IoT вопросы безопасности находятся лишь в начале пути. И сейчас самое время поговорить о лучшей практике в этой области. Согласно исследованиям Gartner, для успеха IoT будут иметь первостепенное значение принципы распознавания устройств, а также обеспечение безопасности новых и поддержание безопасности существующих устройств. Требуется целостный подход, когда идентификация, аутентификация и автоматическое распознавание применяются комплексно. Лучшая практика требует принимать во внимание специфику распределённых необслуживаемых мобильных систем и устройств. Необходима защищённая рабочая среда (AEP – Application Enablement Platform), интегрирующая все устройства IoT, а также безопасное обслуживание и распространение ПО.

В первую очередь, присоединённые устройства и платформы IoT должны получить подтверждённые уникальные идентификаторы. Для этого необходимо:

- строить решения на базе открытых промышленных стандартов;
- максимально использовать проверенные технологии защиты и партнёрских связей;
- закладывать потенциал обеспечения безопасности, масштабируемости и сопротивляемости на первых этапах проектирования устройств;
- встраивать в устройства идеологию сквозных комплексных решений безопасности;
- обеспечивать идентификацию каждого узла сети IoT на основе его уникального ID и полномочий;
- взаимно идентифицировать узлы в сети IoT;
- шифровать все коммуникации между узлами;
- обеспечить встраивание механизмов автоматического контроля легитимности сертификатов узлов и разрешения/запрета их работы на этой основе;
- подтверждать цифровой подписью все коммуникации в дополнение к шифрованию трафика;
- контролировать состояние ПО и конфигураций устройств с помощью цифровой подписи;
- внедрить контроль доступа, основанный на роли устройства;
- осуществить инвестиции в инструменты обслуживания и диагностики сетей, позволяющие выявлять опасные отклонения и сертифицировать построенные решения IoT.

## Базовые элементы безопасности IoT

Безопасная платформа IoT должна:

- обеспечивать доверенную среду функционирования;
- быть спроектированной таким образом, чтобы минимизировать возможность атак (минимум открытых портов, надёжные межсетевые экраны, и т.п.);
- использовать лучшее из технических и функциональных наработок, защищающих устройства IoT от угроз извне;
- быть безопасным и естественно интегрированным компонентом IT-инфраструктуры в целом.

Соответствующие изменения должны затронуть все устройства группы потенциального риска. Аутентификация и шифрование данных требуют масштабируемых решений, обеспечивающих взаимную идентификацию с высокой степенью стандартизации, что позволит разнообразным устройствам, включённым в инфраструктуру, беспрепятственно и безопасно обмениваться данными между собой. Для этого разработано немало методов, среди которых идентификация с доверенным ID, API-ключи, самозаверенные сертификаты, биометрия, связки пароль/логин, решения на базе платформ Trusted Platform Module (TPM), динамические пароли, а также решения с многофакторной аутентификацией.

Несмотря на обилие перечисленных методов, нельзя сказать, что все они легко применимы к среде IoT с учётом функциональности, безопасности и масштабируемости и могут использоваться для необслуживаемых устройств. API-ключи, например, обычно слабы в плане криптостойкости, а ненадёжные связки пароль/логин могут быть подобраны.

Однако многие эксперты сходятся во мнении, что один из лучших на сегодняшний день методов аутентификации и защиты данных – интегрированный сертификат x.509 с PKI (Public Key Infrastructure – инфраструктура открытых ключей). Технология PKI даёт уверенность в подлинности идентификации узла на другой стороне обмена данными. Являясь широко распространённой и хорошо отработанной технологией, PKI уже встроена в самые надёжные промышленные стандарты. PKI поддерживает подписание сообщений и документов, вход в систему и аутентификацию, сертификаты и ключи в виде файлов и токенов и является ядром самозаверенных сертификатов.

## Подход к безопасности IoT от начала до конца

В качестве яркого примера системного подхода к решению описанных проблем можно привести концепцию компании Eurotech. Она создаёт технологические блоки, из которых можно строить распределённые системы устройств и сенсоров, интегрированные в IT-инфраструктуру. Для этого компания предоставляет решения, состоящие из аппаратных платформ, ПО низкого и высокого уровня, операционных систем, инструментов программирования, а также обеспечивает профессиональную поддержку разработчиков, резко сокращающую время и стоимость разработок (рис. 2). Итак, предложение Eurotech для IoT состоит из четырёх основных компонентов:

- облачная платформа интеграции IoT Everyware Cloud (EC);
- платформа разработки Everyware Software Framework (ESF), компью-

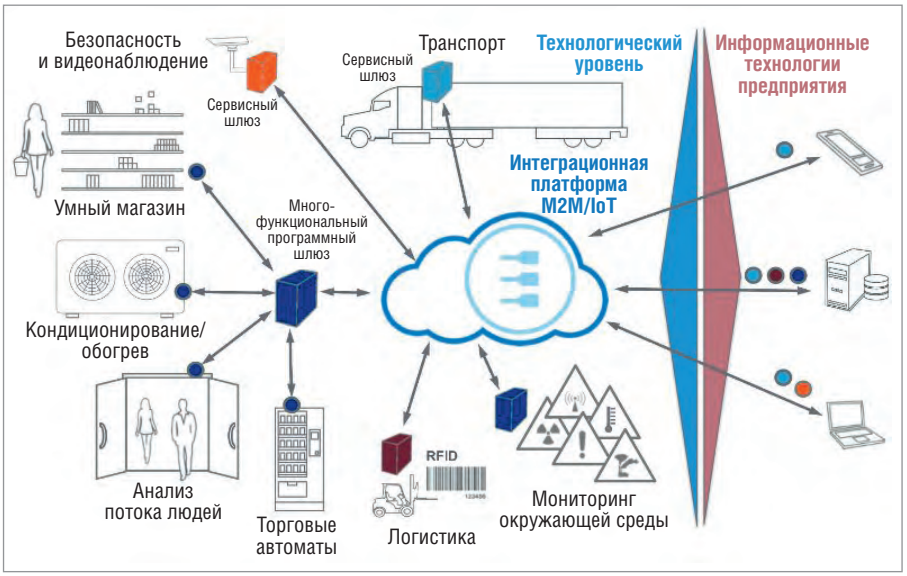



**Рис. 2. Eurotech создаёт безопасную концепцию IoT**

терная платформа и Application Development Framework;

- многофункциональные IoT-шлюзы, спроектированные специально для различных вертикальных рынков;
- профессиональная поддержка разработок IoT.

## Everyware Cloud

Программная платформа Everyware Cloud (EC) разработана специально для поддержки приложений IoT. Она обеспечивает все необходимые сервисы для управления полевыми IoT-устройствами, включая их конфигурацию, сопровождение на всём протяжении жизни и удалённый доступ. Она также даёт возможность сбора данных с полевых устройств и предоставляет эти данные для использования другими приложениями, бизнес-процессами, формирования отчётов и т.п. Согласно концепции Eurotech безопасность заложена в Everyware Cloud с самого начала её разработки и является интегрированной составляющей всех компонентов. В EC использован опыт лучших IT- и Интернет-разработок в области безопасности, изначально заложены механизмы масштабируемости, а также возможности технологий PKI, MQTT on SSL, двухфакторной аутентификации пользователь/администратор.

## Everyware Software Framework

Everyware Software Framework (ESF) обеспечивает высокоэффективную, гибкую и IT-ориентированную компьютерную платформу и среду разработки приложений для построения нового поколения присоединяемых к сети умных устройств и приложений на единой технологической основе с использованием Java и OSGi. ESF позволяет разработчику сконцентрироваться на собственном приложении, избавляя его от рутинной работы благодаря целому ряду функциональных библиотек.

Программируемые многофункциональные шлюзы (Multi-service IoT Gateways) разработаны для применения на устройствах, функционирующих в жёстких условиях высоких температур, повышенной влажности и пыли (рис. 3). Благодаря оптимизированному и сертифицированному IoT-стеку, включающему ОС Linux, Java, OSGi и ESF IoT Edge Framework, обеспечивается максимально безопасное выполнение программ и среды программирования для шлюзов и устройств IoT. В зависимости от требований приложения могут быть задействованы дополнительные возможности для обеспечения безопасности, такие как безопасная загрузка, аппаратное хранение ключей, криптографическая акселерация. Комбинирование продвинутых мер защиты создаёт многоуровневую надёжную систему охраны IoT от угроз.

Сервисы IoT Professional Services гарантируют, что конечный продукт будет соответствовать заданным требованиям системной интеграции и пользовательским спецификациям. Они предлагают ряд программ по сопровождению разработчиков аппаратных и программных средств на всём протяжении проекта.

Для разработчиков доступно также целое семейство тестовых комплектов IoT Development Kit (рис. 4). Они представляют собой полноценные аппаратные платформы с предустановленным программным обеспечением, позволяющие резко сократить трудозатраты по изучению архитектуры системы и адаптации решения к собственным нуждам, а также по прототипированию.

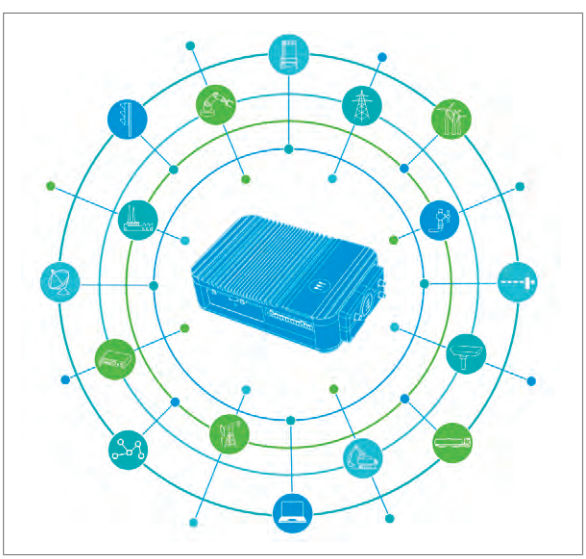


**Рис. 3. Универсальные многофункциональные шлюзы Eurotech**


**Рис. 4. Набор разработчика IoT**

Архитектура Eurotech IoT Security была разработана на базе концепции сквозной безопасности и безопасности каждого элемента системы. Вот некоторые её принципы.

- **Идентификация и контроль доступа.** Конфиденциальность и интегрированность достигаются благодаря модели доступа, основанной на роли узла. Модель контроля доступа и лист контроля доступа следуют принципу наименьшей привилегии и пронизывают все слои архитектуры. Каждый аккаунт управляет списком пользователей и контролирует их полномочия. Everyware Cloud имеет конфигурируемую политику блокировки, привязанную к аккаунту. Она может запретить регистрацию пользователя после заданного числа неудачных попыток входа. Вход в консоль Everyware оснащён защитой в виде двухфакторной аутентификации (2FA). Everyware Cloud поддерживает индивидуальную аутентификацию устройств на базе сертификата x.509 с интегрированным PKI, а также пользовательские приложения с функциональностью PKI.
- **Безопасный обмен данными.** Весь трафик MQTT шифруется посредством SSL-соединения. Доступ к консоли возможен только через HTTPS-соединение. Весь доступ к REST API (Representational State Transfer – передача состояния представления) также происходит только через HTTPS-соединения.
- **Физическое хранение данных.** Облако Eurotech поддерживается дата-центрами, организованными по последнему слову техники, использующими современную архитектуру и инженерные наработки.
- **Логический доступ к данным.** Все базы данных защищены стойкими межсетевыми экранами с жёсткими правилами доступа извне и доступны напрямую только для компьютеров среднего уровня. В базах данных все записи имеют привязку к аккаунту посредством специального идентификатора. В брокере MQTT данные и трафик между разными аккаунтами связываются посредством виртуальной машины.
- **Безопасность устройств и управление встроенными приложениями.** Для оконечных устройств крайне важны безопасность, чёткая аутентификация, отсутствие необоснованно открытых портов, настройка межсетевых экранов, качество встроенного ПО, развитая диагностика и логирование событий, применение стойкой криптографической техники для передачи данных. Безопасность может быть ещё усилена благодаря безопасной загрузке, аппаратно реализованным функциям, а также применению VPN.
- **Управление уязвимостями.** Независимые компании по сертификации безопасности проводят оценку уязвимостей, включая сети, компьютеры и приложения. Eurotech гарантирует, что анализ внутренних и внешних уязвимостей проводится периодически и после всех значимых изменений в оборудовании. Компания исправляет все выявленные критические проблемы с безопасностью в кратчайшие сроки.

Все компоненты Eurotech IoT-архитектуры изначально спроектированы для создания безопасных масштабируемых и надёжных систем и базируются на наиболее успешных и современных стандартах M2M и IoT, поэтому они готовы защитить инвестиции пользователей, как сегодня, так и в отдалённом будущем.

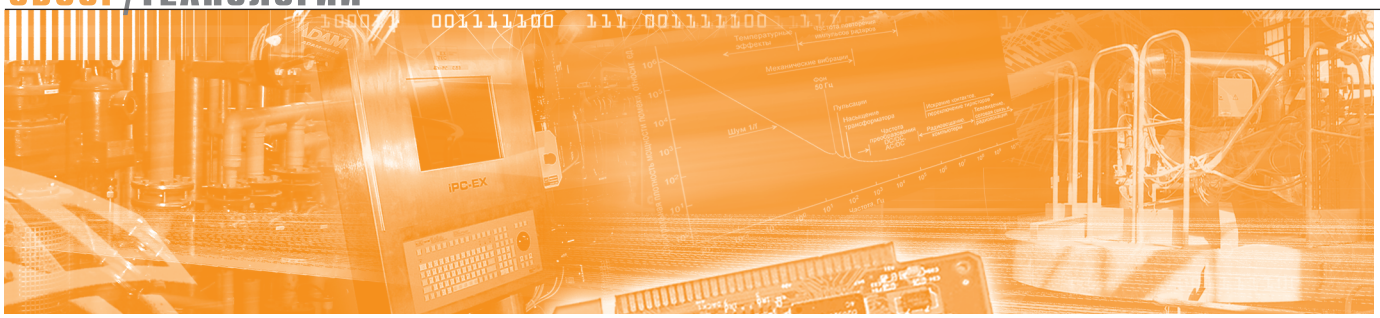
## Заключение

Текущее состояние кибербезопасности и возможность взлома IoT-устройств и инфраструктуры заставляет нас присвоить этой проблеме приоритет номер один.

Безопасность должна стать главным ориентиром для разработчиков устройств IoT, программного обеспечения и инфраструктурного окружения. Если усилия в этой области будут недостаточными, мы рискуем разочароваться в самой концепции IoT. Конфиденциальность, целостность и доступность данных пользователей, а также IoT-инфраструктуры – самые важные задачи для Eurotech, и поэтому безопасность является главной заботой специалистов компании.

Если вы захотели узнать больше о решениях Eurotech для рынка IoT, обратитесь к специалистам компании ПРОСОФТ – официального дилера Eurotech в России.

**Авторизованный перевод**
**Юрия Широкова**
**E-mail: textoed@gmail.com**



Андрей Подлесный, Игорь Афонин

# Программно-технический комплекс на базе серверов AdvantiX и платформы MasterSCADA

**В статье обосновывается необходимость разработки новых программно-технических комплексов для рынка промышленной автоматизации. Описано новое импортозамещающее решение, разработанное компаниями «ИнСАТ» и «Адвантикс».**

## Требования отечественного рынка

Решение задач управления и мониторинга в реалиях современного рынка подразумевает, что проектировщики и разработчики должны учитывать множество дополнительных критериев при оценке и выборе средств автоматизации. Одно из наиболее значимых направлений – импортозамещение, которое предполагает использование только отечественных программно-технических комплексов (далее – ПТК) на объектах критической инфраструктуры Российской Федерации, является не только важным политическим, но и экономическим процессом, влияющим на изменение бизнес-процессов как компаний-разработчиков, так и компаний-потребителей. Это означает, что многие крупные потребители средств автоматизации развернули на своих площадках полигоны для тестирования отечественных решений с целью их последующего внедрения и, как следствие, замещения зарубежных аналогов. Более того, такие комплексы должны предусматривать возможность использования и интеграции средств защиты информации в соответствии с вступившими в силу нормативно-правовыми актами, главным из которых является Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Закон определяет основные принципы госрегулирования в сфере защиты критической информационной инфраструктуры (КИИ) Российской Федерации в целях её устойчивого функционирования при компьютерных атаках. Согласно закону к субъектам КИИ относятся «государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургиче-

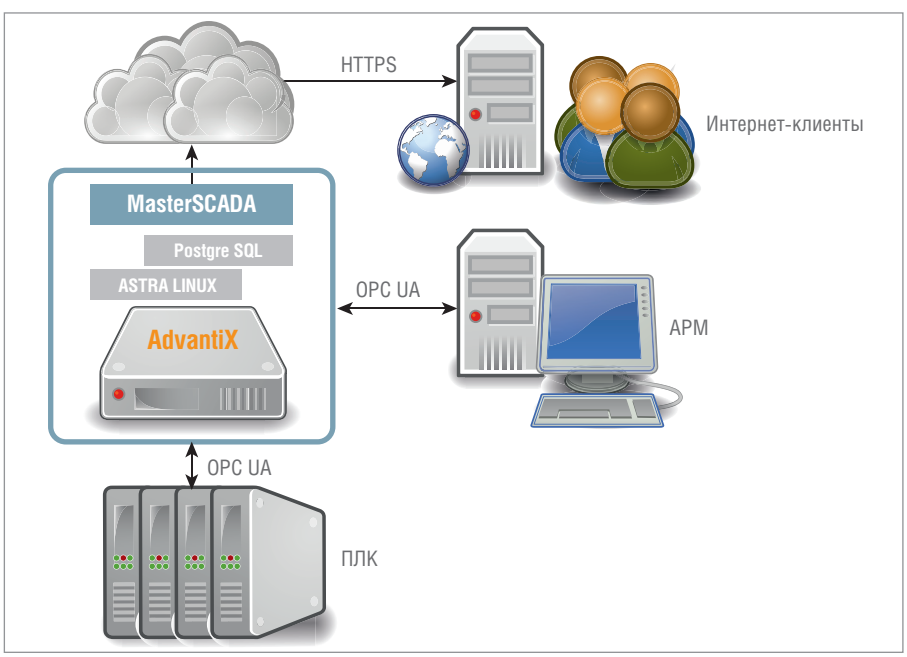



**Рис. 1. Состав программно-технического комплекса**

**Рис. 2. Сервер AdvantiX Intellect IS-MSCADA-C3/AL**

ской и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей» [1], иными словами, практически все крупные системы автоматизации и диспетчеризации РФ. Это означает, что выбор технических средств, в том числе средств защиты информации, невозможен без подробного анализа характеристик конкретного объекта, то есть подготовка к разработке технического задания должна включать дополнительные этапы:

1) систематизация требований информационной безопасности (ИБ) применительно к специфике конкретного объекта и формирование на основе полученных данных об объекте модели угрозы и модели нарушителя;
2) подбор необходимых программно-аппаратных комплексов, решающих задачу создания российской защищённой информационной системы.

Соблюдение указанных этапов – это дополнительное преимущество, которое может помочь компаниям-интеграторам открыть новые направления предоставления услуг, а также поставлять необходимые заказчикам комплексные решения.

Опираясь на требования рынка, компании «ИнСАТ» и «Адвантикс» (торговая марка AdvantiX) разработали российский программно-технический комплекс (ПТК), отвечающий всем современным тенденциям и обладающий уникальными техническими характеристиками (рис. 1).

## Техническая платформа комплекса

Аппаратной платформой ПТК являются серверы AdvantiX Intellect (рис. 2) от передового российского производителя промышленных компьютеров и встраиваемых систем – компании «Адвантикс», которые серийно выпускаются с 2007 года на базе отечественных производственных мощностей. Длительный опыт эксплуатации, а также постоянная работа с проектировщиками и заказчиками систем автоматизации позволяют компании предлагать надёжные и востребованные на рынке решения.

Идеология промышленных компьютеров AdvantiX отвечает требованиям и запросам рынка промышленной автоматизации (рис. 3).


**Рис. 3. Идеология промышленных компьютеров AdvantiX**

Прежде всего, изделия проходят все этапы разработки согласно ГОСТ Р15.201-2000 «Система разработки и постановки продукции на производство» [2], такие как формирование технического задания, опытно-конструкторские работы, выпуск опытных образцов и подготовка производства, что позволяет добиться стабильного качества выпускаемой продукции. Вся конструкторская и технологическая документация хранится в специальном архиве. Ведутся также реестр изменений, возникающих в процессе жизненного цикла изделий, и реестр неучтённых копий документации, которые предоставляются заказчикам по требованию. Изделия поставляются с паспортом, имеющим отметку ОТК.

В серверах используются системные платы, процессоры и контроллеры с уже отработанной архитектурой. Это позволяет значительно повысить надёжность изделий, так как большинство «детских» проблем найдено и устранено как производителями компонентов, так и на этапе ОКР в компании.

Особый акцент при разработке изделий делается на большом сроке доступности – не менее 5 лет, который обеспечивается выбором специальной компонентной базы и постоянным взаимодействием с производителями комплектующих. Это позволяет заказчикам успешно реализовывать новые проекты и поддерживать уже действующие.

Не менее важным моментом для длительной эксплуатации изделий является обеспечение системы установленным согласно эксплуатационной документации комплектом запасных частей, инструментов и принадлежностей (ЗИП) в виде складских запасов либо гарантированных поставок в течение более длительного срока, чем доступность самих изделий.

Необходимым условием для проектирования надёжной системы является расчёт показателей надёжности, поэтому по запросу заказчиков производится расчёт средней наработки на отказ (MTBF) для соответствующей модели эксплуатации изделия (рис. 4).

Для проектных изделий производится также расчёт потребляемой мощности и тепловыделения для заданной конфигурации, поскольку известно, что номинальная мощность блока питания не отражает реальную потребляемую изделием мощность. Значение мощности блока питания определяет максимально возможную мощность, которую с некоторым запасом может дать блок питания

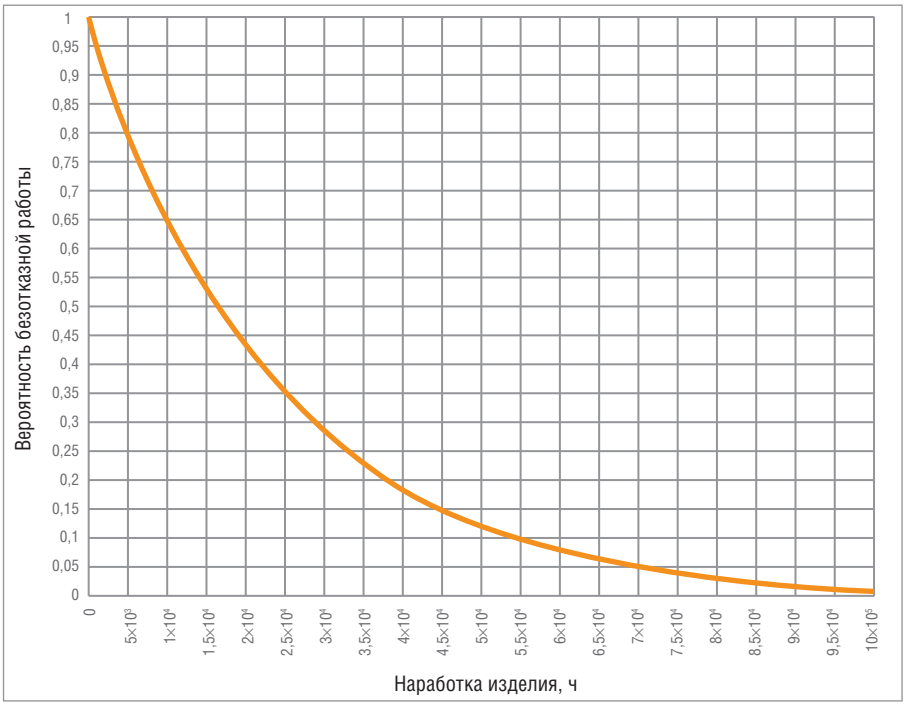



**Рис. 4. Распределение наработки на отказ изделия AdvaniX**

для максимальной комплектации изделия. Это значение используется для расчёта нагрузки на электропроводку, которая должна выдержать максимально возможную нагрузку. С другой стороны, реальная потребляемая мощность зависит от текущей конфигурации изделия. И именно это значение необходимо для расчётов систем кондиционирования и бесперебойного питания.

Ещё одним важным фактором повышения надёжности функционирования системы является мониторинг её состояния и своевременное оповещение. Со стороны аппаратного обеспечения это достигается поддержкой интеллектуального интерфейса управления IPMI (Intelligent Platform Management Interface) с поддержкой функциональности KVM-over-LAN и Media-over-LAN. Это позволяет удалённо производить следующие работы: включение и выключение изделия, мониторинг его состояния, обновление программного обеспечения, в том числе прошивки (Firmware). Это доступно даже в выключенном состоянии без загрузки операционной системы [3].

В соответствии с требованиями безопасности, описанными в начале статьи, была выбрана отечественная операционная система Astra Linux, которая обладает всеми необходимыми сертификатами и разрешительными документами. Кроме того, используется система хранения данных PostgreSQL.

## SCADA-система комплекса

В качестве системы управления для ПТК применяется российская SCADA-система четвёртого поколения MasterSCADA разработки компании «ИнСАТ». Одним из ключевых преимуществ системы является её унифицированная структура, позволяющая использовать любые аппаратные платформы и ОС, например, помимо AstraLinux возможна установка MasterSCADA на ОС «Эльбрус» и QNX. Основным протоколом для взаимодействия элементов платформы является OPC UA (Open Platform Communications Unified Architecture). Для связи с устройствами нижнего уровня используется развитой драйверный интерфейс (OPC DA, HDA, UA, MQTT, Modbus, SNMP, IEC 61850 и прочие). Для мониторинга состояния серверного оборудования AdvantiX по SNMP был разработан специальный функциональный блок, который позволяет контролировать такие параметры, как температура, напряжение питания, скорость вращения вентиляторов, потребляемая мощность и другие. Единая среда разработки позволяет программировать как

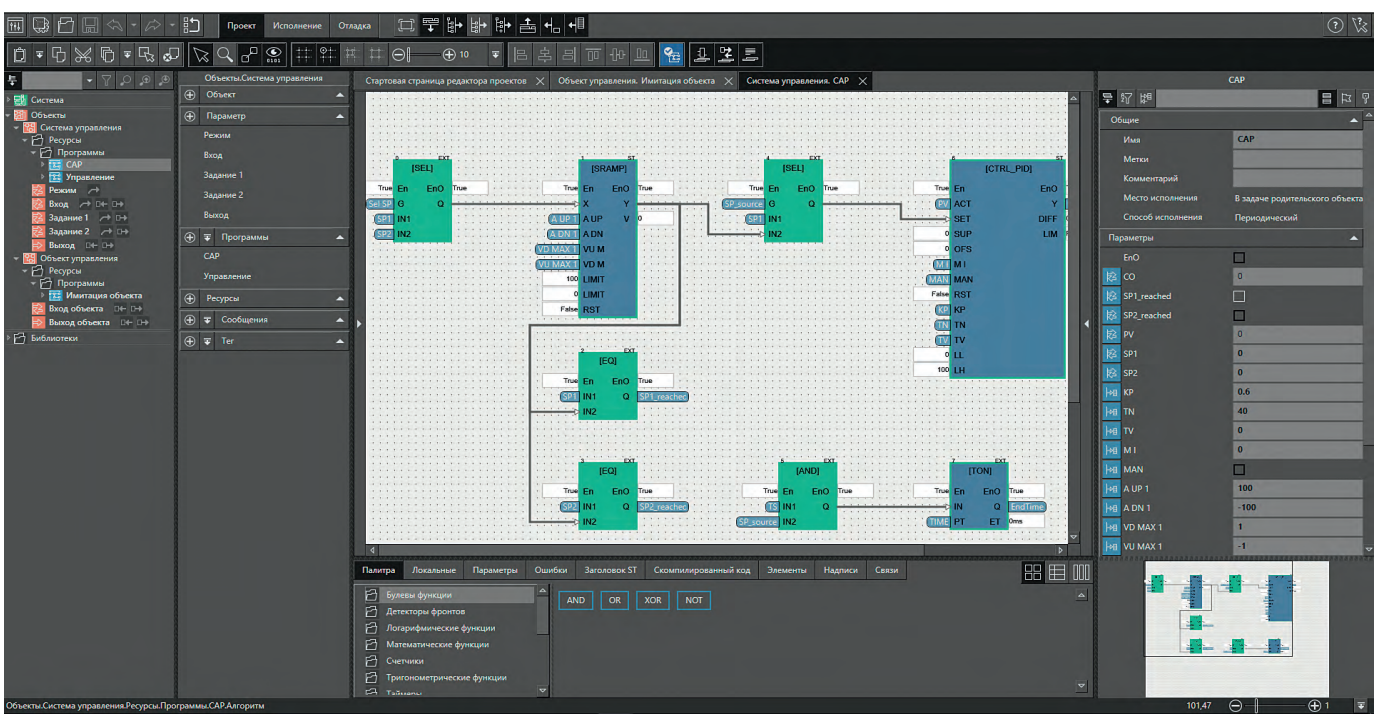


**Рис. 5. Пример окна среды разработки MasterSCADA-4D (язык FBD)**

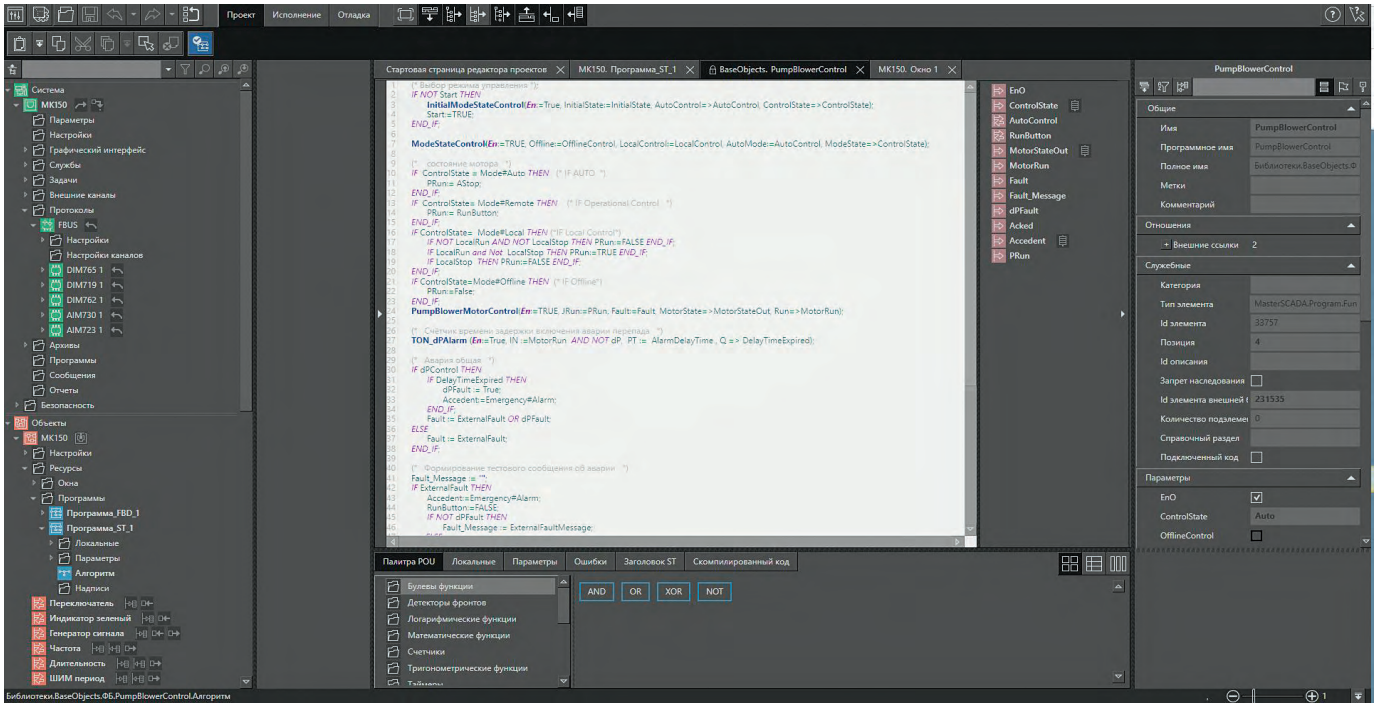


**Рис. 6. Пример окна разработки MasterSCADA 4D (язык ST)**

средний уровень системы – программируемые логические контроллеры (например FASTWEL MK-150), так и верхний уровень в соответствии со стандартом МЭК 61131-3. Благодаря использованию объектно-ориентированных механизмов (инкапсуляция, наследование и тиражирование), а также большой библиотеке готовых математических и логических блоков системные интеграторы получают возможность разработки собственных готовых решений или библиотек, что позволяет им существенно сократить время создания проектов и, как следствие, трудозатраты, уменьшить стоимость и сделать свои предложения ещё более конкурентоспособными на рынке [4] (рис. 5).

MasterSCADA обладает всеми необходимыми функциональными возможностями современной SCADA-системы, в числе которых многофункциональный редактор отчётов, позволяющий создавать отчётные формы любой сложности и вида, в том числе с графическим представлением данных в виде диаграмм, гистограмм и прочих визуальных элементов (рис. 6). Поступающие в модуль отчётов данные могут быть обработаны дополнительными средствами: формульными выражениями, фильтрами и пользовательскими правилами. Обработка этих данных может быть выполнена до, после и в процессе формирования отчёта. Также для предоставления телеметрической информации оператор может использовать тренды, данные для которых структурируются и хранятся в специализированных слоях БД (минутный, часовой, суточный и т.д.), что сокращает время обработки операций и позволяет хранить агрегированные данные для сокращения их объёма. Стоит отдельно отметить, что на базе MasterSCADA может быть развёрнут собственный облачный сервер с отдельными проектами, а не одним общим для разных пользователей, и работать он будет на одной физической машине.

Конечные пользователи смогут подключаться к такому серверу по протоколу HTTPS, используя однофакторную или двухфакторную аутентификацию, с любого устройства: персонального компьютера, планшета или телефона, применяя для отображения встроенный клиент или любой браузер с поддержкой HTML5, что в совокупности с богатыми коммуникационными возможностями делает систему удобным решением для развёртывания проектов в рамках IIoT и Industry 4.0.

Все описанные функции будут входить в программно-технический комплекс, имеющий несколько вариантов поставки, отличающихся производительностью и рекомендованных для различных областей использования. Так, например, для систем до 1000 тегов подходит сборка IS-MSCADA-A5/AL. Она может применяться для объектов малой и средней автоматизации (объекты коммунального хозяйства, небольшие офисные здания, заправочные станции и т.п.). Также имеется модифицированная версия IS-MSCADA-B5/AL, которая обладает дополнительной функциональностью резервирования. Для более крупных объектов применяются сборки IS-MSCADA-C5/AL, которые не имеют ограничений по количеству тегов опроса и могут использоваться в любых распределенных системах управления.

## Планы развития

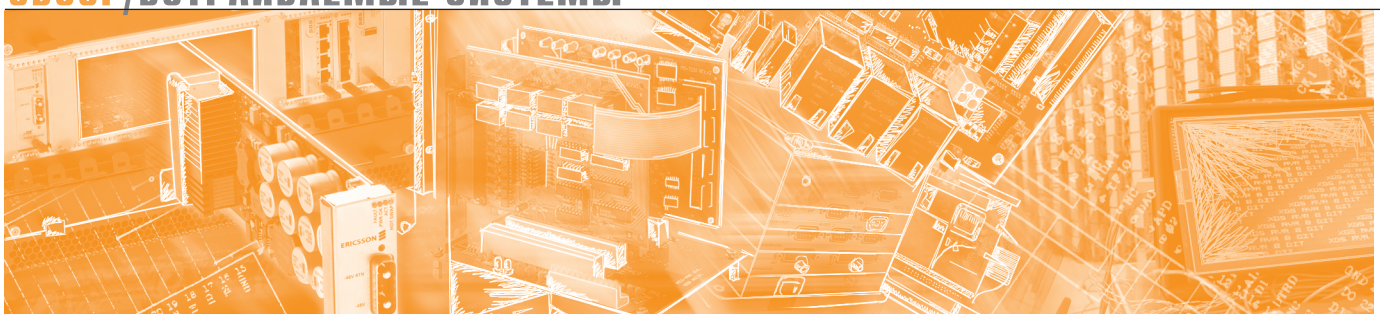
Компании «ИнСАТ» и «Адвантикс» продолжают сотрудничество и в ближайшее время планируют протестировать подобные сборки на базе ОС QNX, а также разработать линейку серверов с новейшими высокопроизводительными процессорами «Эльбрус 8С» производства компании ИНЭУМ. ●

## Литература


1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. ГОСТ Р15.201-2000 «Система разработки и постановки продукции на производство».
3. Intelligent Platform Management Interface [Электронный ресурс] // Режим доступа : https://www.intel.com/content/www/us/en/servers/ipmi/ipmi-home.html.
4. Подлесный А.М. MasterSCADA 4D – отечественная платформа для программирования контроллеров // ИСУП. – 2018. – № 1.



**Авторы – сотрудники компаний «ИнСАТ» и «Адвантикс»**
**Телефон: +7 (495) 232-1693**
**E-mail: info@advantix-pc.ru**



Майкл Хенце

# FPGA – гарантия функциональной безопасности

**В статье рассматривается вопрос обеспечения функциональной безопасности встраиваемых систем для критически важных приложений. Описан подход компании MEN с применением матриц FPGA, имеющий ряд неоспоримых преимуществ перед традиционными решениями.**

Электронные компоненты всегда критически важны для безопасности в тех случаях, когда неисправности или сбои угрожают жизни людей или могут привести к серьёзному экологическому и/или материальному ущербу, поэтому критически важные для безопасности системы всегда должны функционировать надёжно. Необходимой функциональной безопасности можно достичь при помощи логики FPGA (Field Programmable Gate Arrays, или ПЛИС – программируемая логическая интегральная схема).

Зачастую в определённых отраслях промышленности устанавливаются технические требования для критических по безопасности встраиваемых систем, которые соответствуют строгим стандартам. В них нет места ошибкам в аппаратном или программном обеспечении. Типичные применения таких систем – в поездах, автобусах, на кораблях и воздушных судах, они также могут быть составными частями более сложных систем в промышленной автоматизации, медицине, энергетике. В этом контексте фактору функциональной безопасности следует придавать особое значение.

Но возможно ли спроектировать систему таким образом, чтобы она благодаря своей конструкции предусматривала и сводила к нулю все известные риски? Требуется предвидеть также и случайные сбои, вызванные отказами компонентов, влиянием ЭМС или космического излучения, и вероятные ошибки, которых можно избежать при разработке. Можно ли сертифицировать системы в соответствии со стандартами безопасности различных рынков, если на большинство имеющихся стандартных компонентов действие этих стандартов по умолчанию не распространяется?

Самостоятельная проверка обычно занимает очень много времени, особенно если компоненты сложны. Вдобавок иногда она возможна лишь в сотрудничестве с производителем компонентов, что требует погружения в особенности производственных процессов. Но все ли производители компонентов идут навстречу? Зачастую не все, потому что функциональная безопасность является нишевым рынком для большинства поставщиков стандартных компонентов, используемых во встраиваемых компьютерах. Как же разрешить эту дилемму и при этом производить функционально безопасные системы?

## Тестирование стандартных компонентов – это дорого

Очень хорошая альтернатива ретроспективному испытанию стандартных компонентов, предусмотренному процедурой сертификации EASA в меморандуме "EASA CM – SWCEH – 001", – это использование матриц FPGA, в которых функции реализованы по-новому и отвечают нормам безопасности соответствующих стандартов. Это решение подходит для точного выполнения критичных по безопасности требований, имеющихся в соответствующих отраслях промышленности. Кроме того, оно позволяет эффективно реализовать специфические потребности клиентов в малых сериях изделий и предлагать их по привлекательным ценам. Данное решение закладывает основу для обеспечения функциональной безопасности в специфических приложениях. Преимущество FPGA заключается в том, что отпадает необходимость перестраивать всю систему. Пересмотру подвергаются по мере необходимости только библиотечные функциональные блоки для построения логики (блоки IP), что позволяет сэкономить как средства, так и время разработки. Такой подход возможен не только для разработки одной специфической FPGA, но и для конструирования платы или системы с несколькими FPGA.

## Моделирование ошибок и тестирование корректного поведения

Однако прежде чем критически важная для безопасности конструкция будет подготовлена и сертифицирована, необходимо проанализировать её поведение в критических ситуациях. С инструментами разработки FPGA это сделать сравнительно легко, поскольку для проверки поведения системы в виртуальной

среде разработки FPGA можно моделировать даже серьёзные или сложные ошибки. Такая форма эмуляции является частью процесса разработки FPGA даже в случае, если соответствие требованиям функциональной безопасности не нужно. В этом смысле для FPGA не требуются какие-либо дополнительные усилия. Моделирование также может быть использовано не только для доказательства «правильного» поведения в ошибочных ситуациях, но и для подтверждения корректной реализации требуемой функциональности. Таким образом, на базе эмуляции можно создавать полные отчёты моделирования, которые затем могут быть представлены TÜV или другим сертифицирующим органам.

## Расширенные функции мониторинга

Мониторинг надлежащих условий функционирования также играет существенную роль в критически важных для безопасности областях, поскольку это единственный способ обнаружения сбоев и инициирования соответствующих действий. Например, температура и функционирование компонентов или обмен данными должны контролироваться и анализироваться на предмет отклонений от заданных значений, а в аварийной ситуации требуется обеспечить остановку машины или поезда контролируемым образом. Однако готовые компоненты для подключения входных и выходных блоков, такие как последовательные интерфейсы или GPIO (контакты ввода-вывода общего назначения), редко содержат функции мониторинга, необходимые для обеспечения функциональной безопасности, например, в соответствии с EN 50129 для железных дорог или с IEC 61508 для электронных систем с функцией безопасности. Но если нет подходящих микроконтроллеров, такие функции можно очень эффективно реализовать в FPGA. Внедрение функций контроля при помощи FPGA также имеет преимущества перед микроконтроллерами, которые обусловлены свободным конфигурированием и хорошей адаптацией к требованиям конкретного применения.

## Долгосрочная доступность и снижение риска морального износа

Высказывание «никогда не изменяйте работающую систему» применимо и к функционально безопасным системам. С одной стороны, расходы на проверку функциональной безопасности в соответствии со стандартами очень большие, и такие проверки должны проводиться повторно каждый раз, когда вносятся изменения, что означает их чрезвычайно высокую стоимость. С другой стороны, при внесении изменений всегда существует риск появления новой ошибки. По этой причине, особенно на железнодорожном транспорте и в авиации, системы используются десятилетиями без изменений. Но это требует наличия стратегии реагирования на старение компонентов, поскольку стандартные компоненты для промышленности редко доступны более 5–10 лет. FPGA и здесь предлагают решающие преимущества. Дело в том, что реализация каждой функции осуществляется не определённым компонентом, а программно. В результате замены компонентов сравнительно безболезненны, ввиду того что программный код можно перенести в новые FPGA, обеспечив идентичную функциональность. Таким образом, продолжительность проекта более чем 30 лет – не проблема, даже если придётся поменять производителя FPGA. Данный подход к тому же обеспечивает независимость от определённого поставщика.

Используя FPGA, всегда можно интегрировать дополнительную функциональность на самой современной платформе, модернизировав систему. Эта гибкость, естественно, имеет значение и в начале жизненного цикла продукта: если некоторые из функций оборудования реализованы в FPGA, то эту часть можно в дальнейшем развивать и модернизировать. Такая стратегия позволяет сэкономить время при последующих пусконаладочных работах и испытаниях всей системы.

## Замена компонентов при работе в расширенном температурном диапазоне

Одно из самых общих требований, особенно в критических областях, – поддержка расширенного диапазона рабочих температур, обычно –40...+85°C. Здесь часто возникают проблемы с подбором подходящих стандартных компонентов. Однако в последнее время стало значительно труднее или вообще невозможно найти компоненты для выполнения различных аппаратных функций при работе в сверхширокоом диапазоне –55...+125°C. Надо сказать, что FPGA обеспечивают достаточно широкий диапазон, позволяющий работать и при этих экстремальных температурах.

## Лёгкое конструирование систем, невосприимчивых к сбоям

Наиболее важной стратегией снижения риска для системы является избыточность критически важных компонентов, то есть их функционально идентичное умножение. Компонент, отказ которого парализует всю систему, называется единой точкой отказа (SPOF – Single Point of Failure). Любой важный строительный блок системы может превратиться в SPOF. В аэрокосмических приложениях, например, серьёзной проблемой являются ошибки памяти, вызванные космическим излучением. Это приводит к однобитным (SEU – Single Event Upsets) или многобитным (MBU – Multi-Bit Upsets) ошибкам, когда один или несколько битов в элементах памяти меняют состояние от 0 к 1 или наоборот. Если критические компоненты, такие как ЦП, дублированы, это увеличивает функциональную безопасность системы и готовность к работе. Такая избыточность может быть создана с помощью FPGA, преимущество которых в том, что эта логика может быть легко дублирована в каждом экземпляре путём копирования и вставки логических блоков IP. В FPGA это резервирование повторяется и позволяет завершить вычисление, если логика IP FPGA отказывает. В результате на основе флэш-FPGA можно реализовать устойчивую к SEU-ошибкам логику.

## Возможности реального времени и гарантированный отклик

В критически важной для безопасности среде в дополнение к надёжности часто требуется предсказуемое время выполнения. Система должна реагировать на внешнее событие за определённое время даже в наихудшем случае. Однако типичные компьютерные архитектуры используют прерывания и топологии DMA (Direct Memory Access), которые могут отрицательно влиять на время исполнения отдельных задач, когда другая задача запрашивает те же ресурсы. Необходимое детерминированное поведение, то есть точно предсказуемое по времени, в этом случае становится труднодостижимым. По этой причине такие решения не используются там, где предъявляются жёсткие требования реального времени. Однако FPGA поддерживают возможности реального времени, поскольку они построены на основе параллельной логики. Это означает, что разные процессы не конкурируют друг

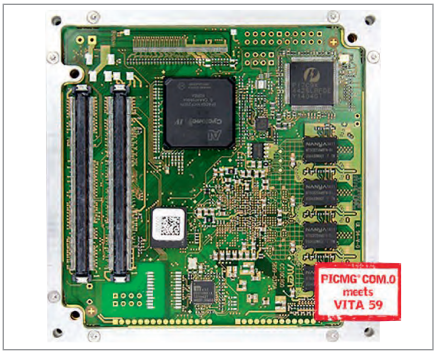



**Рис. 1. Матрица FPGA на модуле Rugged COM Express CC10C с процессором ARM i.MX6**

с другом, но идут своим собственным предопределённым путём, который не нарушается другими событиями. Это значительно облегчает обеспечение детерминированных возможностей в режиме реального времени с чётко определённым поведением во времени.

## Интеграция приложений безопасности

В контексте функциональной безопасности во времена Интернета вещей, Industry 4.0 и Mobility 4.0 рано или поздно возникает проблема безопасности в аспекте защиты от манипуляций. FPGA предлагают множество возможностей для защиты приложения от манипуляций, несанкционированного доступа или дублирования данных. Например, в FPGA может быть запрограммирован уникальный ключ. Там он хранится в зашифрованном виде в энергонезависимой памяти. Этот ключ гарантирует, что доступ к данным смогут получить только приложения и люди, которые его знают. Ключ также может использоваться для идентификации при связи устройства с другими устройствами. Поскольку он прописан аппаратно, им нельзя манипулировать со стороны программного обеспечения, которое всегда однозначно идентифицирует устройство. Код, который реализован в аппаратном обеспечении, не может быть скопирован так же легко, как программное обеспечение. Таким образом, FPGA может добавлять ценные функции безопасности, которые идут намного дальше, чем, например, доверенный платформенный модуль. Мало того, они даже имеют преимущество перед стандартными решениями, потому что, если они запрограммированы индивидуально, они гораздо менее подвержены взлому.

## Ограничения FPGA

Несмотря на все перечисленные преимущества, FPGA имеют и ограничения в использовании. С одной стороны, это затраты. FPGA, конечно, дороже, чем стандартные компоненты, производимые крупными партиями. FPGA можно использовать только в ограниченной степени для реализации сложных решений, поскольку, начиная с определённого уровня функциональности, лучше переключиться на комбинацию программного и аппаратного обеспечения: ведь микроконтроллеры и прикладные процессоры уже имеют фундаментальную логику, включая различную функциональность ввода-вывода и интерфейсы, которые для FPGA должны быть разработаны вновь. Тем не менее, конечно, можно сделать многое и с FPGA. Например, в FPGA уже реализована логика x86. Но мы всё ещё далеки от воспроизведения в FPGA всей логики программного обеспечения, которая существует для x86, поэтому преимущества и недостатки должны быть взвешены в зависимости от характера применения и существующих альтернативных стандартных компонентов. В принципе, FPGA пред-

лагают гибкие и безопасные альтернативы практически для всех задач, где на стороне оборудования или программного обеспечения вы давно бы столкнулись с ограничениями развития. Сегодня без логики FPGA не могут обойтись многие приложения, ориентированные на функциональную безопасность (рис. 1).

## Разработка функционально безопасных систем

Такие компании, как MEN Mikro Elektronik, специализируются на платформах на базе FPGA для критически важных встраиваемых систем и хорошо знакомы с требованиями конкретных отраслей промышленности. На рис. 2 в качестве примера показана высокопроизводительная плата A25 SBC 6U с 16-ядерным процессором и интерфейсом VME-bus на основе FPGA. Плата используется в большом адронном коллайдере ЦЕРН и считается эталоном безопасности среди разработчиков. В некоторых отраслях промышленности распространена практика, согласно которой разработка FPGA не закреплена в стандартах, но поставщики решений полагаются на результаты моделирования, выполненного с помощью средств разработки FPGA, и документируют их для сертификации. Несмотря на большие усилия, связанные с разработкой, FPGA могут сэкономить значительное время в процессе сертификации, которая иногда более затратна, чем сама разработка. Приносят пользу и уже имеющиеся наработки. Например, у компании MEN есть много функциональных блоков, используемых в сертифицированных приложениях. С одной стороны, они выполняют базовые функции плат, с другой стороны, они реализуют специфические функции ввода-вывода.

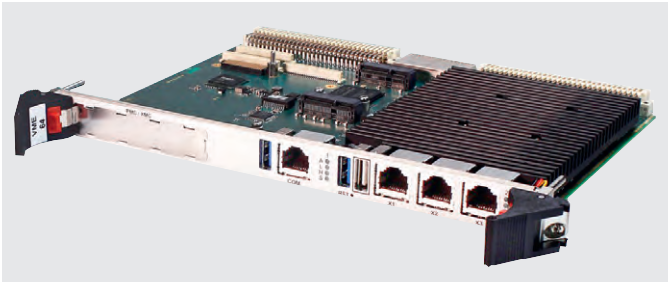


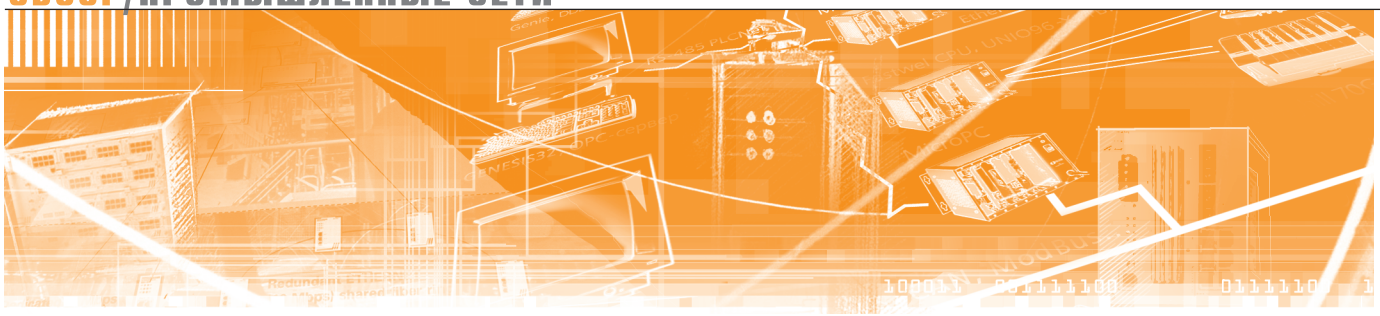
Рис. 2. Высокопроизводительная плата MEN A25 SBC 6U

Строительные блоки IP MEN для FPGA включают:

- графические и сенсорные дисплеи;
- интерфейсы Fieldbus, такие как CAN и MVB;
- различные интерфейсы UART, такие как RS-232 или RS-485;
- интерфейсы Ethernet и HDLC;
- контроллеры SRAM и флэш-памяти;
- GPIO, цифровой ввод-вывод, счётчики, квадратурные декодеры и функции ШИМ.

Все эти IP-блоки могут быть объединены с ядрами, предоставляемыми Altera (Avalon Bus) или сообществом Open Cores Community (Wishbone Bus). Мосты, разработанные MEN, – Wishbone-to-Avalon и Avalon-to-Wishbone – завершают постоянно развивающийся спектр готовых приложений с логикой FPGA, который, конечно же, может быть адаптирован и расширен в соответствии с требованиями заказчика.

**Перевод Юрия Широкова**
**E-mail: textoed@gmail.com**



Сергей Воробьёв

# “Defense in Depth” в действии. Уровень 4: защита промышленных протоколов

## Часть 1

**Данный материал служит продолжением цикла статей, посвящённых многоуровневой защите промышленных Ethernet-сетей на базе принципа “Defense in Depth”. В статье рассмотрен ряд базовых уязвимостей промышленных протоколов Modbus TCP и OPC Classic, а также методы защиты, основанные на глубокой инспекции трафика.**

### Введение

Тщательная и глубокая проверка данных, передаваемых по промышленной Ethernet-сети, является следующим уровнем защиты согласно принципу “Defense in Depth” [1]. Фактически это узконаправленный механизм защиты, который позволяет нейтрализовать угрозы, направленные на оконечные устройства.

Известно, что датчики, ПЛК, HMI – это устройства, которые функционируют на базе хорошо известных промышленных протоколов Modbus TCP, Ethernet/IP, DNP3 и других. И если анализировать IP-пакет данных, например, протокола Modbus TCP, с которым работает датчик или ПЛК, то можно констатировать, что вся необходимая служебная информация находится внутри пакета. Если злоумышленник или вредоносное ПО использует узкоспециализированные шаблоны атак, которые направлены на изменение передаваемых данных внутри промышленных протоколов, то это может привести не только к полной потере контроля над оконечными устройствами, но и к компрометации передаваемых данных. Практических примеров подобных инцидентов достаточно много, начиная от воровства топлива на АЗС путём передачи ложных данных о температуре окружающей среды, заканчивая выходом из строя критически важных узлов и агрегатов промышленного предприятия. Наглядной демонстрацией последнего может служить широко известный промышленный вирус Stuxnet, а также авария на сталелитейном заводе в Германии. В первом случае это привело к выходу из строя центрифуг для обогащения урана, во втором к застыванию доменной печи.

Методики защиты, описанные в предыдущих статьях цикла, позволяют обеспечить защиту от самых многочисленных и разнообразных угроз, но если атака направлена на протокол передачи данных, на изменение служебной информации, содержащейся в передаваемых пакетах, и атакующий уже получил доступ к сети, то нужен иной инструмент анализа и защиты. Средства, основанные на использовании классического L3- или L2-брандмауэра, не позволяют это реализовать, так как принцип их работы основан на проверке заголовка в начале пакета либо фрейма. Брандмауэр, функционирующий на уровне L3, согласно модели OSI позволит внести ограничение на уровне порта, например, полностью закрыть протокол Modbus TCP путём ввода ограничений на передачу по порту 502. Это даст возможность отключить множество ненужных клиентов от оконечных устройств, но не предотвратит передачу ложных данных. Необходим иной подход, который позволит «залезть» внутрь пакета и проанализировать передаваемые данные на уровне регистров протокола. Решение, которое поможет преодолеть данную проблему и защитить оконечное устройство, – это проверка пакетов данных (packet inspection). Осуществлять её необходимо непосредственно на верхних уровнях модели OSI при помощи специализированных брандмауэров. При работе подобного устройства каждый пакет передаваемых данных полностью распаковывается и проверяется на уровне протоколов и полезной нагрузки. А задержки, которые очень критичны в промышленной сети, должны быть сведены к минимуму.

Далее в качестве примера подобного брандмауэра рассмотрим функциональность программно-аппаратного комплекса Tofino Xenon от компании Hirschmann (рис. 1), который позволяет защитить не только промышленные, но и проприетарные протоколы различных устройств, работающих по Ethernet-сети.

### SPI и DPI: в чём различие?

Начнём с того, что сейчас встречаются два достаточно близких термина, относящихся к проверке данных, которые содержатся в IP-пакетах, это SPI – Stateful Packet Inspection и DPI – Deep Packet


**Рис. 1. Внешний вид брандмауэра Tofino Xenon**

Inspection. SPI можно дословно перевести как инспекция пакетов с хранением состояния. Брандмауэр, в котором заявлена поддержка SPI, является пакетным фильтром, анализирующим данные на транспортном уровне модели OSI.

Изначально технология SPI создавалась, исходя из необходимости защитить сессию протокола TCP/IP. Когда протокол TCP создаёт сессию с другим сетевым устройством, используется определённый порт на устройстве с противоположной стороны, также открывается порт на исходном устройстве-отправителе. В соответствии со спецификацией TCP-порт отправителя будет некоторым числом, большим чем 1023 и меньшим чем 16384. Порт назначения на удалённом устройстве имеет фиксированный номер. Например, для SMTP это будет 25, для Modbus TCP – 502. Смысл SPI – это реализация пакетного фильтра, который должен разрешать либо запрещать трафик по определённым портам. Один из примеров настройки правила для пакетного фильтра (не SPI и DPI) – это разрешение на пропуск всего входящего трафика для портов с большими номерами, так как это будут возвращаемые пакеты от системы назначения. Но подобное открытие портов создаёт риск несанкционированного проникновения в локальную сеть [2].

Брандмауэры с поддержкой SPI решают эту проблему путём создания списка для исходящих TCP-соединений, соответствующих каждой сессии. Данный список затем используется для проверки допустимости любого входящего трафика. В сущности, если у брандмауэра заявлена функциональность SPI, это добавляет анализ транспортного уровня в архитектуру пакетного фильтра. Пример подобного брандмауэра был описан в статье [3]. Как правило, подобная функциональность необходима на границе сети.

Немного иной принцип работы у брандмауэров с поддержкой Deep Packet Inspection. DPI – это глубокая проверка данных не только на сетевом и транспортном уровне, как в случае с SPI, но и проверка на всех вышестоящих уровнях модели OSI, включая прикладной (рис. 2). Это очень ресурсозатратный про-цесс, который, как правило, требует существенных вычислительных мощностей. При этом зачастую возникает вопрос относительно того, откуда брать данные и что анализировать? Сейчас существует ряд подходов, которые используют разработчики DPI-систем, один из самых распространённых – это получение данных из SPAN-порта коммутатора (Switch Port Analyzer). Подключив к нему мощную платформу для проверки и анализа трафика, можно выявить многие процессы, происходящие в сети. Но это решение не всегда является хорошим, так как при анализе данных необходимо чётко понимать структуру сети, какие именно данные проходят в данном сегменте сети, что является входящим и исходящим потоком данных, а также откуда их нужно брать. При этом знание протокола передачи должно быть достаточно глубоким и применимым в реальной системе. Если рассмотреть популярный промышленный протокол Ethernet/IP (EIP – Ethernet Industrial Protocol), который используется в сетях ControlNet и DeviceNet, то можно констатировать, что для анализа данных, помимо стандартного ряда параметров, присущих любой Ethernet-сети, необходимо учитывать достаточно большое количество служебной информации, передающейся в пакете (Class ID, Member ID, Service ID, Connection Point, Port Seg Number, Data Seg Number, CIP service, Instance ID и т.д.) Подобный перечень индикаторов потенциально вредоносных действий можно обозначить практически для любого промышленного протокола. Помимо Ethernet/IP сюда можно отнести Modbus TCP, OPC Classic, DNP3, IEC104, GOOSE и т.д., и достаточно большое количество проприетарных протоколов, данные которых могут быть скомпрометированы, например, WAGO CODESYS, S7-COMM, Emerson DeltaV и т.д.

В итоге можно констатировать, что DPI – это комплексная и сложная проверка на уровне данных, которые несут полезную нагрузку в промышленных протоколах. Для её реализации необходимо чётко понимать структуру передаваемой информации, как на уровне стандартов, так и на уровне возможных отклонений от них, а также присутствие их в том или ином сегменте сети. При этом помимо проверки данных необходимо анализировать полученную информацию о нетипичном поведении протоколов, вовремя сигнализировать об этом поведении и предотвращать подобные ситуации.

## Tofino Xenon – невидимый защитник промышленных протоколов

Одним из примеров устройства, в котором реализована технология DPI, является программно-аппаратный комплекс **Tofino Xenon**. Комплекс состоит из аппаратной платформы и программного обеспечения. Аппаратная платформа реализована в промышленном исполнении, при этом является конфигурируемой и позволяет подстроиться под существующую сетевую инфраструктуру. Комплекс устанавливается в разрыв сети и может быть оснащён как оптическими, так и медными портами типа RJ-45 со скоростью до 100 Мбит/с. Из важных особенностей аппаратной части можно отметить пропускную способность, которая составляет 2000 пакетов в секунду, а также то, что комплекс является полностью прозрачным на сетевом уровне,

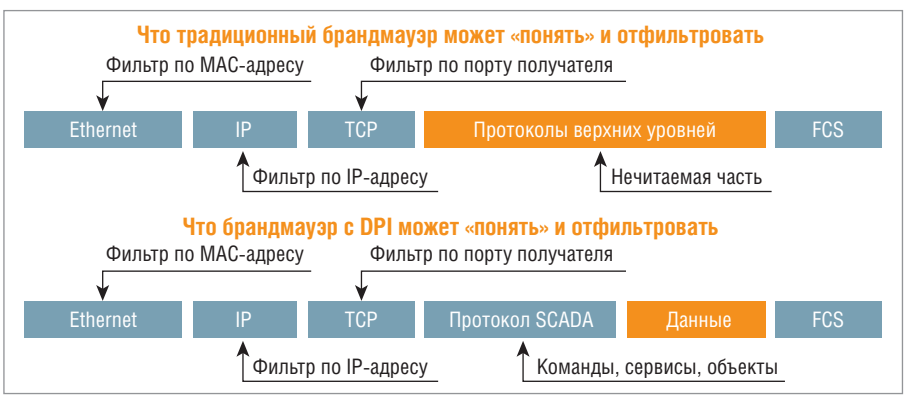



**Рис. 2. Отличия принципа работы DPI-брандмауэра от традиционного**

*Таблица 1*

**Краткий список протоколов, поддерживаемых Tofino Xenon**

| Производитель | Серия | Серверы и приложения | Протоколы |
|---|---|---|---|
| 1 | 2 | 3 | 4 |
| **ABB** | AC400 | Engineering Workstation | ABB Time |
| | AC800M | Operator Workspace | MI |
| | | Controller Network Interface | RNRP |
| | | Server Network Interface | RemSys |
| | | Aspect Server | |
| | | Domain Controller | |
| | | Multisystem Integration Server | |
| **Allen-Bradley** | CompactLogix | | Ethernet/IP (CIP) |
| | ControlLogix | | Rockwell CSP (TCP and UDP) |
| | PLC-5 | | |
| | SLC-5 | | |
| **Cisco** | 1600, 1800, 2600, 2800, 3800 routers | | |
| | ASA&PIX firewalls | | |
| **Emerson** | DeltaV | | DeltaV |
| | Provox | | |
| **GE** | 90-30 | | GE QuickPanel Configuration Protocol |
| | 90-70 | | GE SRTP |
| | VersaMAX | | MOST/PAC8000API |
| | VersaMAX Micro | | |
| | PAC8000 SafetyNet | | |
| **Промышленные IT-протоколы** | | Wonderware HMI | DNP3 |
| | | | FF Fieldbus Message Specification |
| | | | FF system management |
| | | | GOOSE-IEC61850 |
| | | | IEC MMS |
| | | | IEC 60870-5-104 |
| | | | IEEE 1588 PTP |
| | | | ISO networklayer protocol; |
| | | | MRP (Media Redundancy Protocol) |
| | | | OPC Classic TCP |
| **IT-протоколы** | | | DHCP (клиент и сервер) |
| | | | DNS |
| | | | FTP |
| | | | HTTP (web) |
| | | | HTTPS |
| | | | ICMP (ping) |
| | | | IGMP |
| | | | Intel NIC Teaming Protocol |
| | | | IPv6 |
| | | | Kerberos Authentication |
| | | | LDAP |
| | | | LLDP |
| | | | LLMNR |
| | | | NETBIOS Datagram |
| | | | NETBIOS Name Resolution |
| | | | NETBIOS Session Service |
| | | | Network Time Protocol (NTP) |
| | | | Novell Netware Protocol |
| | | | Remote Replication Agent |
| | | | Reverse ARP |
| | | | SMB |
| | | | SNMP |
| | | | SNMP Trap |
| | | | Spanning Tree Protocol (STP) |
| | | | SSH Secure Shell Protocol |
| | | | Symantech AV |
| | | | Telnet |
| | | | TFTP |
| | | | UPnP (TCP and UDP) |
| | | | VRRP |
| | | | WS-Discovery |
| | | | WSUS |

*Окончание таблицы 1*

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| **Hirschmann** | OpenRail | | Hiper Ring Protocol |
| | RSR | | Hirschmann redundant Ring Coupling |
| | MICE | | |
| | BAT Wireless | | |
| | Octopus | | |
| | RS40 | | |
| | MACH 100 | | |
| | MACH 1000 | | |
| | MACH 3000 | | |
| | MACH 4000 | | |
| | LION | | |
| | RAIL Video | | |
| **Honeywell** | C200 | | Honeywell CDA |
| | C300 | | Honeywell FTE |
| | | | Honeywell Safety Manager |
| | | | PLANTSCAPE |
| **Mitsubishi** | | | Mitsubishi MELSCQNA |
| **Omron** | | | FINS (UDP) |
| **OSISoft** | | PI Data Historian | PI Data Historian |
| **Schneider Electric** | Momentum | | Modbus TCP |
| | Premium | | Modbus UDP |
| | Quantum | | |
| | Twido Nano | | |
| **Siemens** | SIMATIC S7/200/1200/ | | |
| | 300/400(FH)/C | | |
| **WAGO** | 750-842 PLC | | WAGO CODESYS |
| **Yokogawa** | Cendum | | Yokogawa Stardom |
| | Stardom | | Vnet/IP |

*Таблица 2*

**Модули Tofino Xenon**

| Наименование | Краткое описание программного модуля |
|---|---|
| **Tofino Firewall LSM** | Базовый модуль, включающий возможность анализа промышленных, IT и проприетарных протоколов |
| **NetConnect** | Модуль для возможности удалённого конфигурирования |
| **Tofino Modbus TCP Enforcer LSM** | Модуль для глубокого анализа протокола Modbus TCP |
| **Tofino OPC Classic Enforcer LSM** | Модуль для глубокого анализа протокола OPC Classic |
| **Tofino Xenon IEC 104 Enforcer LSM** | Модуль для глубокого анализа протокола IEC104 |
| **Tofino Xenon DNP3 Enforcer LSM** | Модуль для глубокого анализа протокола DNP3 |
| **Tofino EtherNet/IP Enforcer LSM** | Модуль для глубокого анализа протокола Ethernet/IP |
| **Tofino Xenon GOOSE Enforcer Loadable Security Module (LSM)** | Модуль для глубокого анализа протокола GOOSE |

у него нет IP-адреса и определить его наличие в сети практически невозможно. При этом у устройства присутствует режим тестирования, который помогает проверять правила трафика без какого-либо риска случайного блокирования сообщений, имеющих решающее значение для работы оконечных устройств.

Конфигурирование Tofino Xenon можно осуществить как удалённо, так и записав конфигурацию на специализированный USB-носитель. Программная часть состоит из ПО для конфигурирования – Tofino Configurator, которое предназначено для комплексной настройки параметров безопасности сети и программных модулей. Программные модули определяют функциональность межсетевого экрана Tofino Xenon. При этом для каждого устройства возможно сформировать индивидуальный набор модулей, в зависимости от требований, предъявляемых к конкретному сегменту сети. Программных модулей несколько, и они предназначены для различных промышленных протоколов, рассмотрим более подробно каждый из них.

## Tofino Firewall LSM

Данный модуль является базовым для всех устройств Tofino и фактически позволяет управлять трафиком, пропускать либо блокировать его. В процессе работы происходит проверка всех коммуникаций в сети по контрольному списку данных, куда входит IP- и MAC-адрес, а также, что немаловажно, тип сетевого протокола, в том числе промышленного. Любое сообщение, которое не входит в список разрешённых, будет заблокировано, а информация о нём отправлена в виде log-файла.

Данный модуль содержит предварительно определённые шаблоны для более чем 25 популярных промышленных ПЛК, включая правила для защиты устройств с известными уязвимостями (табл. 1).

Регистратор событий (Event Logger) также по умолчанию включён в данный модуль. Регистратор событий контролирует события, которые происходят в промышленной сети, а также отправляет сигналы тревоги. Система регистрации событий может как отправлять сообщения об угрозах на удалённый сервер syslog, так и хранить список в энергонезависимой памяти Tofino. Также в составе комплекса Tofino Xenon могут быть установлены модули группы Enforcer, которые позволяют проводить анализ и тонкую настройку фильтров для промышленных протоков (табл. 2).

## Tofino Modbus TCP Enforcer LSM

Модуль Modbus TCP Enforcer позволяет осуществить анализ трафика Modbus TCP на достаточно глубоком уровне – уровне регистров передаваемых данных. Необходимость подобной проверки связана с тем, что Modbus, наверно, самый «хороший» пример по уязвимости именно промышленных протоколов. Это связано с тем, что протокол Modbus, который применяется на огромном количестве предприятий, известен ещё с 70-х годов прошлого века. Впервые спецификация была опубликована компанией Modicon в 1979 году, сейчас эта компания называется Schneider Electric. И начиная с момента публикации спецификации, этот протокол набирал популярность и проник практически во все сферы промышленности. Можно сказать, что сейчас Modbus – это стандарт де-факто среди промышленных протоколов. При этом протокол достаточно простой и лёгкий в реализации. Огромное количество производителей ПЛК и оконечных устройств используют его (Schneider Elecric, Advantech, ABB, FASTWEL, Emerson, WAGO и т.д.). При этом Modbus настолько популярен, что многие noname-производители имеют поддержку именно Modbus. И было бы всё хорошо, но в те далёкие годы, когда спецификация протокола была разработана, никто в принципе не думал о безопасности. В качестве линии для передачи данных использовались RS-232/485, всё было изолировано внутри промышленного объекта либо цеха.

В результате увеличения скоростей передачи данных и доли интеллектуальных устройств Modbus решили перевести на стек TCP, и в результате этого в XXI веке Modbus представлен в виде протокола Modbus TCP. Но что изменилось? Да в принципе изменений совсем немного. Modbus TCP – это по-прежнему протокол типа «запрос-ответ», на установку соединения в нём ничего не завязано. В спецификации, конечно, есть пункт про установку соединения и дальнейшую его поддержку, где указано, что не следует разрывать его после каждого ответа, но это рекомендуется делать только для оптимизации, чтобы избежать «торможения». Если заглянуть внутрь пакета, то существенные значения: идентификатор устройства, код операции и данные (зависят от операции) – остались без изменения. И вроде бы поле «идентификатор устройства» логически должно отвечать за базовую безопасность, но, увы, оно используется не для защиты, а лишь только для адресации. Это поле используется и в протоколе Modbus RTU, и в Modbus TCP. В случае с TCP-версией оно либо игнорируется при непосредственном подключении, либо в дальнейшем используется шлюзом для маршрутизации. Относительно поля «код операции» можно сказать, что в TCP-версии при ответе устройства в нём может содержаться код ошибки, либо может быть полное дублирование отправленной информации, что наиболее вероятно. Получается, что при переходе к TCP-версии протокол фактически не изменился. Modbus-данные упаковываются в Ethernet-пакет, и используется порт 502. Все плюсы и минусы, присущие изначальной версии протокола, остались неизменными. Шифрование, аутентификация, авторизация – это всё не про Modbus. Но есть один момент с безопасностью, который всё-таки прописан в спецификации: указано, что на критически важных объектах связывающиеся узлы должны проверять друг друга по IP-адресу.

Если рассмотреть функциональность Modbus, то можно выделить три большие группы функций, которые позволяют нам узнать про устройство: стандартные (прописаны в спецификации), зарезервированные и пользовательские, последние вендор использует по своему усмотрению. В разрезе безопасности и защиты протокола стоит рассматривать лишь первый тип. К нему относится доступ к данным – чтение/запись из регистров. Также стандартно доступен достаточно большой список диагностических функций, который различен для разных каналов связи. Для TCP-версии наиболее интересна функция device identification, то есть система присвоения уникального идентификатора устройству. В стандарте прописано, что устройство должно сообщить о себе ряд обязательных (vendor name, product code, MajorMinorRevision) и необязательных данных (vendorUrl, ProductName, ModelName, UserApplicationName). Но стандарты зачастую не соблюдаются. Кто-то из производителей передаёт их, кто-то не передаёт, а кто-то передаёт, но другими способами. Например, используя ПО Modbus Device Identificator, можно просканировать всю сеть и определить абсолютно все Modbus-устройства, которые там используются. При этом подобных утилит очень много: пара приложений ModSim/ModScan, fuzzing-утилиты для поиска уязвимостей и ряд других, не стоит забывать про всем известные Wireshark и Python. Последняя позволяет очень просто создать скрипт (листинг 1), передающий Modbus-данные в Ethernet-сеть.

В итоге можно сделать вывод, что, имея доступ к Ethernet-сети без каких-либо дополнительных уровней защиты, можно довольно просто просканировать все Modbus-устройства и, например, обнулить все регистры, либо точечно передать ложные данные.

Ситуацию может спасти DPI-проверка данных. Но и тут не всё так однозначно, простота и удобство Modbus-протокола несут определённые сложности в реализации его защиты. Важно понимать, что для TCP протокол Modbus – это конвейер данных, информация передаётся байт за байтом. И устройство, вы-

Листинг 1. Пример скрипта для передачи информации по протоколу Modbus TCP

```
# скрипт, позволяющий передать ложные данные
from pyModbusTCP.client import ModbusClient
import time
c = ModbusClient()
c.host("192.168.1.1")
c.port(502)
c.open()
while True:
    address = 12288
    while 1 < 2:
        c.write_single_coil(address,0)
        c.write_single_register(12293,0)
        c.write_single_register(12291,100)
        regs=c.read_input_registers(12291,4)

    if regs is not None:
        print(regs)
    else:
        print("Fail!")
    time.sleep(1)
```

EtherWAN
www.etherwan.com

# Высокоскоростные удлинители Ethernet
## с питанием по сигнальной линии

**PoE-камера**

IEEE 802.3at / IEEE 802.3af


Модель ED3538T – удлинитель Ethernet по VDSL с передачей питания по сигнальному кабелю

Модель ED3538R – удлинитель Ethernet по VDSL с питанием от сигнального кабеля и передачей PoE-питания конечному устройству

- Передача питания для обратного преобразователя и конечного устройства на расстояние до 1300 м
- Скорость передачи данных по технологии Ethernet-over-VDSL до 100 Мбит/с
- Передача до 30 Вт на конечное устройство по PoE
- Удлинение Ethernet по двухжильному кабелю на расстояние до 2200 м
- Работа при температурах –40…+75°C

**Характеристики моста ED3538T – ED3538R с включенным питанием по сигнальной линии**

| Дистанция между удлинителями (м) | Скорость передачи данных по VDSL (Мбит/с) | Мощность для конечного PoE-устройства (Вт) |
|---|---|---|
| 300 | 100 | 30 |
| 600 | 60 | 14 |
| 800 | 45 | 9,5 |
| 1200 | 20 | 5 |

**Характеристики моста ED3538T – ED3538R с автономным питанием каждого удлинителя**

| Дистанция между удлинителями (м) | Скорость передачи данных по VDSL (Мбит/с) | Мощность для конечного PoE-устройства (Вт) |
|---|---|---|
| 1400 | 15 | 30 |
| 1600 | 10 | 30 |
| 1800 | 33 | 0 |
| < 2200 | 13 | 0 |

полняющее DPI, должно поверять каждый Modbus-пакет в Ethernet-пакете, фактически разворачивать и собирать пакет данных с полезной нагрузкой, как матрёшку. Ведь ложные данные могут содержаться в последовательности передаваемых Modbus-пакетов. Помимо механизмов фильтрации также необходимо проводить аналитику тех событий, которые происходят в сети при использовании промышленных протоколов.

В Modbus TCP индикаторами наличия вредоносных действий могут выступать следующие события:

- наличие Modbus-соединений, которые являются нетипичными для данной зоны;
- наличие неудачных попыток установки TCP/UDP-соединения по порту 502;
- сканирование порта 502 в широком диапазоне адресов;
- наличие команды сканирования от slave-устройства;
- использование команд, специфичных для различных производителей;
- поток пакетов данных ADU (Application Data Unit) с множеством различных команд;
- нетипичные команды;
- непоследовательная история полученных данных в ответах устройств;
- передача Modbus-данных в обход DMZ;
- трафик Modbus с использованием протокола UDP.

В модуле Tofino Modbus TCP Enforcer LSM реализована достаточно богатая функциональность, которая позволяет защитить протокол Modbus TCP. Фактически, используя данный модуль, можно обеспечить защиту данных на уровне регистров. Для каждого оконечного устройства можно задать ряд правил, которые будут включать разрешение или запрет доступа.

Создаваемое для протокола «правило на доступ» будет включать следующие параметры:

- связка IP/MAC-адрес;
- перечень значимых регистров;
- тип возможных операций (запрет доступа, только чтение, только запись, запись/чтение);
- идентификатор устройства;
- наличие проверки базовых команд (1–6, 15, 16, 20–24);
- установка контроля соединения;
- политики исключений;
- реакция в случае блокировки сообщения.

Сформировав данный список разрешённых запросов (рис. 3), можно защитить Modbus- устройство. Tofino Modbus TCP Enforcer LSM является «инспектором» контента для Modbus-протокола. При работе происходит полная DPI-проверка каждого Modbus-запроса и ответа, как для входящего, так и для исходящего трафика. Любая команда, которая не находится в списке разрешённых, или любая попытка доступа к регистрам данных, которая находится за пределами разрешённого диапазона запросов, блокируется, о чём сообщается на специальный IP-адрес. В итоге установка устройства Tofino Xenon с модулем Modbus TCP Enforcer LSM позволит не только защитить сеть на уровне протокола, но и повысить надёжность и снизить нагрузку сети.

## Tofino OPC Classic Enforcer LSM

Далее перейдём к модулю, который предназначен для защиты OPC-сервера. OPC (Open Platform Communications) – семейство программных технологий,

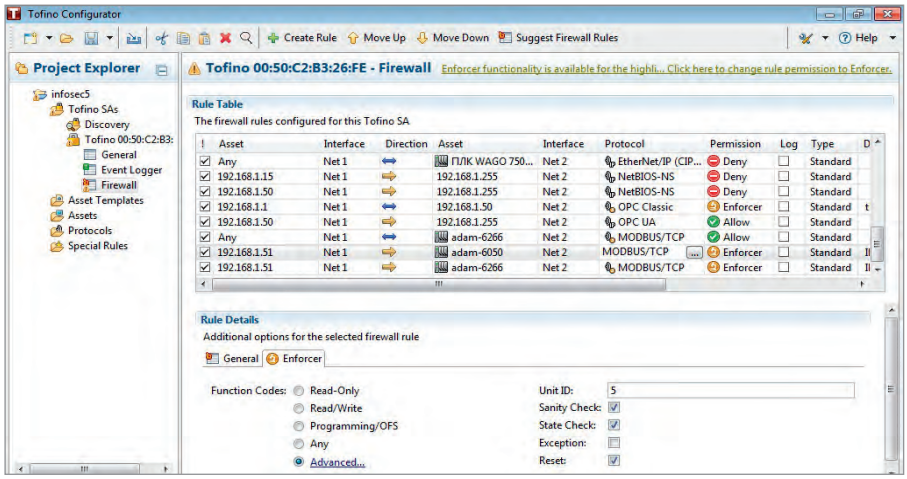



**Рис. 3. Настройка DPI-фильтра для протокола Modbus TCP**

предоставляющих единый интерфейс для управления объектами автоматизации и технологическими процессами. Технология OPC подразумевает работу по принципу клиент-сервер. В качестве OPC-клиента выступает программа диспетчеризации (SCADA) либо HMI (Human-Machine Interface), а OPC-сервер служит связующим звеном между клиентом и оконечными устройствами. OPC-серверы взаимодейству-ют с коммуникационными протоколами (Modbus, Profibus, Interbus, CAN-Bus и т.д.). Эта технология позволяет организовать доступ к данным промышленных систем автоматизации. Другими словами, благодаря стандартизации интерфейса стало возможным подключение любого физического устройства к любой SCADA-системе, если оно соответствует стандарту OPC. Но как обстоят дела с безопасностью сервера? Ведь он, по сути, является ключевой фигурой для связи между устройствами. Начнём с того, что сейчас доступны две технологии: OPC UA и OPC Classic. Первая является принципиально новым набором спецификаций, которая имеет достаточно широкий диапазон средств безопасности, от простой аутентификации с помощью пароля и обмена цифровыми подписями до полного шифрования передаваемых сообщений [4].

А вот с технологией OPC Classic всё достаточно непросто, особенно в плане безопасности. OPC Classic не определяет безопасность как часть каких-либо спецификаций интерфейса. По умолчанию OPC Classic построен на основе «транспорта» DCOM/COM от Microsoft (начиная с 1996 года). Сильно упрощая, можно сказать, что сервер экспортирует функции, которые клиент может вызывать, вынуждая сервер выполнить то или иное действие [5].

При этом связь организуется при помощи динамического распределения портов. Это и является основной уязвимостью OPC Classic. Протокол Modbus TCP использует порт 502, а HTTP использует порт 80, их редко кто-то меняет. А у OPC Classic диапазон номеров возможных портов может варьироваться от 1024 до 65535. При каждом открытии се-

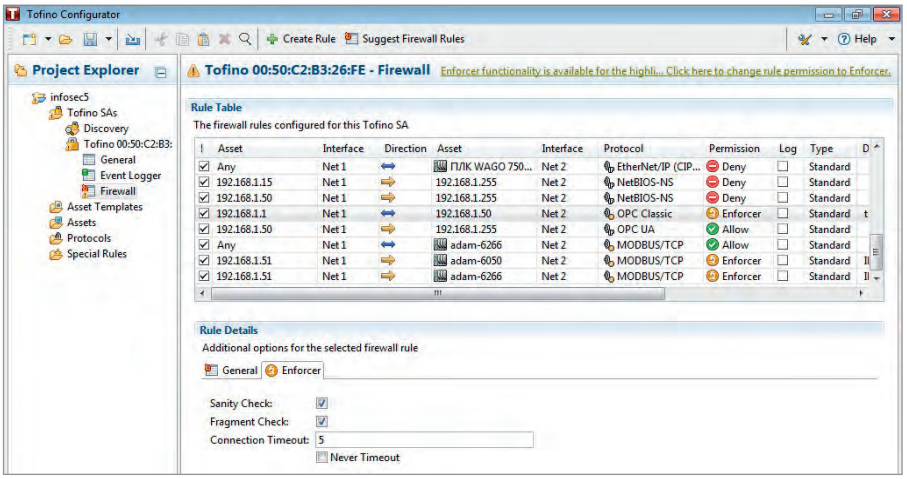



**Рис. 4. Настройка DPI-фильтра для протокола OPC Classic**

анса связи OPC-клиентом происходит динамическое назначение нового номера порта. Подключившись к OPC-серверу, OPC-клиент запрашивает номер TCP-порта, который должен быть использован для этой сессии. Затем производится новое соединение и заново отправляется запрос на номер свободного порта. По этой причине протокол OPC сложно и почти невозможно защитить с помощью классических стандартных брандмауэров, так как при настройках нужно будет открыть большой диапазон портов. Кроме того, в OPC Classic сервер должен иметь возможность инициировать связь с клиентом для обратных запросов, требующих доступа с сервера к клиенту. Эта функциональность приводит к тому, что все OPC-клиенты также настроены так, как будто бы они были OPC-сервером, а все OPC-серверы настроены так, как если бы они были OPC-клиентами.

Другими словами, для возможности работы OPC необходимо открыть практически все порты брандмауэра в обоих направлениях. В целом сервер OPC Classic может быть сконфигурирован так, чтобы обеспечить достаточную степень безопасности, но всегда стоит помнить, что она обеспечивается функциональностью DCOM/COM.

Один из вариантов решения данной проблемы – это контроль удалённого вызова процедур со стороны клиента (RPC – Remote Procedure Call, класс технологий, позволяющих вызывать функции или процедуры в другом адресном пространстве). На транспортном уровне RPC используют в основном протоколы TCP и UDP. RPC может быть настроен так, чтобы либо ограничивать диапазон используемых портов, либо статически назначать фиксированный порт данному серверу OPC Classic. Но назначение фиксированного порта может не работать на различных версиях OPC Classic. В итоге такое решение необходимо дополнительно тестировать, чтобы убедиться в его работоспособности. Иной вариант решения – это контроль пользователем OPC каждого соединения с помощью DPI-инспекции. Необходимо контролировать за-

просы на подключение к серверу, обратные ответы к клиенту, фактически контролировать всю сессию, которая включает такие параметры, как тип сообщения, номер порта, адрес OPC-сервера, адрес OPC-клиента. При подобном подходе можно обеспечить защиту OPC-сервера.

Примером подобного решения, которое может контролировать сессию OPC Classic, основанную на технологии Microsoft DCOM/COM, является программный модуль Tofino OPC Classic Enforcer LSM в составе программно-аппаратного комплекса Tofino Xenon. Tofino OPC Classic Enforcer LSM проверяет, отслеживает и защищает каждое соединение, созданное приложением OPC. Комплекс динамически открывает только TCP-порты, необходимые для каждого соединения, и только между конкретным OPC-клиентом и сервером, который создал соединение (рис. 4). При настройке данных нет необходимости изменений конфигурации на клиентах и серверах OPC.

В качестве дополнительной защиты со стороны OPC-клиента (как правило, это машина на которой установлена SCADA-система) желательно использовать хороший антивирус, ограничивающий на уровне системы управления эфирные окна сеанса обмена запросами и ответами между OPC-клиентами и серверами.

## Заключение

Глубокая проверка данных (DPI) на уровне промышленных протоколов является защитой, способной распознать самые изощрённые угрозы. Многие промышленные протоколы, такие как Modbus и OPC Classic, имеют ряд уязвимостей, которые могут привести к печальным и очень затратным последствиям.

Один из вариантов защиты – это глубокий анализ специфичных данных, присущих тому или иному протоколу. Программно-аппаратный комплекс Tofino Xenon – один из примеров устройства, которое может обеспечить реальную защиту промышленных протоколов и оконечных устройств.

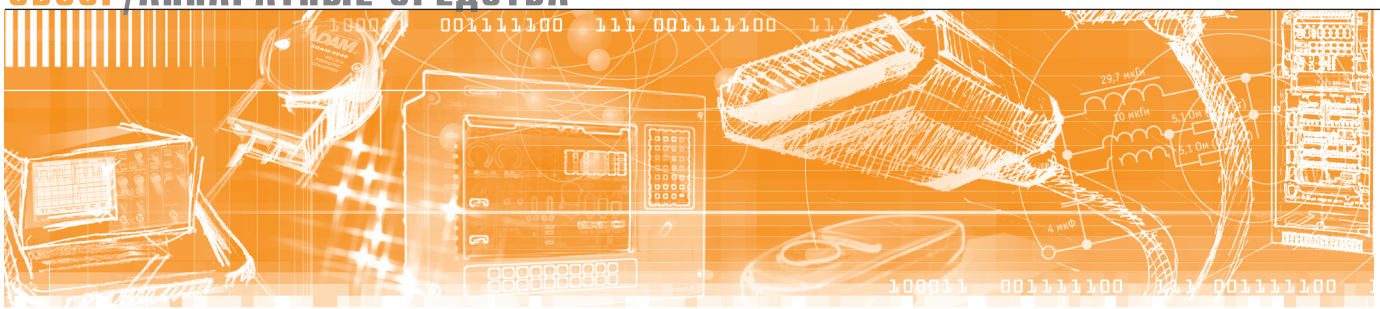
В данной статье были рассмотрены модули для защиты протоколов Modbus TCP и OPC Classic. В следующей части статьи будут описаны типичные уязвимости для протоколов Ethernet/IP, IEC104, DNP3 и GOOSE, а также механизмы их защиты. ●

## Литература


1. Воробьёв С. Глубокая защита промышленного сетевого периметра // Современные технологии автоматизации. – 2017. – № 4.
2. Классификация firewall'ов и определение политики firewall'а [Электронный ресурс] // Режим доступа : https://www.intuit.ru/studies/courses/20/20/lecture/625?page=6.
3. Воробьёв С. "Defense in Depth" в действии. Уровень 1: защита границы сети // Современные технологии автоматизации. – 2017. – № 4.
4. Спецификация OPC UA [Электронный ресурс] // Режим доступа : http://www.bookasutp.ru/Chapter9_2_4.aspx.
5. Введение в COM/DCOM [Электронный ресурс] // http://www.delphikingdom.ru/asp/viewitem.asp?catalogid=1108.



**Автор – сотрудник фирмы ПРОСОФТ**
**Телефон: (495) 234-0636**
**E-mail: info@prosoft.ru**



*Дмитрий Кабачник*

# Взрывозащищённый планшет Getac EX80 под управлением Windows 10

**В статье рассказывается о новейшем полностью защищённом планшете EX80 компании Getac, который предназначен для использования во взрывоопасных зонах. Приводится подробный обзор его технических характеристик, рассматриваются аксессуары и возможности применения.**

## Введение

В первом квартале 2018 года компания **Getac** представила свой новый 8″ защищённый планшет **EX80** под управлением операционной системы Windows 10 для работы в опасных средах. Getac EX80 (рис. 1) можно безопасно использовать в зонах с потенциально взрывоопасной атмосферой, которая часто встречается на различных нефтегазовых, нефтехимических и производственных предприятиях. Сам термин «взрывоопасная зона» ведёт происхождение из электротехники, где таким образом определяется место, в котором находятся легковоспламеняющиеся газы, пары, пыль или волокна. Электронное оборудование, которое используется в этих зонах, должно быть спроектировано таким образом, чтобы оно никоим образом не могло воспламенить потенциально взрывоопасные вещества. Устройства, которые соответствуют таким требованиям и регламентам, называются взрывобезопасными или взрывозащищёнными.

Одной из проблем при создании таких устройств является то, что взрывоопасные зоны на одном объекте могут иметь разную степень потенциальной опасности. Большинство таких объектов являются многоуровневыми, то есть некоторые участки безопасны и не требуют специальных мер предосторожности, тогда как другие уже отно-


**Рис. 1. Планшет Getac EX80**

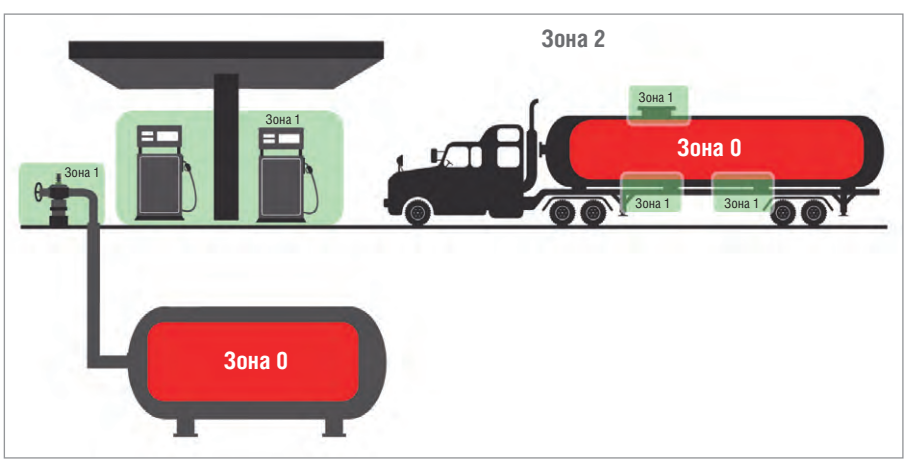



**Рис. 2. Расположение взрывоопасных зон на бензоколонке**

сятся к категории опасных в большей или меньшей степени. Каждая из таких зон имеет свои требования к электронным устройствам в части их взрывобезопасности и электронной безопасности. Примером может служить изображение зон на самой обычной автозаправочной станции (рис. 2).

Даже находясь в одном здании, сотрудники могут работать в разных областях, это означает, что все электронные устройства, которые используются, должны быть сертифицированы согласно требованиям, предъявляемым к каждой из зон. Именно поэтому сотрудникам необходим мобильный производительный компьютер, сертифицированный для использования во всех опасных зонах.

## Обзор технических характеристик планшета

Начнём с аппаратной платформы планшета Getac EX80. Согласно требованиям по взрывобезопасности, должны быть устранены все возможные причины воспламенения, связанные с использованием электронного устройства. Эти требования серьёзно влияют на дизайн корпуса мобильного компьютера, на температуру его внешних частей, механическую прочность, зарядку, устранение разъёмов различных портов, использование которых может вызвать искру в опасной зоне, и многое другое. Если говорить о EX80 [1], то устройство имеет довольно скромные габариты, обусловленные в основном размерами дисплея и батареи. Планшет имеет размеры всего 240×155 мм, а его толщина составляет лишь 29 мм. При этом он может выдерживать падения с высоты 1,8 м, что подтверждено испытаниями согласно американскому военному стандарту MIL-STD-810G. Надо отметить, что тесты по этому стандарту не ограничены стандартными процедурами проверки на падение с высоты, вибрацию и удар, а включают в себя испытания на защиту от соляного тумана и влажности. EX80 имеет довольно широкий диапазон рабочих температур от –21 до +50°C и защищён от влаги и пыли в соответствии с IP67, что означает возможность погружать планшет на глубину до 1 м в течение 30 минут. Таблица 1 содержит технические характеристики планшета EX80, а также перечень сертификатов взрывозащиты, которым соответствует этот мобильный компьютер.

Для обеспечения соответствия нормам взрывобезопасности устройство не имеет стандартных портов доступа, поскольку такие электронные составляющие должны быть полностью герметизированы и закрыты. Даже 20 винтов, удерживающих корпус, имеют необычный формат, чтобы препятствовать разбору планшета в опасной зоне. Взрывозащищённое исполнение означает и другие отклонения от стандартного исполнения. Так, например, температуре поверхности устройства уделено больше внимания – для её регулировки и предотвращения воспламенения используются специальные датчики и дополнительное охлаждение. Зарядка планшета также осуществляется без стандартного разъёма питания, использование которого могло бы вызвать искру и воспламенение. Обязательно следует отметить, что модель защищена от короткого замыкания. Помимо этого, в мобильном компьютере используются антистатические материалы и специальное изолирующее покрытие электронных компонентов планшета для исключения любой возможности появления искры. Getac проводит для EX80 обширные термические и ударные испытания, чтобы иметь уверенность в качестве сборки каждого изделия. Модульность устройства, означающая широкие возможности по кастомизации, принятая компанией Getac в своих изделиях и

*Таблица 1*

**Технические характеристики планшета Getac EX80**

| | |
|---|---|
| Операционная система | Windows 10 Pro |
| Мобильная вычислительная платформа | Процессор Intel Atom x5-Z8350 1,44 ГГц, в пиковом режиме до 1,92 ГГц, кэш 2 Мбайт |
| Видеоконтроллер | Intel HD Graphics |
| Дисплей | 8-дюймовый ЖК-дисплей, технология IPS TFT, разрешение WXGA (1280×800) |
| | Дисплей с технологией LumiBond для чтения при солнечном свете, 600 нит |
| | Ёмкостный сенсорный экран с поддержкой работы в перчатках |
| Накопитель и память | 4 Гбайт LPDDR3 |
| | eMMC 128 Гбайт |
| Клавиатура | 6 функциональных клавиш (Windows, питание, две программируемые клавиши, увеличение и уменьшение громкости) |
| Указывающее устройство | Сенсорный ёмкостный мультитач-экран |
| Интерфейсы ввода-вывода данных | FHD-веб-камера |
| | Задняя камера 8 Мпиксел с автофокусом и светодиодной вспышкой |
| | Разъём для док-станции |
| | Опциональное гнездо для SIM-карты |
| Интерфейсы связи | 802.11a/b/g/n |
| | Bluetooth (v4.0) |
| | Выделенный GPS (со встроенной антенной) |
| | Опциональный модуль мобильной широкополосной связи 4G LTE |
| Программное обеспечение | Getac Utility (включая Power Manager) |
| | Опциональный Absolute DDS Persistence |
| Беспроводные модули | Считыватель HF RFID |
| Питание | Офисная док-станция (зарядная база, блок питания 24 Вт, ~100–240 В, 50/60 Гц) |
| | Литий-ионный аккумулятор (7,4 В; 4200 мА·ч) |
| Размеры (Ш×Г×В) и масса | 240×155×29 мм |
| | 1,48 кг |
| Защищённость | Сертификаты MIL-STD-810G и IP67 |
| | Выдерживает падение с высоты 1,8 м |
| | Сертифицированно стойкий к воздействию соляного тумана |
| | Устойчив к вибрации и падениям |
| Условия окружающей среды | Температура эксплуатации –21…+50°C, хранения –51…+71°C |
| | Относительная влажность 95% без образования конденсата |
| Взрывозащита | ATEX/IECEx |
| | Ex II 1 GD |
| | Ex ia op is IIC T4 Ga |
| | Ex ia op is IIIC T135eC Da |
| | UL913 |
| | Класс I, зона 0, AEx ia op is IIC T4 Ga |
| | Класс II, зона 20, AEx ia op is IIIC T135eC Da |
| | Класс I, раздел 1, группы A, B, C, D |
| | Класс II, раздел 1, группы E, F, G |
| | Класс III, раздел 1 |


**Рис. 3. Дисплей EX80 в разобранном виде**

столь популярная среди пользователей, когда речь идёт об устройствах общего назначения, в данном случае играет отрицательную роль. По требованиям взрывобезопасности любые изменения в мобильном компьютере потребуют повторной сертификации, поэтому от многих опций во взрывобезопасных устройствах приходится отказываться.

Следует подробно рассмотреть дисплей планшета (рис. 3). Getac EX80 оснащён 8″ ЖК-дисплеем с разрешением WXGA (1280×800), в котором используется матрица с технологией IPS TFT, что существенно увеличивает угол обзора и полностью устраняет цветовые и контрастные сдвиги. Благодаря технологии LumiBond 2.0, которая также применяется в данном устройстве, EX80 подходит для работы под прямыми солнечными лучами или яркими источниками искусственного света, которые часто встречаются на различных производственных объектах. Максимальная яркость дисплея Getac EX80 составляет 600 кд/м$^2$. Для сравнения нужно отметить, что яркость монитора обычного персонального компьютера колеблется в диапазоне значений от 200 до 250 кд/м$^2$. Планшет оснащён сенсорным дисплеем с функцией распознавания нескольких одновременных прикосновений. Отличительной особенностью такого мультитач-экрана является возможность работать с ним в перчатках, что по достоинству должны оценить многие специалисты, сталкивающиеся с необходимостью часто снимать перчатки при работе со своей мобильной техникой. С отображаемой на дисплее информацией также можно работать с помощью стилуса, поставляемого вместе с планшетом. Дисплей защищён двухмиллиметровым закалённым стеклом, которое не треснет и не разобьётся даже при серьёзных физических воздействиях.

Любое современное мобильное устройство должно обладать достаточной производительностью для работы с требовательным современным программным обеспечением. Взрывозащищённые планшеты не являются исключением, поэтому Getac EX80 оснащён производительным четырёхъядерным процессором Intel Cherry Trail X5-Z8350 серии Atom с тактовой частотой 1,44 ГГц и с кэш 2 Мбайт. Процессор выполнен по 14-нанометровому техпроцессу и в пиковом режиме может выдавать до 1,92 ГГц. Относящийся к серии Intel Atom процессор среднего уровня часто используется в безвентиляторных мобильных устройствах, в том числе и в планшетах. ОЗУ и память компьютера фиксированы и не меняются в зависимости от комплектации. Пользователь получит 4 Гбайт оперативной памяти LPDDR3 и 128 Гбайт твердотельной памяти eMMC.

EX80 обладает достаточным арсеналом беспроводных интерфейсов: есть двухдиапазонный Wi-Fi 802.11a/b/g/n, Bluetooth версии 4.0 и высокочастотный RFID. Также имеется встроенный GPS для определения местонахождения планшета в данный момент. В LTE-версии устройства пользователям опционально доступен модем 4G LTE WWAN.

Поскольку в EX80 отсутствует разъём питания, зарядка осуществляется через

## Для классификации защищённого компьютерного оборудования производители обычно используют следующие стандарты:

Для классификации защищённого компьютерного оборудования производители обычно используют следующие стандарты:

- North American National Electric Code (NEC) – Североамериканский электрический кодекс;
- Международная директива IECEx;
- Европейская директива ATEX (ATmospheres Explosives).

Рассмотрим классификацию по этим стандартам.

NEC в первую очередь различает классы:

- класс 1 (легковоспламеняющиеся газы);
- класс 2 (легковоспламеняющаяся пыль);
- класс 3 (легковоспламеняющиеся волокна).

Каждый из классов, в свою очередь, подразделяется на:

- раздел 1 (вещество присутствует всё время);
- раздел 2 (вещество присутствует в течение короткого времени).

Затем следует третий уровень (группа) для описания конкретного типа газа, пыли или волокон.

В IEC/ATEX, в первую очередь, различают:

- легковоспламеняющиеся газы и пары (G);
- воспламеняющуюся пыль (D).

Затем легковоспламеняющиеся газы:

- зона 0 (всегда присутствует);
- зона 1 (вероятно присутствует);
- зона 2 (иногда присутствует).

Воспламеняющаяся пыль разделяется следующим образом:

- зона 20 (всегда присутствует);
- зона 21 (вероятно присутствует);
- зона 22 (иногда присутствует).

В каждой зоне также классифицируется и само оборудование для этих зон:

- категория I (присутствует непрерывно);
- категория II (присутствует с перерывами);
- категория III (иногда присутствует).

Рассмотрим в качестве примера обычную АЗС. По классификации NEC подземные газовые резервуары и цистерны грузовиков относятся к классу 1, разделу 1; площадь вокруг грузовика-цистерны или заправочной колонки будет также соответствовать классу 1, разделу 1; а общая площадь АЗС – класс 1, раздел 2 [2].

Используя классификацию IEC/ATEX, подземные цистерны с топливом и цистерны грузовиков можно отнести к зоне 0, категории I; площадь вокруг грузовика-цистерны или заправочной колонки будет представлять собой зону 1, категории I; а остальная площадь АЗС – зона 2, категория 2.

Представленная здесь информация существенно упрощена, поскольку оба стандарта имеют несколько дополнительных критериев классификации, таких как температура, уровни защиты и т.д. ■

Рис. 4. EX80 на док-станции

Рис. 5. Планшет EX80 на четырёхточечном ремне

контакты с поверхностным креплением через док-станцию из комплекта поставки (рис. 4). Док-станция, безусловно, должна устанавливаться во взрывобезопасной зоне. Планшет оснащён литий-ионным аккумулятором ёмкостью 4200 мА·ч и напряжением в 7,4 В, которого, по заявлениям производителя, должно хватать на 8,5 часов беспрерывной работы в экономном режиме. У EX80 отсутствует функция «горячей» замены аккумулятора, что, с одной стороны, является минусом, а с другой стороны, эту замену приходилось бы осуществлять только во взрывобезопасной зоне. Поэтому, скорее всего, отсутствие данной опции связано с соблюдением безопасности во взрывоопасных зонах, плюс добавление дополнительного аккумулятора увеличило бы вес, размеры и, самое главное, стоимость планшета.

В дополнение к мобильному компьютеру пользователи могут заказать несколько аксессуаров для упрощения работы с ним в условиях производства. Например, четырёхточечный наплечный ремень позволяет освободить обе руки при работе с устройством (рис. 5), а браслет на руку с функцией вращения и подставки позволяет легко удерживать планшет одной рукой или поставить его рядом с оборудованием на подставку (рис. 6).

## Подводя итоги

EX80 является удобным, современным и полностью защищённым план-

**Рис. 6. Планшет EX80 на подставке, в качестве которой используется браслет на руку**


**Рис. 7. Экранная форма Windows 10 на планшете EX80**

шетом под управлением Windows 10 (рис. 7). Одновременно это сертифицированное согласно ATEX, IECEx и UL913 устройство для работы во взрывоопасных средах, что делает его незаменимым для всех производств, где пользователи могут столкнуться с опасными средами и где необходимо использование надёжной мобильной техники. EX80 обеспечит своим пользователям высокое качество изображения, точный ввод информации и максимальную безопасность в сочетании с высокой производительностью.

Благодаря этому планшет Getac EX80 подходит для работы на различных нефтегазовых предприятиях, где одна-единственная искра может привести к катастрофе. ●

## Литература

1. Getac EX80 [Электронный ресурс] // Режим доступа : http://getac.ru/tablets/ex80/features.html.
2. Guide to Explosive Atmospheres [Электронный ресурс] // Режим доступа : http://ecatalog.weg.net/files/wegnet/WEG-guide-to-explosive-atmospheres-wallchart-50042119-quick-guide-english.pdf.

**Автор – сотрудник фирмы ПРОСОФТ**
**Телефон: (495) 234-0636**
**E-mail: info@prosoft.ru**

Getac

Windows 10
Getac рекомендует Windows 10


Getac S410

# ПОЛУЗАЩИЩЁННЫЙ. ПОЛНОСТЬЮ НАДЁЖНЫЙ.

- Процессоры Intel® Core™ i3/i5/i7 7-го и 8-го поколения
- Основная батарея повышенной ёмкости с функцией «горячей» замены
- Опциональный сверхъяркий дисплей 800 кд/м² с сенсорной панелью multitouch
- Улучшенные функции аутентификации: сканер отпечатка пальцев и считыватель карт
- Широчайший набор портов ввода-вывода

ProSoft®
WWW.PROSOFT.RU

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

**МОСКВА**
(495) 234-0636
info@prosoft.ru

**САНКТ-ПЕТЕРБУРГ**
(812) 448-0444
info@spb.prosoft.ru

**ЕКАТЕРИНБУРГ**
(343) 356-5111
info@prosoftsystems.ru

УЗНАТЬ БОЛЬШЕ

# FASTWEL I/O в распределённых системах управления

*Виктор Пальгов*

**В статье рассматриваются структура и функции распределённой информационно-управляющей системы газораспределительной станции на основе контроллера FASTWEL I/O. Описаны преимущества распределённых систем перед централизованными.**

На протяжении всей истории развития программируемых логических контроллеров (ПЛК), от первых логических аппаратов на жёсткой дискретной логике компании Modicon до ПЛК, свободно программируемых на пяти технологических языках международного стандарта МЭК61131-3, параллельно совершенствовались и способы информационного взаимодействия контроллеров. Первые промышленные ПЛК не отличались изяществом форм и простотой обслуживания. Их габариты, аппаратные средства и средства конфигурирования определяли условия и правила взаимодействия с периферийным оборудованием. По большей части такие системы строились по централизованному принципу, что для разработчиков подобных систем и служб эксплуатации в ту пору представлялось оптимальным.

Технологическая революция в микроэлектронике 70-х годов XX века породила целые семейства разнообразных микропроцессоров и однокристальных микроЭВМ, за которыми впоследствии прочно закрепился термин «микроконтроллер». Микроконтроллеры отличались архитектурой, структурой внутренней памяти, системой команд, разрядностью информационной шины и арифметических вычислений. Однако, несмотря на разнообразие типов, у всех микроконтроллеров было одно достоинство – они прекрасно подходили для построения ПЛК, которые, в свою очередь, совершили революцию в сфере автоматизации технологических процессов. Со временем ПЛК прочно заняли место промышленных контроллеров, работающих в режиме реального времени.

Вместе с тем, несмотря на значительные перемены в исполнении, производительности и способах программирования ПЛК, структура системы управления в большинстве промышленных применений остаётся прежней, то есть централизованной. Такое положение дел объясняется не только консерватизмом разработчиков АСУ ТП и служб эксплуатации. Если говорить о предприятиях газовой промышленности и конкретно о газораспределительных станциях, то здесь определяющую роль играют требования промышленной безопасности. При всём существующем разнообразии на рынке ПЛК найдётся не так много устройств, обладающих необходимыми массогабаритными и энергетическими характеристиками, а также отказоустойчивостью, позволяющими эксплуатировать их на опасных производственных объектах в потенциально взрывоопасных средах.

## Предпосылки создания системы

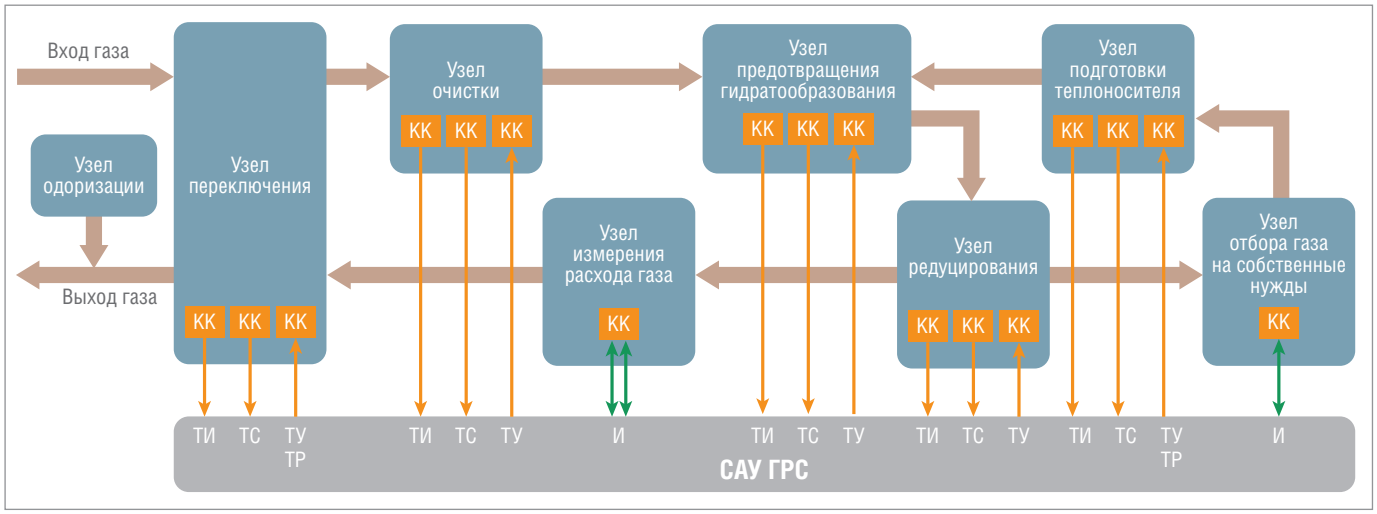
На заводе «Газпроммаш» в рамках выполнения собственной программы НИОКР была поставлена задача разработать серию устройств, позволяющих оборудовать каждый технологический узел газораспределительной станции блоками локальной автоматики, объединёнными общей информационной сетью. Задача построении подобных систем, на первый взгляд, не отличается оригинальностью. И всё же специфика применения и особенности функционирования разрабатываемого оборудования требуют досконального знания технологических процессов на газораспределительных станциях и блоках подготовки газа, необходимости проработки алгоритмов для каждого технологического узла и алгоритмов взаимодействия этих узлов между собой. Таким образом, система в целом не должна ограничиваться тривиальным сбором данных от датчиков, установленных на технологических узлах, и выполнять команды от верхнего уровня автоматизации. По совокупности реализуемых функций и способам информационного взаимодействия разработанная на заводе аппаратно-программная конструкция представляет собой распределённую информационно-управляющую систему – РИУС.

## Задача и её решение

Чтобы определить необходимый объём автоматизации, достаточно перечислить состав современной газораспределительной станции (ГРС) по технологическим узлам:

- узел переключения;
- узел очистки газа;
- узел предотвращения гидратообразования;
- узел подготовки теплоносителя;
- узел редуцирования газа;
- узел измерения расхода газа;
- узел отбора газа на собственные нужды;
- узел одоризации.

Структура традиционной системы автоматизации ГРС, взаимодействие САУ ГРС с первичными датчиками и испол-




**Условные обозначения:** КК – клеммная коробка; ТИ – телеизмерения; ТС – телесигнализация; ТУ – телеуправление; ТР – телерегулирование; И – интерфейс информационной сети.

**Рис. 1. Структура системы автоматики централизованного типа**

нительными механизмами выглядит так, как показано на рис. 1. При этой структуре бóльшая часть сигнальных кабелей от датчиков и исполнительных устройств идёт напрямую в САУ ГРС или через промежуточные клеммные коробки, объединяющие несколько кабелей в один многожильный.

## Архитектура РИУС

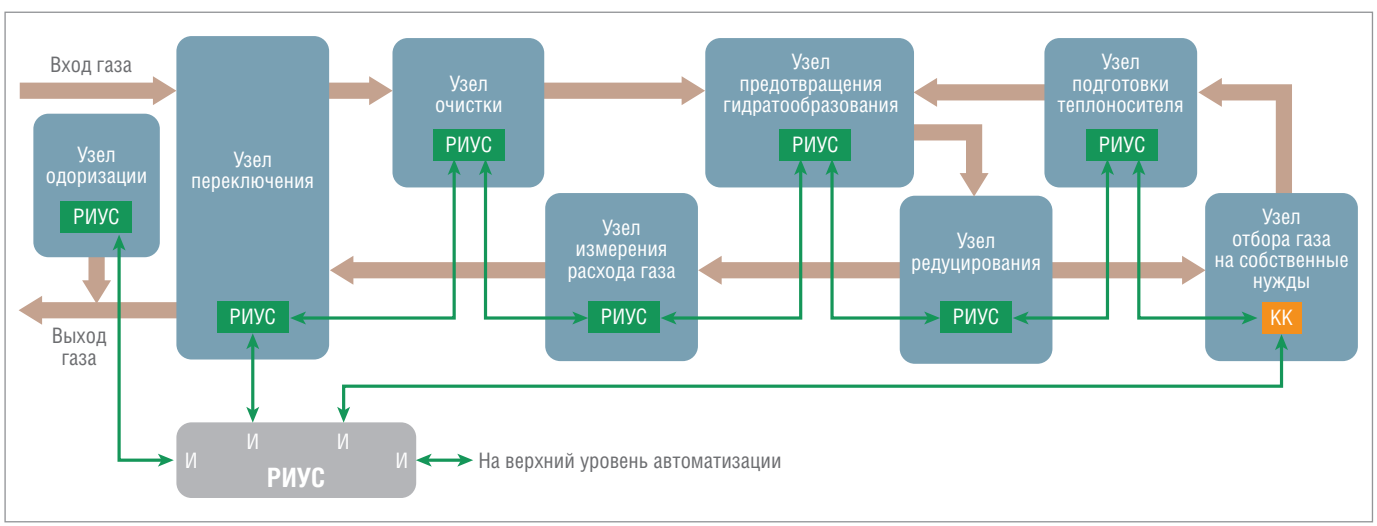
В случае применения РИУС структура системы автоматизации ГРС будет выглядеть как совокупность контроллеров, заключённых во взрывонепроницаемую оболочку и объединённых в единую информационную сеть, как показано на рис. 2. Здесь каждый технологический узел ГРС оборудован собственной локальной системой автоматики, являющейся частью распределённой информационно-управляющей системы. Для каждого технологического узла характерен свой набор первичных датчиков, исполнительных устройств и определённый набор алгоритмов автоматического управления.

Преимущества распределённых систем перед централизованными давно известны и описаны в различной научной и практической литературе по автоматизации. Вот лишь некоторые основные характеристики РИУС, определяющие выгоды от её применения:

- высокая надёжность (отказ одного из компонентов РИУС не приводит к отказу системы в целом);
- повышенное быстродействие, обусловленное параллельной работой нескольких контроллеров в системе;
- устойчивость к сбоям и помехам как следствие локальной установки блоков и уменьшения длины сигнальных линий;
- возможность поузлового проектирования с использованием структуры объекта управления;
- упрощённый порядок модернизации системы.

## Аппаратно-программная реализация

Для реализации системы разработчиками был выбран российский модульный программируемый логический контроллер для жёстких условий эксплуатации – FASTWEL I/O. Это один из немногих контроллеров, представленных на российском рынке ПЛК, обеспечивающий необходимые массогабаритные и вычислительные характеристики для размещения во взрывозащищённом корпусе с маркировкой взрывозащиты 1ExdIIBT5. Немаловажным аргументом в пользу такого выбора является наличие у производителя разрешения Федеральной службы по экологическому, технологическому и атомному надзору на применение в нефтяной и газовой промышленно-




**Условные обозначения:** И – интерфейс информационной сети; РИУС – узел распределённой информационно-управляющей системы.

**Рис. 2. Структура системы автоматики распределённого типа**

сти. Кроме того, номенклатура модулей ввода-вывода FASTWEL I/O позволяет оптимизировать аппаратную структуру для конкретного технологического узла. Например, для автоматизации узла переключения понадобится следующий набор модулей:

- программируемый контроллер узла сети Modbus RS-485 CPM712-01;
- модуль подключения источника питания 24 В/6,3 А OM752-01;
- три 8-канальных модуля дискретного ввода DIM762-01;
- два 8-канальных модуля дискретного вывода DIM719-01;
- один 8-канальный модуль аналогового ввода AIM791-01;
- один 2-канальный модуль аналогового вывода AIM730-02;
- модуль оконечной нагрузки шины OM750-01 (заглушка шины FBUS).

Блок управления узлом переключения в приведённой комплектации полностью обеспечивает выполнение технологических алгоритмов и алгоритмов аварийной защиты:

- аварийное отключение ГРС со стравливанием газа при пожаре и загазованности;
- аварийное отключение ГРС без стравливания при низком входном давлении газа;
- закрытие выходного крана по превышению давления газа на выходе ГРС;
- включение в работу обводной линии ГРС при неисправностях на станции;
- проверка работоспособности крана-регулятора на обводной линии;
- управление аварийной вытяжной вентиляцией.

Программная реализация алгоритмов РИУС выполнена в среде разработки CODESYS, дополненной пакетом адаптации прикладных программ FASTWEL I/O.

## Функционирование и особенности реализации системы

На этапе разработки алгоритмов для технологических узлов специалисты руководствовались документом ПАО «Газпром» «Перечень типовых функций, выполняемых САУ ГРС по технологическим узлам и системам». Большая часть алгоритмов была ранее написана разработчиками для централизованной системы управления ГРС.

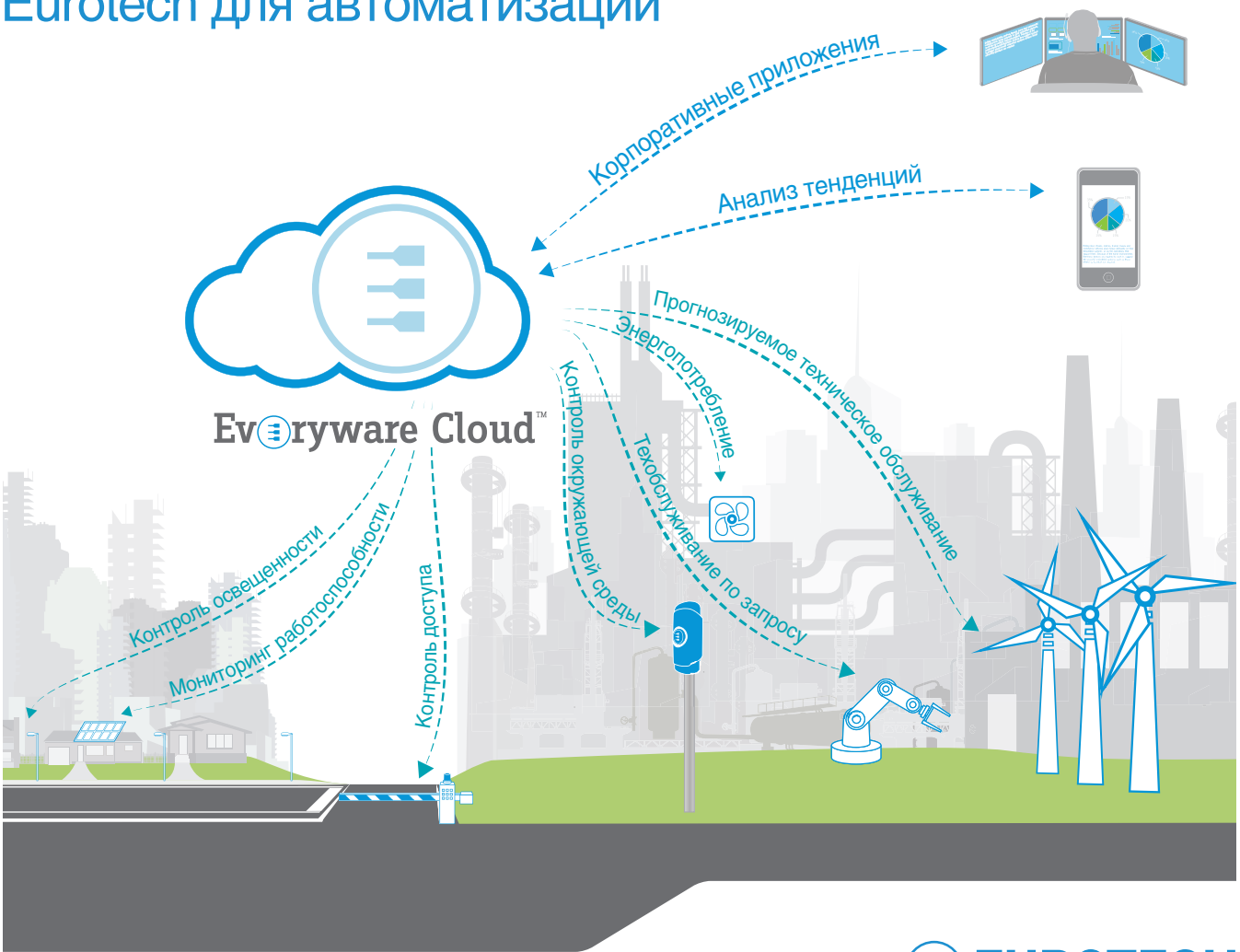
Каждый из перечисленных алгоритмов может быть инициирован автоматически, при регистрации аварийной ситуации на ГРС, запущен по инициативе оператора ГРС либо дистанционно диспетчером линейного производственного управления. Также возможна дистанционная блокировка любого алгоритма.

Кроме базовых алгоритмов, относящихся к аварийной защите ГРС, защите эксплуатирующего персонала и потребителей газа, каждый блок РИУС выполняет множество различных функций диагностики состояния периферийного оборудования КИПиА и самодиагностики контроллера.

Для датчиков аналоговых сигналов выполняется контроль обрыва и короткого замыкания кабеля, выхода измеряемого сигнала за пределы технологических уставок, а также вычисление критической скорости возрастания или убывания измеряемого сигнала и его фильтрация.

Для дискретных сигналов отслеживается целостность сигнального кабеля и при необходимости устраняется дребезг контактов датчика.

# Облачные технологии
## Eurotech для автоматизации




EUROTECH
Imagine. Build. Succeed.

Решения Eurotech позволяют заказчикам удобно и безопасно подключать оборудование и датчики к корпоративным программным приложениям с помощью **Everyware Cloud™ — M2M-платформы.**

### Выполняемые функции

- Управление устройством
- Приложение для устройства и управления жизненным циклом
- Контроль состояния устройства/связи в режиме реального времени
- Поддержка промышленных протоколов
- Простая интеграция с корпоративными приложениями
- Сбор потоков данных с различных устройств в реальном времени
- Анализ данных в реальном времени, их хранение и предоставление исторических данных

Взятый ПАО «Газпром» курс на внедрение безлюдных технологий в системах транспортировки, хранения и распределения газа существенно повышает требования к диагностике состояния эксплуатируемого оборудования, его своевременному техническому обслуживанию и ремонту. С этой целью для каждого типа оборудования, подключённого к блоку РИУС, разработаны специальные алгоритмы диагностики, предотвращения выхода из строя и предупреждения аварийных ситуаций. К примеру, шаровой кран с электропневматическим блоком, имеющий два соленоида управления и два контакта сигнализации, сопровождается следующим набором алгоритмов:

- закрытие/открытие по команде с отслеживанием достижения крайнего положения;
- контроль времени перемещения в крайнее положение;
- контроль изменений длительности открытия и закрытия крана;
- дожатие крана после регистрации конечного положения;
- контроль самопроизвольного открытия или закрытия крана;
- возврат крана в крайнее положение после самопроизвольного открытия/закрытия;
- периодическая проверка способности крана к перемещению.

Технологические уставки, временны́е характеристики и коэффициенты масштабирования для каждого датчика и исполнительного устройства хранятся в энергонезависимой памяти контроллера СРМ712. Бóльшая часть из них может быть установлена или изменена дистанционно при непременном разграничении прав доступа эксплуатирующего персонала. Некоторые параметры вычисляются автоматически в процессе самодиагностики.

Как было сказано ранее, каждый блок РИУС отвечает за конкретный технологический узел ГРС. Все блоки РИУС объединены в информационную сеть. Эта сеть может быть выполнена на базе витой пары с интерфейсом RS-485, Ethernet промышленного типа или волоконно-оптического кабеля. В двух последних случаях вместо контроллера узла сети СРМ712 используется его модификация с интерфейсом Ethernet – СРМ713. Один из блоков, как правило, – блок, отвечающий за обмен данными с верхним уровнем автоматизации, является координатором взаимодействия между всеми остальными блоками в распределённой сети. Для его реализации привлекательной выглядит новая разработка в линейке контролле-

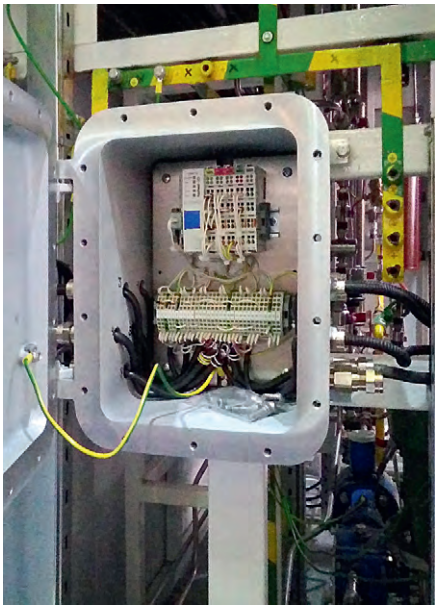


**Рис. 3. Взрывозащищённый блок РИУС на одоризационной установке**

ров FASTWEL I/O – универсальный контроллер CPM723. Заявленные характеристики производительности и развитые коммуникационные возможности кажутся перспективными в промышленных сетях со смешанной топологией, к которым относится информационная сеть РИУС.

Блоки РИУС, расположенные во взрывоопасных зонах, заключены во взрывонепроницаемую оболочку. На рис. 3 представлена фотография блока, смонтированного на одоризационной установке. Блоки, установленные в невзрывоопасных помещениях, таких как операторная или помещение котельной, имеют общепромышленное исполнение. Кроме того, есть внешние блоки, отвечающие за работу подогревателя газа и одоризатора.

## Заключение

Возвращаясь к преимуществам распределённых систем перед централизованными, всё же следует отметить, что наиболее рациональным применение РИУС видится на объектах блочно-модульного типа, когда технологические узлы ГРС расположены на площадке на некотором удалении друг от друга и от помещения операторной, где обычно находится главный шкаф автоматики. На таких объектах их применение выгодно за счёт сокращения межблочных кабельных линий, кабельных проходок и вводов, клеммных коробок и, как следствие, уменьшения сроков монтажных и пусконаладочных работ.

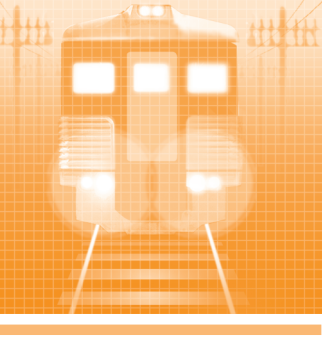
С другой стороны, для моноблочных конструкций ГРС, расположенных на едином фундаменте, применение РИУС тоже может дать некоторые выгоды, как проектировщикам, так и изготовителям. Как правило, моноблочные здания имеют габариты, позволяющие перевозить их железнодорожным или автомобильным транспортом, а также модульную конструкцию, состоящую из нескольких отсеков.

На объекте эти конструкции собираются воедино. При этом кабельные линии монтируются от клеммных коробок или приборов до шкафа автоматики и тянутся по коробам и лоткам через все модули ГРС. В случае применения РИУС от каждого модуля достаточно протянуть только две-три кабельные линии электропитания и связи, что существенно сокращает время работы монтажной бригады на объекте.

Стоит остановиться на ещё одном преимуществе РИУС – это унификация технологических узлов. Разнообразие конструкций узлов одного типа ограничено заданными входными и выходными параметрами давления и производительности. Следовательно, имея ряд известных конструкций, различающихся основными параметрами, такими как давление, диаметр входного и выходного трубопроводов, число выходов и т.д., оснащённых необходимым количеством контролирующего и запорно-регулирующего оборудования с локальной системой автоматики, можно значительно ускорить проектирование и конструирование ГРС любого уровня сложности.

Работы в этом направлении в рамках НИОКР ведут специалисты завода «Газпроммаш», имея в планах внедрение подобной системы на одном из предприятий ПАО «Газпром». ●

**E-mail: victor-palgov@yandex.ru**





# Открытая системная архитектура для управления поездами

**Открытые стандарты несут массу выгод в различных областях автоматизации. Особо заметны они, когда речь идёт о проектировании надёжных и безопасных систем, в частности, автоматики для подвижны́х составов и путей сообщения железных дорог. На примере модульной платформы menTCS в статье рассказано о преимуществах подхода к конструированию систем для железнодорожного транспорта на основе предварительно сертифицированных стандартных блоков.**

Применение открытых стандартов для электронных систем управления в поездах позволяет сделать аппаратное и программное обеспечение независимыми от поставщика и, таким образом, даёт свободу выбора поставщиков и технических решений. Кроме того, открытые технологии помогают избежать возможных проблем с функциональной совместимостью и являются решающим фактором в предотвращении серьёзных проблем, вызванных старением, то есть гарантируют достаточно долгий жизненный цикл систем. Основная идея применения открытых отраслевых стандартов – вытеснение старых проприетарных систем, все ещё доминирующих на рынке железных дорог.

Внедрение в Европе ETCS (European Train Control System – Европейская система управления движением поездов) вкупе со стандартизированной системой передачи данных GSM-R (глобальная система мобильной связи на железных дорогах) должно положить конец пестроте технических реализаций систем управления поездами. Но даже здесь широта интерпретации спецификаций ETCS приводит к таким различиям в реализации у поставщиков, что цель трансграничной функциональной совместимости всё ещё не достигнута.

И здесь возникает проект openETCS, инициированный компанией Deutsche Bahn. Цель проекта openETCS – обеспечить стандартизованную среду разработки для моделирования, тестирования и валидации, а также упростить внедрение будущих систем ETCS.

В то время как ETCS и openETCS продвигают стандартизацию в отношении внедрения, программного обеспечения и коммуникаций, аппаратные средства разных поставщиков систем по-прежнему в основном остаются проприетарными, а значит, несовместимыми между собой.

Это приводит к тому, что компьютерные системы не только требуют высоких первоначальных затрат на разработку, но они также до́роги в эксплуатации в течение всего жизненного цикла. Операторы привязаны к поставщикам системы, а расширения или запасные части доступны только у одного поставщика.

Использование стандартных, открытых и предварительно сертифицированных компьютерных модулей поможет как поставщикам систем, так и операторам. Поставщики систем всё ещё могут оградить себя от конкуренции за счёт создания собственных систем и программного обеспечения, однако им больше не нужно будет заботиться о совместимости оборудования. При этом они могли бы ускорить выход своей продукции на рынок. А вот операторам (владельцам) систем это даст ещё больше преимуществ: они смогут приобретать запасные части и расширения системы у разных поставщиков, если те соответствуют стандарту. Таким образом, расходы на запасные части, а вместе с ними и общие затраты на жизненный цикл систем будут уменьшаться.

## Обязательность соблюдения стандартов

Итак, необходимо новое поколение критически важных для безопасности модульных систем управления и контроля, основанных на открытых отраслевых стандартах. Как и ранее созданные системы, они должны быть очень надёжными, рассчитанными на работу в течение многих лет в суровых условиях, характерных для железнодорожного сектора.

Как проектировать такие системы, частично описано, например, в стандарте EN 50155. Он предусматривает требуемую устойчивость к экстремальным температурам и быстрым её изменениям, вибрации, ударным нагрузкам и электромагнитным помехам, но этого недостаточно.

## Стандарты SIL

Системы, в которых ошибка или отказ могут нести опасность для жизни человека или для окружающей среды, или вызывать большие финансовые потери, должны соответствовать особым требованиям к функциональной безопасности. (SIL – Safety Integrity Level, или уровень полноты безопасности рассматривает опасные ситуации отказов, которые приводят к авариям, катастрофам и человеческим жертвам. – *Прим. пер.*). К таким системам относятся и компьютеризированные системы для безопасного управления поездами, которые должны соответствовать обширным международным требованиям безопасности EN 50128/IEC 62279 для программного обеспечения и EN 50129/IEC 62425 для аппаратного обеспечения.

Обеспечение доказательств соблюдения этих требований не является ни простой, ни быстрой задачей для производителя.

## Сертификация – «убийца проектов»

В новом проекте разработка необходимой документации на соответствие стандартам безопасности может удвоить или даже утроить финансовые затраты, а также продолжительность его выполнения. Соответствующие спецификации функциональной безопасности на железнодорожном рынке включают критерии RAMS (надёжность, доступность, управляемость, безопасность) EN 50126/EN 50128 для программного обеспечения и EN 50129 для аппаратного обеспечения. Все они требуют больших усилий по документированию, которые поставщики решений предпочитают свести к минимуму.

## Предварительная сертификация оборудования

Стратегическим ходом для значительного сокращения усилий по документированию является использование предварительно сертифицированного оборудования, поскольку оно в значительной степени основано на стандартизированных технологиях.

Таким образом, если предположить, что существует поставщик решений с конкретными знаниями о требованиях соответствия стандартам 501xx, можно было бы делегировать эту часть документации непосредственно поставщику.

Вследствие этого у вас появятся два преимущества: во-первых, это позволит снизить расходы на производство внутренней документации, во-вторых, это сэкономит драгоценное время, которое в конкурентной борьбе за самые инновационные решения является одним из наиболее важных факторов, – тот, кто первым выходит на рынок, имеет самые большие рыночные возможности, пользуется эксклюзивностью и может диктовать ключевые стандарты.

Внимание здесь должно быть сосредоточено на открытых и модульных системах: именно они позволяют реализовать гибкие конфигурации для различного использования в поездах или на железных дорогах. Заменяя лишь отдельные модули, а не полные системы, вы снижаете также затраты на техническое обслуживание, поэтому открытые стандарты, безусловно, являются существенным вспомогательным фактором и для поддержания уже сертифицированной системы в рабочем состоянии как можно дольше.

## CompactPCI – хорошее решение

Модульные платформы COTS, основанные на стандарте CompactPCI от PCI Industrial Manufacturing Group (PICMG), которые поддерживаются с 1997 года и специально спроектированы для разработки чрезвычайно прочных модульных конструкций с пассивными объединительными панелями, в целом соответствуют требованиям надёжности. Тем не менее, стандарт описывает только основные технологии и не включает в себя сертификацию и документацию, предусмотренные EN 50155 и EN 50126, EN 50128 и EN 50129. Несмотря на это от использования таких модульных COTS-платформ поставщики решений получают большую выгоду, поэтому существует необходимость распространить этот стандарт на железнодорожные технологии.

## Система управления menTCS: безопасность и стандартизация

Хорошим примером стандартизованного решения является новая модульная система контроля поездов menTCS, совместимая с EN 50155 и основанная на CompactPCI. Она предлагает все преимущества, которые имеют признанные отраслевые стандарты. Решение хорошо подходит для критически важных железнодорожных приложений и предварительно сертифицировано до SIL 4 в соответствии с EN 50126, EN 50128 и EN 50129. Благодаря своей модульной конструкции оно может быть адаптировано для любых типов применений. Например, в подвижном составе menTCS – отличное решение для автоматического управления поездом (ATO), автоматической защиты поезда (ATP) или точного управления поездом (PTC) и усиленного контроля поезда (ETC). В путевых приложениях оно может использоваться для управления сигналами и переключениями до уровня безопасности SIL 4 (рис. 1).

## Архитектура системы menTCS

Сердцем системы является центральный контроллер MH50C. Он обеспечивает основную логику управления в виде предварительно сертифицированной многопроцессорной платы на базе CompactPCI и может быть настроен на использование до 6 карт расширения в зависимости от требований приложения. Кроме того, доступно до 63 модульных ячеек ввода/вывода menTCS для подключения удалённых входов/выходов к центральному контроллеру. Это важно для установок в высокоскоростных поездах, где каждому пассажирскому вагону нужен свой блок ввода/вывода для подключения датчиков и приводов. Концепция модульного расширения также удобна для таких устройств, как системы сигнализации, где модули ввода/вывода menTCS могут использоваться для управления определёнными участками железной дороги по мере необходимости.

В этом случае устройства ввода/вывода menTCS подключаются через шину кольцевой топологии на основе Ethernet. Это не только упрощает соединение, но и значительно повышает надёжность, поскольку используется избыточный канал связи.

Компоненты модульной концепции семейства, сертифицируемые отдельно,


**Рис. 1. Сертифицированная система управления движением SIL 4 MEN основана на открытом стандарте CompactPCI**

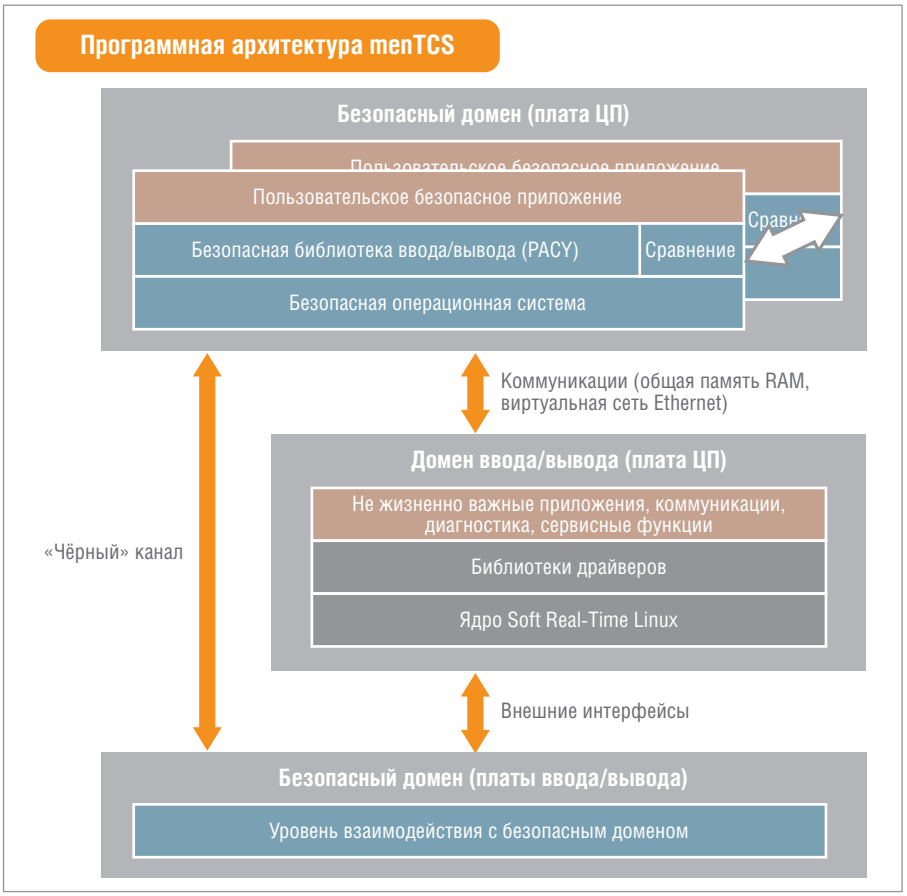



**Рис. 2. Платформа menTCS является первой в мире системой, не зависящей от конечного приложения**

при необходимости могут упростить разработку полностью сконфигурированных 19-дюймовых систем.

## Гибкость расширения и интерфейсов

Модульная концепция ввода/вывода стандартизованной архитектуры menTCS обеспечивает разработчикам большую гибкость и позволяет им посредством карт стандарта CompactPCI легко оснастить контроллер и удалённые блоки ввода/вывода коммуникационными интерфейсами. Для подключения к сети TCN можно использовать интерфейсные платы MVB. Дополнительные бортовые компоненты и блоки управления могут быть подключены через RS-485, CAN, ProfiNet и другие полевые шины. Для подключения IoT доступны WLAN, GSM-R, GPS, GLONASS или Galileo, а также возможна работа через стандартные маршрутизаторы и коммутаторы Ethernet.

## Масштабируемая безопасность

Поскольку все критически важные для безопасности модули menTCS предварительно сертифицированы на самый высокий уровень безопасности SIL 4 в соответствии с EN 50128 и EN 50129, они отвечают всем требованиям, которые могут возникать в критически важных для железных дорог приложениях, от SIL 2 для систем ATO до SIL 4 для сигнализации. Это позволяет разработчикам сосредоточиться исключительно на программном обеспечении, избавляя от забот об аппаратной части. В зависимости от конечного приложения уровень безопасности оборудования может быть определён в любое время и без дополнительных инженерных усилий.

## Безопасные домены упрощают разработку программного обеспечения

Аппаратная платформа menTCS разработана таким образом, что программное обеспечение для управления безопасностью строго изолировано от периферийного программного обеспечения, не относящегося к сертификации. Это достигается благодаря выполнению критически важных функций управления в отдельных безопасных доменах. Тем самым обеспечивается их обособленность от общих некритических функций ввода/вывода. Эта изоляция выполняется как на аппаратном, так и на программном уровне. Благодаря такому строгому разделению более сложное и критически важное для безопасности программирование ограничивается исключительно безопасными доменами, что облегчает разработку программного обеспечения, а также упрощает и ускоряет сертификацию по SIL. В дополнение к сокращению объёмов аппаратной документации это второй важный фактор, способствующий значительной экономии средств во внутренних разработках (рис. 2).

## Высокопроизводительные контроллеры уровня SIL 4

В основе контроллера menTCS MH50C лежит процессорная плата F75P CompactPCI PlusIO SBC, сертифицированная по SIL 4. Это одноплатный компьютер, объединяющий три процессора Intel Atom E680T. Два процессора в нём выполняют критически важные функции управления. Они связаны с PCIe через FPGA (ПЛИС – программируемая логическая интегральная схема), которая обеспечивает синхронизацию контрольных точек приложения с SIL 4 для требуемой избыточности 2oo2 (2 out of 2 voting – мажоритарная схема 2 из 2). Третий процессор отвечает за общий ввод/вывод. Благодаря широкой распространённости и многолетнему рыночному опыту работы с этими процессорами все известные критически важные ошибки уже известны и документированы. Поэтому, если соблюдаются известные правила проектирования плат, систематические ошибки, которые могут повлиять на поведение безопасности, исключаются.

## Безопасный домен с QNX Neutrino

Для исполнения критически важных приложений контроллер menTCS MH50C имеет предустановленную операционную систему реального времени QNX Neutrino, специально адаптированную к интегрированному оборудованию. По сравнению с проприетарными операционными системами эта интеграция сама по себе экономит разработчикам и OEM-производителям около двух миллионов евро в расходах по проекту и позволяет им избежать всех рисков, связанных с сертификацией. Пакет поддержки платы для разработок под QNX Neutrino также является сертифицированным по SIL 4 на платформе menTCS и, следовательно, с самого начала обеспечивает наивысшую степень надёжности.

QNX Neutrino использует микроядерную архитектуру, которая строго изоли-

ADVANTIX
ПРОМЫШЛЕННЫЕ СИСТЕМЫ

Технологии надёжности

# CompactPCI ▪ Компьютеры специального назначения

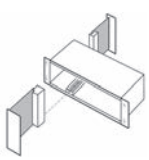
**Блочные каркасы** с различными механическими характеристиками, в том числе с ударопрочностью до **25g**

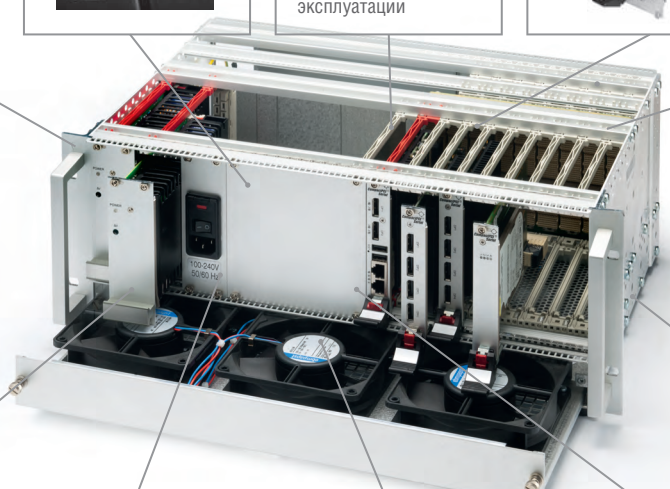
Эффективное электромагнитное **экранирование**

**Процессорные модули** PICMG 2.0, 2.16, 2.30; CPCI-S.0 (Serial) на различных процессорных платформах AMD и Intel для работы в жёстких условиях эксплуатации

**Кросс-платы и модули расширения** PICMG 2.0, 2.16, 2.30, CPCI-S.0 (Serial)

Подключение модулей **тыльного ввода-вывода**





**Источники питания** одинарные или резервированные: встраиваемые или в виде сменных блоков

**Панели ввода** с клеммами заземления и разъёмами питания разных типов

**Вентиляторы** с возможностью «горячей» замены. Система охлаждения, в том числе с кондуктивным отводом тепла

**Лицевые панели** универсальные и заказные для вставных блоков

**Различные габариты** и варианты компоновки

рует программные процессы, что не позволяет им взаимно влиять на производительность и поведение друг друга. Это, в свою очередь, гарантирует, что система всегда остаётся в безопасном состоянии, поскольку даже вредоносные программы не могут влиять на критически важные для безопасности процессы. Кроме того, QNX Neutrino поддерживает разделение и гибкую настройку использования ресурсов процессора. Критически важные для безопасности приложения могут быть запрограммированы на языках C или Ada, а также на основе платформы SCADE или Soft PLC (программно реализованный ПЛК). Разработчики могут использовать знакомую среду разработки, что сводит к минимуму дорогостоящую повторную сертификацию. По запросу доступны и другие операционные системы, такие как INTEGRITY от Green Hills, PikeOS от Sysgo или VxWorks от Wind River.

## Унифицированный ввод/вывод

Чтобы упростить обработку ввода/вывода в безопасном домене, компания MEN Mikro Elektronik интегрировала инфраструктуру ввода/вывода PACY (PACY – безопасная среда для приложений и данных, абстрагирующая их от аппаратной платформы) в безопасный домен, что обеспечивает прозрачный уровень абстракции между безопасным доменом и доменом ввода/вывода. Это означает, что идентичные функции в одном домене всегда адресуются одинаково и становятся независимыми от аппаратной реализации входов и выходов. Для PACY не имеет значения, обращается ли команда к реле или к цифровому вводу/выводу. Это делает интеграцию menTCS гораздо более простой и гибкой. Системы для поездов и путей с различными датчиками и исполнительными механизмами для реализации одинаковых функций теперь можно оснащать идентичными системами управления, значительно упрощающими модернизацию.

Среда PACY реализована как структура на модульной основе, что обеспечивает гибкое расширение с помощью отдельных клиентских модулей, а также связывание с любым C-приложением. В будущем разработчики смогут определять функциональные блоки PACY, объединяющие несколько задач в одну макрокоманду. Таким образом, часто используемые процессы, такие как функция экстренного торможения, могут быть просто активированы как стандартные процедуры без необходимости программировать их в каждом случае. Связь между безопасным управлением и безопасным торможением осуществляется посредством домена ввода/вывода (рис. 3).

## Домен ввода/вывода с Linux

Поскольку третий процессор Intel Atom обрабатывает аппаратный ввод/вывод совершенно отдельно от безопасного домена, гарантируется, что домен ввода/вывода никогда не будет влиять на логику безопасного управления. MEN Mikro Elektronik использует для данной цели интегрированную и предварительно сертифицированную ОС Linux. Это даёт клиентам доступ к полностью развитой и проверенной экосистеме с готовыми инструментами и драйверами, доступными для использования «из коробки». Дополнительная ОС предоставляется по запросу.

Связь между безопасной системой и картами ввода/вывода контроллеров

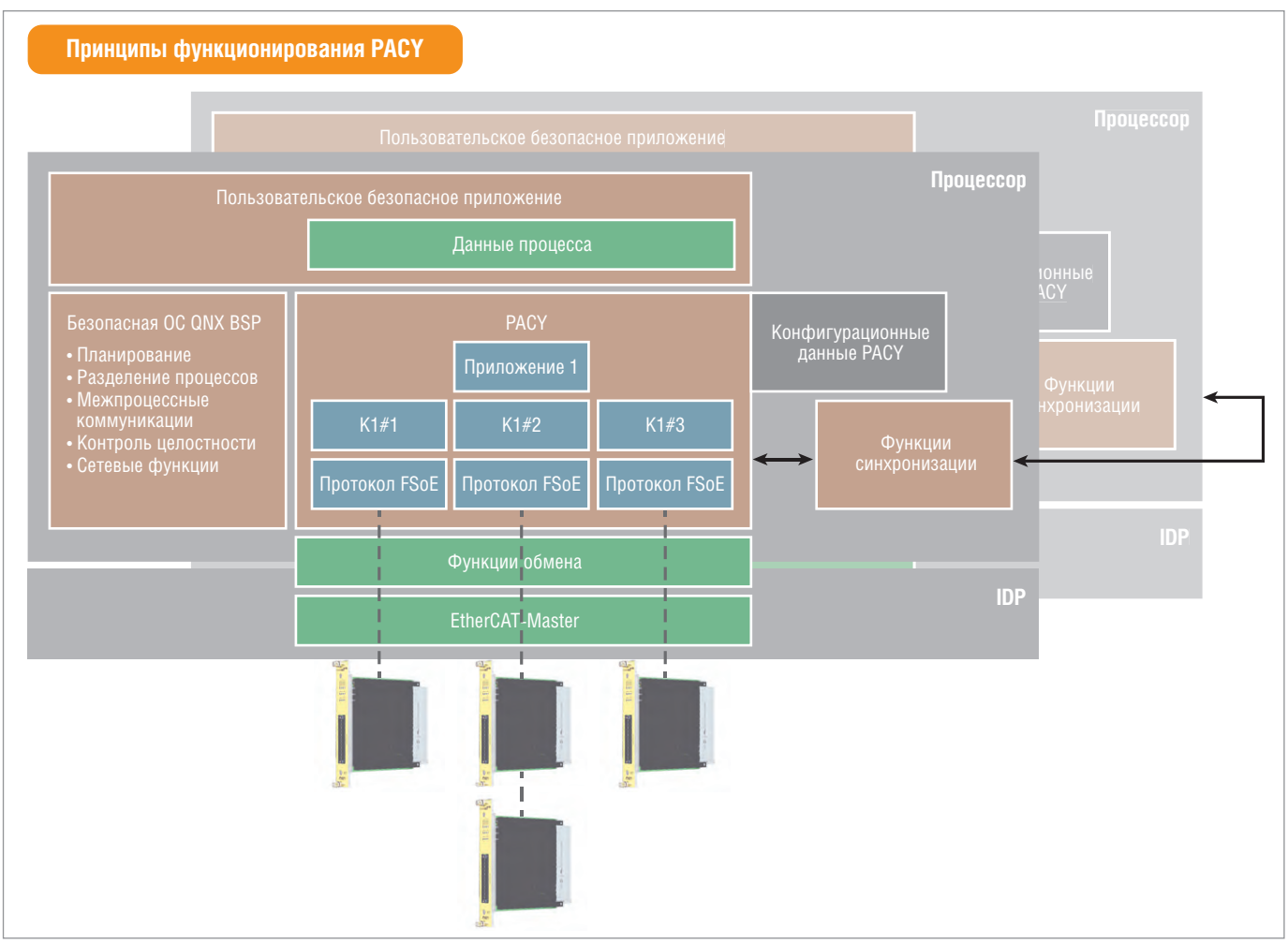



**Рис. 3. Структура безопасного ввода/вывода PACY**

menTCS, а также модулями ввода/вывода реализована по протоколу EtherCAT. EtherCAT – это Ethernet-стандарт реального времени с гарантированными циклами реального времени менее 5 миллисекунд, отвечающий всем требованиям безопасной связи с компонентами menTCS. EtherCAT не требует коммутаторов, поскольку он поддерживает кольцевую топологию с резервированием каналов связи. Для надёжного обнаружения изменённых, дублированных или потерянных пакетов данных в EtherCAT используется протокол функциональной безопасности FSoE (Fail Safe over EtherCAT). Таким образом, весь канал связи ввода/вывода функционирует как «чёрный» канал, обеспечивая необходимую функциональную безопасность связи.

## Вывод: не бойтесь готовых систем

Платформа menTCS хорошо подходит для всех критически важных железнодорожных применений и демонстрирует возможности и преимущества систем управления поездом, основанных на открытых стандартах.

Она предлагает операторам поездов и путей, а также сторонним поставщикам решений автоматизации много преимуществ, которые сегодня являются уникальными на рынке Smart Railways. Крупные OEM-производители, в настоящее время доминирующие на рынке SIL-сертифицированных приложений, как и более мелкие компании, будут только в выигрыше от использования инновационной платформы menTCS, позволяющей быстро создавать IoT-совместимые приложения и интеллектуальные железнодорожные решения.

Таким образом, предлагаемое аппаратное обеспечение является хорошей альтернативой для построения стандартизованных систем управления ETCS. ●

**Перевод Юрия Широкова**
**E-mail: textoed@gmail.com**

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

## Аддитивное производство – важный компонент Industry 4.0

Аддитивное производство (*Additive Manufacturing, AM*) – общее название всех технологических процессов, которые позволяют создавать трёхмерные объекты, добавляя слой за слоем материал: пластик, металл, бетон, в будущем даже человеческую ткань.

Общим для всех AM-технологий является использование цифровой 3D-модели из программы автоматизированного проектирования (САПР), специального оборудования и наслаиваемого материала. Как только схема готова, оборудование AM считывает данные из архива САПР и спекает или последовательно добавляет слои жидкости, порошка или листового материала, послойно изготавливая 3D-объект.

Сфера применения технологии *Additive Manufacturing* безгранична. Первоначально она использовалась для ускоренного создания опытных образцов (визуализации прототипов), и в настоящее время она применяется для изготовления готовых деталей в авиастроении, стоматологии, имплантологии, автомобилестроении и даже при создании коллекций prêt-à-porter.

В то время как принцип послойного добавления материала достаточно прост, его практическая реализация зависит от того, где технология применяется:

- в качестве инструмента визуализации в дизайне;
- как средство для создания персонализированных продуктов потребительского класса;
- в промышленном производстве;
- для производства небольших партий деталей;
- для производства органов человека в недалёком будущем.

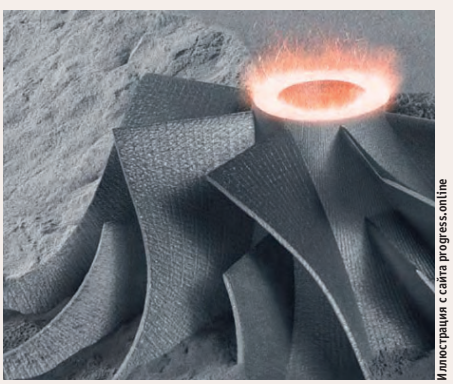


Иллюстрация с сайта progress.online

В некоторых случаях AM понимается как дополнительный компонент субтрактивного процесса (удаление материала, высверливание, фрезеровка) и в меньшей степени в качестве формирующего (ковка, штамповка). В общем, аддитивное производство может предложить профессионалам и потребителям среду создания, моделирования и/или ремонта любого продукта и в процессе своего развития переопределит ныне действующую модель производства.

Аддитивные технологии изменят мир так же, как изменил в своё время Интернет, возможно, спектр их применения выходит далеко за пределы существующих потребностей человека. ●

*По материалам valve-industry.ru*

## Информационная граница на замке: начались поставки компьютеров AdvantiX со специальной проверкой

Компания «Адвантикс» – ведущий отечественный производитель электроники для ответственных применений – объявляет о новой возможности для заказчиков – купить компьютерное оборудование **AdvantiX**, прошедшее специальную проверку и специальное исследование.

Приобретение компьютера государственными органами или учреждениями, работающими с секретной информацией, иногда требует особого подхода. В определённых случаях этим структурам необходимо иметь стопроцентную гарантию того, что процесс обработки данных исключает их утечку.

Для обеспечения уверенности заказчика в отсутствии «прослушивающих закладок» в электронном оборудовании компания начала продажу своих изделий в комплексе с услугами *«Специальная проверка» (СП)* и *«Специальное исследование»* (СИ).

Спецпроверка и специсследование компьютера могут быть необходимы организации, если в её информационном потоке присутствуют персональные данные и конфиденциальные сведения. А в случае обработки информации, содержащей служебную или государственную тайну, проведение СП и СИ обязательно.

Спецпроверка позволяет обнаружить внутри оборудования устройства для скрытого считывания информации или подтвердить их отсутствие. Часто такие устройства называют «жучками».

Специсследование оборудования проводят для измерения радиуса распространения электромагнитного излучения, в котором возможно несанкционированное считывание информации, а также для определения необходимых мер по предотвращению хищения данных.

Подводя итог, отметим, что купив компьютер AdvantiX и дополнительные услуги по его проверке, заказчики из государственных структур смогут получить не только желаемую технику, но и уверенность в её безопасности, подкреплённую соответствующими документами от компетентных органов. ●

# Аппаратно-программный комплекс ХОРК.Метео-ЭФ для испытательного климатического стенда

Алексей Бурханов

**В статье приводится описание типового построения испытательного климатического оборудования, рассматриваются особенности климатических камер для моделирования воздействия повышенной температуры рабочей среды и повышенной относительной влажности. Описывается климатическое оборудование на базе контроллеров линейки FASTWEL I/O, предназначенное для проведения испытаний бытовых холодильных приборов на соответствие стандартам энергоэффективности.**

## Испытательное климатическое оборудование

Испытательное климатическое оборудование (ИКО) применяется для моделирования агрессивных факторов среды и определения воздействия этих факторов на образцы материалов и изделий в самых различных направлениях производства. Как правило, в нашей стране основными заказчиками испытательного климатического оборудования являются предприятия оборонно-промышленного комплекса, в то время как в Европе такое оборудование используется на всех общепромышленных предприятиях.

По моделирующим факторам ИКО делится на оборудование для испытаний на воздействие повышенных и пониженных рабочих температур среды, относительной влажности, пониженного и повышенного атмосферного давления, на статическое и динамическое воздействие песка и пыли, на воздействие морского (соляного) тумана, выпадающих осадков (дождя), конденсируемых осадков (инея, росы) и солнечного излучения.

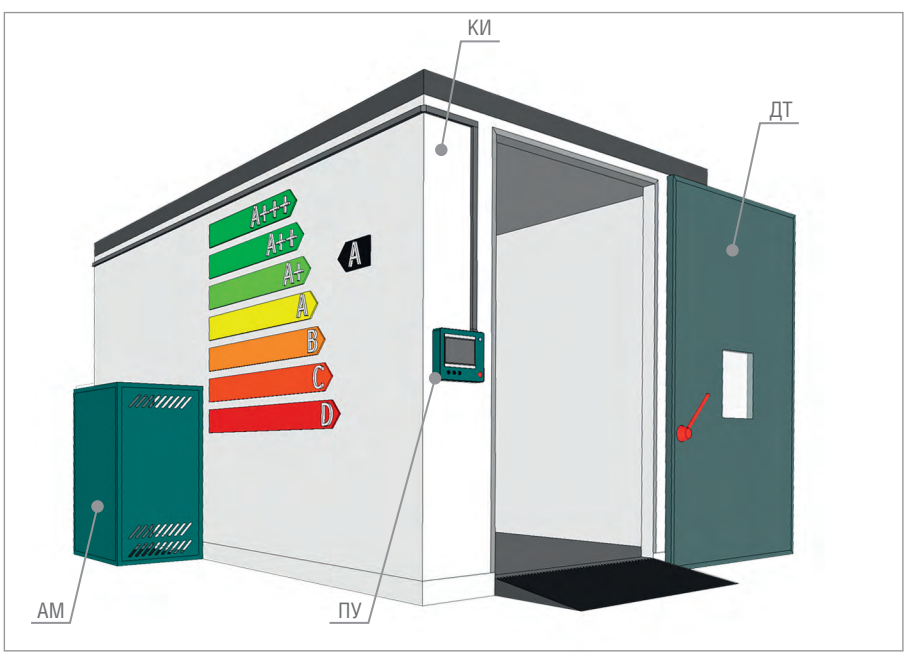
Типовой единицей такого оборудования является климатическая камера. Различают климатические камеры цельнокорпусные и сборные. Конструктивно камеры состоят из испытательного объёма, аппаратного модуля и системы управления. Испытательные стенды включают в себя специализированные климатические камеры и представляют собой совокупность аппаратных и программных средств для проведения профильных испытаний (рис. 1).

## Испытания на энергоэффективность

Проект «А-класс – норма жизни» инициирован проектом Минобрнауки России/ПРООН (Программы развития ООН) – ГЭФ (Глобального экологического фонда) «Стандарты и маркировка для продвижения энергоэффективности».

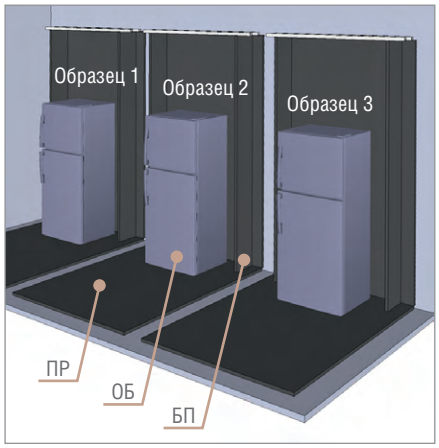
Программа предполагает оснащение ряда крупных региональных центров стандартизации и метрологии оборудованием для проведения испытаний на энергоэффективность бытовых холодильных приборов по ГОСТ IEC 62552-2013.

По техническому заданию требовалось разработать и изготовить инфор-




**Условные обозначения:** КИ – камера испытательная; ДТ – дверь; АМ – модуль аппаратный; ПУ – пульт управления.

**Рис. 1. Испытательный климатический стенд**




**Условные обозначения:** ПР – платформа; ОБ – образец; БП – перегородка.

**Рис. 2. Размещение образцов**

**Рис. 3. Шкаф с оборудованием информационно-измерительной системы**


**Рис. 4. Аппаратная спецификация системы управления**

мационно-измерительную систему, состоящую из испытательной климатической камеры, рабочего места оператора, средств измерений и специального ПО.

## Испытательная камера

Для моделирования климатических условий при испытаниях изготовлена климатическая камера тепла и влажности, позволяющая реализовать внутри неё температурные режимы +10...+43°C при относительной влажности 40...95% с испытательным объёмом, пригодным для размещения трёх платформ с холодильниками в соответствии ГОСТ IEC 62552-2013 (рис. 2).

Основными исполнительными механизмами в камере являются высокотемпературная холодильная машина, пароувлажнитель, блок электронагревательных устройств и вентиляторы.

Холодильная машина имеет в своём составе компрессор и набор соленоидных клапанов для управления холодопроизводительностью.

В качестве пароувлажнителя установлен модульный пароувлажнитель с цифровым программным управлением и подключением по сети RS-485.

Нагревательное устройство представляет собой малоинерционный нихромовый нагреватель.

Вентиляторы климатической камеры оснащены приводами с частотным управлением.

В качестве измерительного преобразователя установлен цифровой датчик температуры и относительной влажности, имеющий высокую точность.

## Система управления

Система управления спроектирована непосредственно для установки на климатическую камеру в составе информационно-измерительной системы (рис. 3). Для обеспечения высокой точности поддержания параметров режима – температуры и относительной влажности – в испытательном объёме в качестве приборов управления были использованы приборы из линейки FASTWEL I/O.

В качестве контроллера была использована модель CMP713 – контроллер узла сети Modbus TCP с установленной подсистемой CODESYS. Также установлен типовой набор модулей для ввода-вывода дискретных сигналов +24 В (рис. 4).

Для ввода универсальных сигналов 4...20 мА от преобразователя температуры и влажности используется четырёхканальный модуль аналогового ввода сигналов постоянного тока 4...20 мА AIM723.

Для ввода сигналов термосопротивлений установлен модуль аналогового ввода сигналов термометров сопротивления AIM725. Оба модуля у производителя представлены в двух версиях, отличающихся точностью измерений (по сути – разрядностью и быстродействием АЦП). Для обеспечения связи контроллера с приборами по сети RS-485 установлен интерфейсный модуль NIM745.

Отличительной особенностью приборов из линейки FASTWEL I/O является наличие внутреннего интерфейса – скоростной шины FBUS.

Структурная схема системы управления представлена на рис. 5.

Для реализации человеко-машинного интерфейса использована цветная сенсорная панель оператора Weintek MT8100iE. Сопряжение с контроллером осуществляется по протоколу Modbus TCP через неуправляемый 5-портовый коммутатор MOXA EDS-205. Организация сети представлена на рис. 6.

Панель управления выполнена модульной на кронштейне. На ней уста-


**Рис. 5. Структурная схема системы управления**

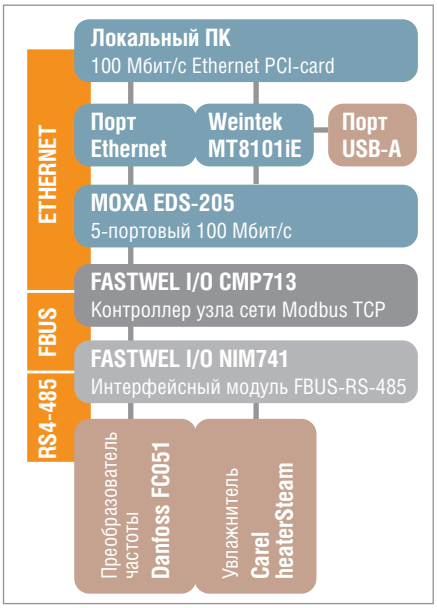
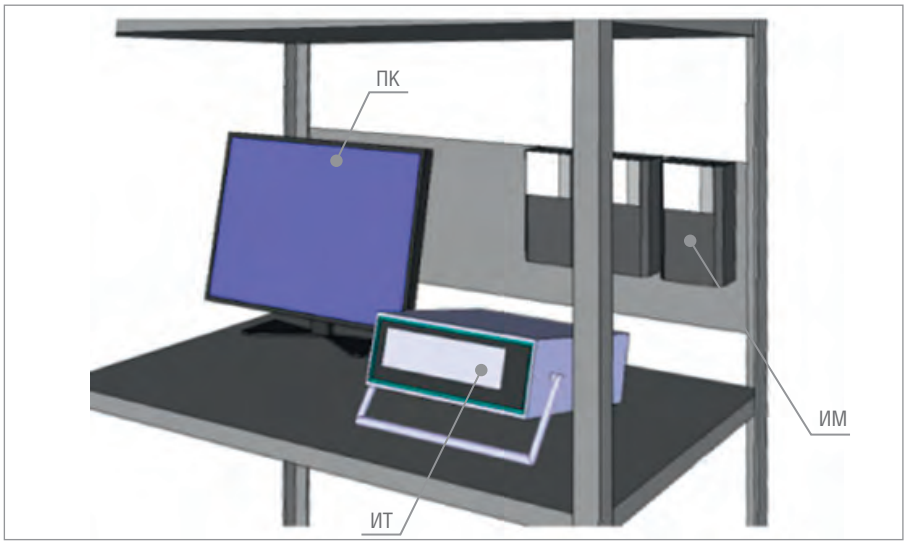



Рис. 6. Организация сети




**Условные обозначения:** ПК – настольный компьютер; ИТ – измеритель температуры; ИМ – измеритель мощности.

Рис. 7. Компоновка АРМ

новлены переключатель вкл./выкл., панель оператора, интерфейсные разъёмы для подключения к сети Ethernet и USB.

Интерфейс Ethernet используется для подключения системы управления климатической камеры к настольному ПК из состава автоматизированного рабочего места оператора.

Порт USB предназначен для подключения USB флэш-диска для экспорта значений результатов испытаний.

## Особенности алгоритма управления режимами работы климатической камеры

В климатической камере требуется непрерывно поддерживать параметры микроклимата – температуру и относительную влажность. Сложность заключается в большой инерционности исполнительных механизмов при охлаждении, нагреве, осушке и увлажнении. Кроме того, температура и относительная влажность являются связанными параметрами. Необходимо, чтобы регуляторы были настроены максимально точно, с учётом инерционности механизмов и запаздывания при измерении мгновенных значений параметров.

Для решения такой задачи контроллер линейки FASTWEL I/O подходит наилучшим образом. Он обеспечивает высокоскоростной обмен между модулями по внутренней шине FBUS, быстрый опрос измерительных преобразователей и максимально быстрый цикл выполнения программы подсистемой CODESYS. CODESYS снижает быстродействие системы управления, но является эффективным решением, позволяющим максимально быстро реализовать сложный алгоритм управления, используя языки стандарта МЭК 61131-3.

## Автоматизированное рабочее место оператора

В состав информационно-измерительного комплекса входит автоматизированное рабочее место оператора, имеющее в своём составе настольный ПК, принтер, стойку для подключения бытовых холодильных приборов, три прецизионных многоканальных измерителя температуры МИТ-8.10М1 производства ЗАО «ИзТех», три многофункциональных измерителя активной и реактивной мощности A1802RLXQ-P4G-DW-4 производства ELSTER.

Указанные приборы подключаются к настольному ПК по последовательной шине USB, при этом для сопряжения измерителей мощности используется стандартный конвертер RS-232/USB.

Компоновка рабочего места оператора представлена на рис. 7.

## Функциональные возможности комплекса при проведении испытаний бытовых холодильных приборов по ГОСТ IEC 62552-2013

Образцы для испытаний устанавливаются на специальные платформы, размещённые в испытательном объёме. На платформах и боковых перегородках закрепляются датчики температуры согласно методике и программе испытаний.

Далее с панели управления или с настольного ПК задаются параметры режима, и камера запускается на исполнение программы. В настройках программы задаются временны́е таймеры, реализующие возможность подачи электропитания на образцы при достижении градиентом распределения температуры и относительной влажности требуемых значений в испытательном объёме климатической камеры. Климатическая камера в совокупности с системой управления имеет высокие параметры точности поддержания температуры, относительной влажности и градиента распределения этих параметров в испытательном объёме, согласно ГОСТ IEC 62552-2013 точность поддержания температуры в контрольной точке составляет ±0,5°С и относительной влажности ±1,0%. Линейный градиент температуры должен быть не хуже ±1,0°С/м, относительной влажности ±2,0%/м.

Интерфейс специального ПО на ПК позволяет задать уставки температуры и влажности, по достижении которых автоматически подаётся напряжение питания на образцы. Для приближения условий испытаний образцов к эталонным питание осуществляется от стабилизированных источников питания.

Одновременно происходит запись показаний двенадцати контрольных датчиков температуры, закреплённых на платформе и боковых стенках.

Запись показаний измерителей мощности осуществляется с привязкой ко времени испытаний. Временны́е интервалы записи измерений (дискретность) доступны к изменению в настройках программы.

Таким образом, оператор комплекса получает возможность работать в еди-

ной информационно-измерительной системе, позволяющей непрерывно отслеживать и записывать архив испытаний, содержащий значения параметров режима испытаний, контрольных температурных датчиков, параметров питающей сети и потребляемой полной мощности образцов. Также оператору доступны функции работы с архивом – различные выборки, построение графиков и гистограмм в любом табличном редакторе. Настройки специального ПО позволяют расставлять временны́е метки, настраивать таймеры, а также настраивать уведомления по электронной почте и SMS.

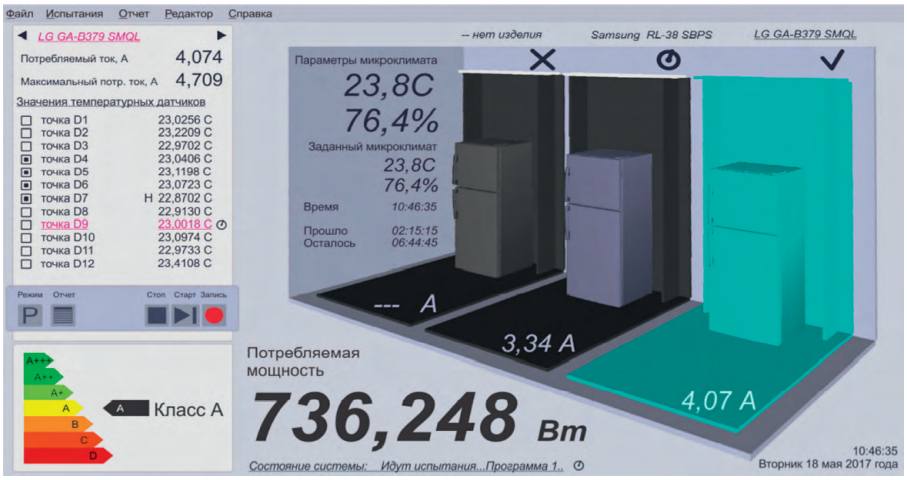



**Рис. 8. Основная экранная форма программы из состава СПО**

## Специальное ПО из состава комплекса

Специальное программное обеспечение для ПК разработано на языке C++ с использованием дополнительных библиотек. Специальное ПО позволяет считывать значения измерителей температуры и измерителей мощности.

Основная экранная форма программы представлена на рис. 8.

## Зелёные технологии

Оснащение региональных центров стандартизации и метрологии информационно-измерительными комплексами, описанными в настоящей статье, позволяет выполнять проверку образцов бытовых холодильных приборов на соответствие стандартам и классам энергоэффективности.

Специальное ПО из состава аппаратно-программного комплекса ХОРК.Метео-ЭФ позволяет автоматизировать процесс проведения испытаний, систематизировать полученные результаты для последующей обработки и внесения изменений в конструкцию и устройство бытовых холодильных приборов.

Использование бытовых приборов и техники с высокими классами энергоэффективности позволит значительно сократить выбросы углекислого газа и энергопотребление.

ООО «ХОРК» в своей работе в части проектирования, производства и эксплуатации оборудования всегда идёт курсом на повышение эффективности расходуемых ресурсов. Только бережное отношение к ресурсам сегодня поможет сохранить Землю для человека завтрашнего дня. ●

**E-mail: burhanov@hork.ru**

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

## Panasonic использует AR-очки, искусственный интеллект и IoT в ресторанах будущего

AR-очки, искусственный интеллект и Интернет вещей будут широко использоваться в ресторанах будущего – такой смелый прогноз сделали японская корпорация Panasonic и её инкубатор идей Game Changer Catapult. Стороны даже представили прототип решения Kronosys, сочетающего все указанные технологии, на выставке SXSW 2018 в США.

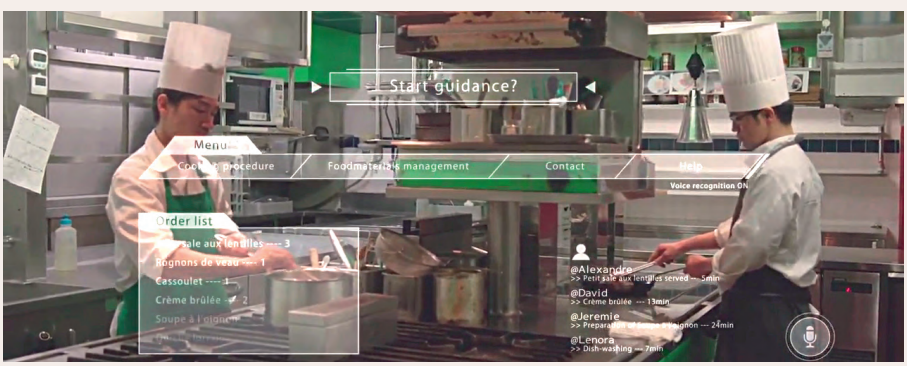
В чём кроется главная проблема современного общепита? В высокой текучести кадров. Многие начинающие повара не выдерживают сложностей адаптации в новом коллективе, жёсткого ритма работы, поздних часов работы, отсутствия поддержки от более профессиональных коллег. Новым людям нужны тренинги, на которые у шеф-поваров и руководства нет ни времени, ни возможностей.

Panasonic и Game Changer Catapult предлагают использовать технологии дополненной реальности (AR-очки), систему распознавания голоса, облачные технологии (для хранения и обработки информации), а также искусственный интеллект, чтобы организовать систему удалённой поддержки молодых поваров. А дополнив решение IoT-совместимой бытовой техникой, камерами с технологией распознавания лиц, POS-терминалами и подключив всё это к системе управления поставками, можно создать по-настоящему умный ресторан будущего.

Процесс использования Kronosys прост. Надев очки, пользователь сразу попадает в основной интерфейс, из которого с помощью голосовых команд открывается доступ к текстовому и видеоконтенту по приготовлению конкретных блюд и другим командам. Здесь же можно увидеть список необходимых продуктов и их наличие на кухне.

Сама форма AR-очков буквально освобождает руки повара. Возможности удалённого обмена аудио и видео позволяют одному тьютору поддерживать сразу несколько молодых сотрудников в разных ресторанах. Кроме того, с помощью очков можно общаться с бэк-офисом. Благодаря функции распознавания речи и возможностям перевода с/на многие языки AR-очки подойдут людям с разным культурным и профессиональным уровнем и помогут вывести их на передовую кулинарного фронта в максимально сжатые сроки.

Данные от каждого носителя очков могут передаваться и аккумулироваться в облаке. Функция дата-логов позволит лучше понимать поведение людей и управлять закупками, повышая общую эффективность предприятия. ●



# AU Optronics: технологии лидеров

*Алексей Лебедев*

**В статье рассказано о дисплейных решениях компании AU Optronics, раскрыты некоторые технологические особенности модельного ряда. Сделан обзор применений ЖК-дисплеев. Описана также деятельность AU Optronics в сфере «зелёной» энергии.**

## Кратко о компании AU Optronics

Компания AU Optronics (AUO) была образована в сентябре 2001 года путём слияния двух фирм – Acer Display Technology и Unipac Optoelectronics Corporation. Позднее (в октябре 2006 года) AUO приобрела компанию Quanta Display Inc, усилив свои позиции на рынке производителей дисплеев.

С 2005 года AUO входит в тройку ведущих производителей ЖК-дисплеев (вместе с LG-Display и Samsung) и на сегодняшний день насчитывает более 43 000 сотрудников, имеет филиалы и представительства в Тайване, Китае, Японии, Сингапуре, Южной Корее, США и Европе.

AUO стремится сохранить лидерство в технологиях отображения информации благодаря непрерывному технологическому прогрессу своей продукции. Три ядра технологий отображения: a-Si, LTPS и AMOLED – позволяют создать прекрасное качество изображения, стильный внешний вид и интегрированные решения и тем самым удовлетворяют самым разнообразным требованиям рынка.

Технологии, разработанные AUO для обеспечения наилучшего качества изображения, включают ультравысокое разрешение, широкую цветовую гамму, высокий динамический диапазон HDR (High Dynamic Range Imaging – коррекция освещённости изображения с целью получения более высокой пиковой яркости и большей темноты там, где света не должно быть), сверхвысокую частоту обновления и яркость. AUO также активно развивает изогнутые и сверхтонкие формы дисплеев с узкими рамками, которые обеспечивают людям более качественное визуальное восприятие изображения.

У AUO есть более 10 фабрик, на которых производится полная линейка дисплеев для самых разнообразных применений. Видеорешения включают в себя дисплеи для ЖК-телевизоров, настольных мониторов и информационных дисплеев (PID – Public Information Display). Мобильные решения охватывают дисплеи для ноутбуков, планшетов и смартфонов, обычные дисплеи, а также дисплеи для использования в автомобилях, в аудио- и видеосистемах и в носимых устройствах.

## Дисплейные решения AUO

**a-Si-панели** – активная ЖК-матрица, выполненная по технологии TFT (Thin Film Transistor – тонкоплёночный транзистор) на основе аморфного кремния. Эта технология весьма старая и не подразумевает изготовление дисплеев больших разрешений, но до сих пор актуальна ввиду равномерного распределения яркости по длине и ширине матрицы.

Как показано на рис. 1, TFT-дисплей состоит из цветового фильтра, массива тонкоплёночных транзисторов и модуля подсветки.

В TFT-дисплее молекулы жидких кристаллов вводятся между двумя про-

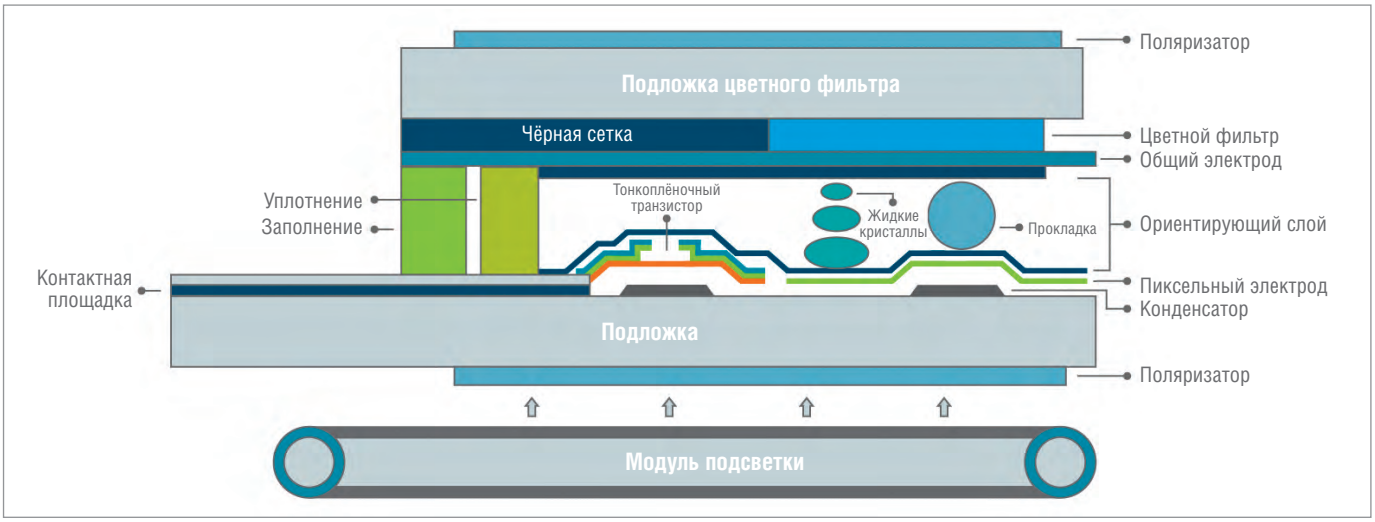



**Рис. 1. Сечение TFT-дисплея**

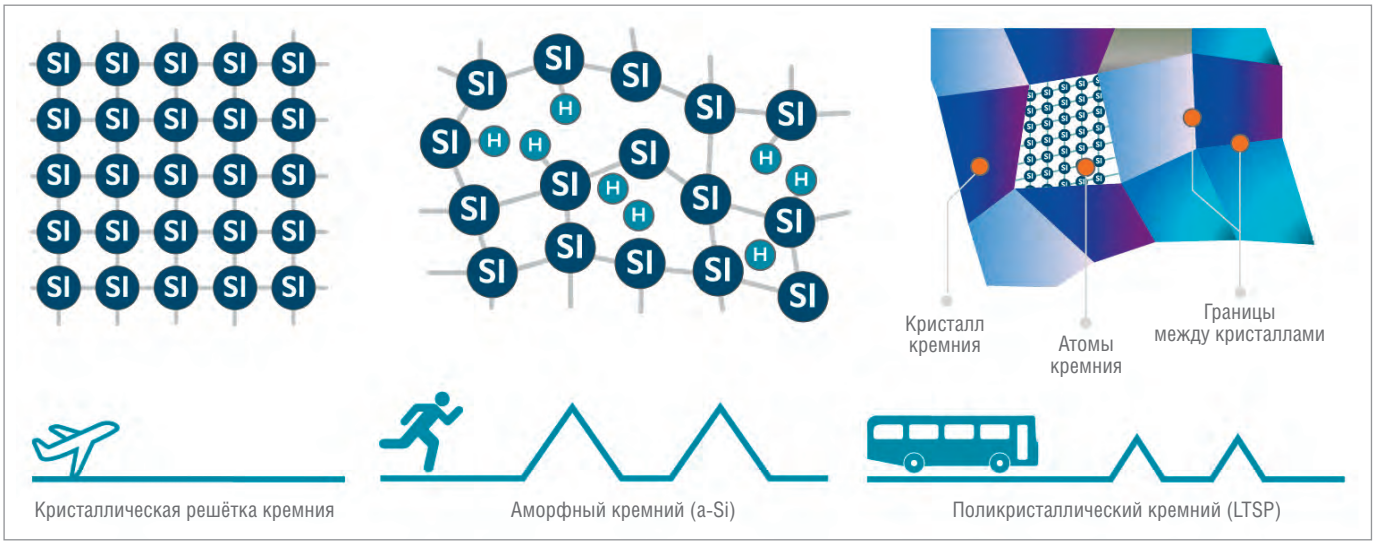



**Рис. 2. Структуры кремния и сравнение подвижности электронов**

зрачными электродами. Свет от модуля подсветки проходит через поляризатор и попадает в слой жидких кристаллов. TFT-транзистор создаёт электрическое поле в слое жидких кристаллов (его интенсивность регулируется напряжением, приложенным к пиксельному электроду), которое меняет ориентацию жидких кристаллов и тем самым создаёт оттенки серого света от полной яркости до полной темноты.

Каждый пиксель состоит из трёх субпикселей красного, зелёного и голубого цветов. Субпиксели располагаются вплотную, но не сливаются, так как между ними находится непрозрачная чёрная сетка. Для получения разных цветов свет, генерируемый модулем подсветки, пропускается через жидкие кристаллы, и в сочетании с определённым уровнем серого получается нужный цветовой эффект.

После создания матрицы TFT-транзисторов и подложки цветного фильтра жидкие кристаллы вводятся между ними, затем эти два слоя ламинируют и присоединяют поляризатор.

Окончательный процесс создания ЖК-дисплея состоит из процесса подключения IC (Integrated Circuit) и PCBA (Printed Circuit Board Assembly) – управляющего драйвера и платы управления – к стеклянной подложке с последующей сборкой модуля подсветки.

**LTPS-процесс** (Low Temperature Polysilicon – низкотемпературная поликремниевая технология) представляет собой современную технологию изготовления TFT ЖК-дисплеев на основе поликристаллического кремния, который состоит из многочисленных кристаллов кремния размером от 0,1 до нескольких микрон.

В полупроводниковой промышленности поликремний обычно образуется методом химического осаждения (создание плёнки) при низком давлении из газообразной фазы с последующим отжигом при температурах свыше +900°C. Этот метод известен как SPC (твердофазная кристаллизация). Однако стекло начинает искажаться (плавиться) при +650°C, поэтому метод SPC не подходит для изготовления плоских дисплеев.

LTPS – это технология поликремниевого покрытия, предназначенная для производства плоских ЖК-дисплеев. На сегодняшний день используют разные способы получения LTPS-структур. Чаще всего применяют метод металлоиндуцированной кристаллизации (MIC – Metal-Induced Crystallization), метод каталитического осаждения паров химическим способом (Catalytic CVD) и метод лазерного отжига.

Суть метода MIC заключается в изменении технологии SPS путём предварительной металлизации плёнки поликремния. Это даёт возможность выполнить отжиг на более низких температурах (не более +600°C).

Химический метод Catalytic CVD позволяет избавиться от финального отжига. Сочетание паров газов ($SiH_4$, $H_2$) и катализаторов (W, Ta) позволяет получить LTPS-плёнку при температуре не более +300°C.

Лазерный отжиг – наиболее часто встречающийся способ в настоящее время. С помощью эксимерного лазера нагревают и расплавляют аморфный кремний (a-Si) с низким содержанием водорода. Затем кремний повторно кристаллизуется в виде поликристаллической плёнки LTPS [1].

Процесс LTPS намного сложнее, чем a-Si TFT, но подвижность электронов LTPS TFT более чем в 100 раз выше, чем у a-Si TFT (> 100 $см^2/В{\cdot}с$). На рис. 2 показаны варианты структур кремния (Si, a-Si, LTPS) и отображено условное сравнение подвижности электронов в них.

Основные характеристики дисплеев LTPS TFT-LCD перечислены далее.

1. *Низкое энергопотребление и сверхвысокое разрешение.* Высокая подвижность электронов означает, что меньшие транзисторы могут обеспечить необходимый заряд. Ёмкость также выше, чем у a-Si TFT. Когда эффективная площадь пропускания света становится больше, можно добиться такой же яркости, используя меньшую подсветку или мощность, при этом достигается высокое разрешение.
2. *Узкие рамки дисплеев.* Обычный a-Si TFT-дисплей требует драйверов с двух-трёх сторон, что затрудняет изготовление дисплеев с тонкими рамками. LTPS TFT-дисплей может интегрировать IC-драйвер непосредственно в стеклянную подложку, что позволяет сделать очень узкую рамку и получить высокое качество изображения. Интегральная схема LTPS TFT-дисплея требует меньше внешних сигнальных соединений, снижая количество частей ЖК-матрицы.
3. *Уменьшенная толщина.* Поскольку некоторые из драйверов IC могут быть размещены в стеклянной подложке, это позволяет упростить печатную плату и уменьшить её размер. По мере того как ЖК-матрица уменьшается, дисплеи становятся легче и тоньше.
4. *Основа для OLED.* OLED использует специальную токоведущую архитектуру. LTPS с высокой плотностью

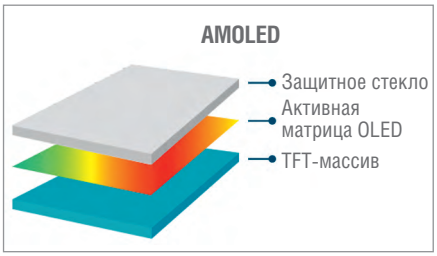



**Рис. 3. Структура AMOLED-дисплея**

элементов позволяет реализовать OLED-дисплей с высокой яркостью и лучшим качеством изображения, также увеличивается время жизни OLED-дисплея. Высокая подвижность электронов означает, что на OLED-дисплей можно подать более высокий ток возбуждения, что делает LTPS подходящей базой для OLED-дисплея с активной матрицей (AMOLED).

На сегодняшний день технология LTPS в основном используется при изготовлении дисплеев смартфонов, однако выпуск этих дисплеев для ноутбуков и планшетов также весьма актуален. Помимо AUO активно продвигают LTPS-дисплеи для ноутбуков такие тайваньские производители, как JDI, Tianma и ряд других. Создание более привлекательных моделей ноутбуков и планшетов требует применения более качественных по многим параметрам дисплеев. Это скажется на повышенном энергопотреблении и, как следствие, снизит время работы от батареи. Чтобы сохранить дизайн изделий и не допустить увеличения габаритов из-за батареи повышенной ёмкости, на помощь могут прийти именно LTPS-дисплеи, которые обеспечат требуемые характеристики.

**Дисплей AMOLED** (Active Matrix OLED – активная матрица на органических светоизлучающих диодах) – одна из ведущих тенденций в современных технологиях отображения. Он играет важную роль в мобильных устройствах, которые требуют низкого энергопотребления, небольшого веса и высокой цветопередачи.

AMOLED-дисплей является самоэмиссионным и не требует подсветки или цветного фильтра. Его преимущества включают лёгкость, малую толщину, низкое энергопотребление, высокую контрастность, насыщенность цвета, широкий угол обзора и быстрое время отклика.

AUO продолжает развивать технологию AMOLED. Помимо применений для смартфонов, AUO изготавливает AMOLED-дисплеи ультравысокого разрешения для продуктов типа «умные» часы и устройств виртуальной реальности.

Активная матрица OLED наносится на TFT-массивы (рис. 3), которые активируются при прохождении электрических токов. Эти TFT-массивы действуют как переключатели для каждого пикселя, а также содержат накопительный конденсатор, который позволяет использовать большие дисплеи. Дисплеи AMOLED не имеют ограничений по размеру и работают по тем же основным принципам, что и OLED-дисплеи.

Обычно AMOLED-дисплей состоит из двух TFT-транзисторов на каждый пиксель – один для запуска и остановки зарядки накопительных конденсаторов, а другой для обеспечения постоянного напряжения и тока в пикселе.

Основные достоинства AMOLED-дисплеев:

- быстрое время отклика;
- яркие цвета;
- большие углы обзора.

## Технологии отображения AUO

### Сверхвысокое разрешение

Изображение на панели дисплея состоит из пикселей. Разрешение дисплея – это количество пикселей, которые может отображать панель. Панель, обладающая способностью отображать больше пикселей, имеет более высокое разрешение и чёткое изображение.

PPI (Pixels per Inch) – это количество пикселей на квадратный дюйм. Чем выше PPI, тем больше деталей отображает панель. При одинаковых размерах экранов более высокое разрешение означает более высокое число PPI.

Технология ультравысокого разрешения (UHD 4K) на сегодня стала основной тенденцией для больших дисплеев. UHD 4K используется в ЖК-телевизорах, PID-дисплеях, настольных мониторах, ноутбуках и смартфонах. UHD 4K имеет разрешение 3840×2160 пикселей, то есть ЖК-панель или отображаемое содержимое имеют горизонтальное разрешение 3840 пикселей и вертикальное разрешение 2160 пикселей. Это двойное вертикальное и горизонтальное разрешение Full HD (1920×1080). Поскольку UHD 4K имеет в 4 раза больше пикселей, чем Full HD, то использование этой технологии позволяет представлять гораздо более чёткие и подробные изображения. Помимо улучшения тонких деталей и резкости, такой дисплей обеспечивает более глубокое изображение, большее чувство пространства и глубину на статическом содержимом, а также плавное движение. В сочетании с широкой цветовой гаммой это создаёт яркие и живые цвета.

В настоящее время пользователи читают, передают и совместно используют большое количество текстов, изображений и видеоматериалов на персональных мобильных устройствах. Это повышает требования к экранам, способным показывать более тонкие детали. Мобильные устройства, такие как смартфоны, планшеты, ноутбуки и носимые дисплеи, имеют повышенные требования к плотности пикселей на дисплее. Таким образом, PPI является важным параметром измерения качества изображения.

Чем выше значение PPI, тем более чётко и подробно информация будет отображаться (рис. 4). Высокое значение параметра PPI позволяет отображать символы с повышенной резкостью и более полно представлять веб-контент без потери качества при масштабировании. Помимо качественного представления деталей и глубины изображения дисплеи формата UHD 4K хорошо подходят и для воспроизведения видео высокого разрешения. К примеру, AUO


**Рис. 4. Визуальное сравнение различных значений PPI**

# iBASE

# Сервисные вычислительные решения
## для пассажирского транспорта

СООТВЕТСТВИЕ EN 50155

ОТОБРАЖЕНИЕ ИНФОРМАЦИИ • ВИДЕОНАБЛЮДЕНИЕ • СВЯЗЬ И ОПОВЕЩЕНИЕ • КОНТРОЛЬ ОПЛАТЫ

ЛУЧШЕЕ СООТНОШЕНИЕ ЦЕНА – КАЧЕСТВО

BC Best Choice

### Встраиваемые компьютеры MPT-3000/MPT-7000

- Процессор Intel Atom E3845/Core i7-6600U
- Диапазон рабочих температур –40…+70°C
- Поддержка двух сотовых сетей
- Модульный DC/DC-преобразователь
- Вибростойкость и ударопрочность
- Специализированные модули расширения MiniPCIe
- Внешний слот расширения PCIe (у MPT-7000)

### Панельные компьютеры BYTEM-103/BYTEM-123

- Диагональ дисплея 10,4″/12,1″
- Диапазон рабочих температур –40…+70°C/–25…+55°C
- Проекционно-ёмкостная сенсорная мультитач-панель
- Процессор Intel Atom E3845
- Степень защиты по передней панели IP65 и с тыльной стороны IP54

### Ультраширокоформатные моноблоки ARD-028/ARD-038

- Диагональ дисплея 28″/38″, разрешение 1920 × 360/540, яркость 700 кд/м$^2$
- Встроенный одноплатный компьютер на базе процессора Intel Atom E3825/ Pentium N4200


ProSoft® WWW.PROSOFT.RU
ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

| | | |
|---|---|---|
| МОСКВА | (495) 234-0636 | info@prosoft.ru |
| С.-ПЕТЕРБУРГ | (812) 448-0444 | info@spb.prosoft.ru |
| АЛМА-АТА | (727) 321-8324 | sales@kz.prosoft.ru |
| ВОЛГОГРАД | (8442) 260-048 | volgograd@prosoft.ru |
| ВОРОНЕЖ | (920) 402-3158 | chikin@prosoft.ru |
| ЕКАТЕРИНБУРГ | (343) 356-5111 | info@prosoftsystems.ru |
| КАЗАНЬ | (843) 203-6020 | info@kzn.prosoft.ru |
| КРАСНОДАР | (861) 224-9513 | krasnodar@prosoft.ru |
| Н. НОВГОРОД | (831) 215-4084 | nnovgorod@prosoft.ru |
| НОВОСИБИРСК | (383) 202-0960 | info@nsk.prosoft.ru |
| ОМСК | (3812) 286-521 | omsk@prosoft.ru |
| ПЕНЗА | (8412) 49-4971 | penza@prosoft.ru |
| САМАРА | (846) 277-9166 | info@samara.prosoft.ru |
| УФА | (347) 292-5216 | info@ufa.prosoft.ru |
| ЧЕЛЯБИНСК | (351) 239-9360 | chelyabinsk@prosoft.ru |

УЗНАТЬ БОЛЬШЕ

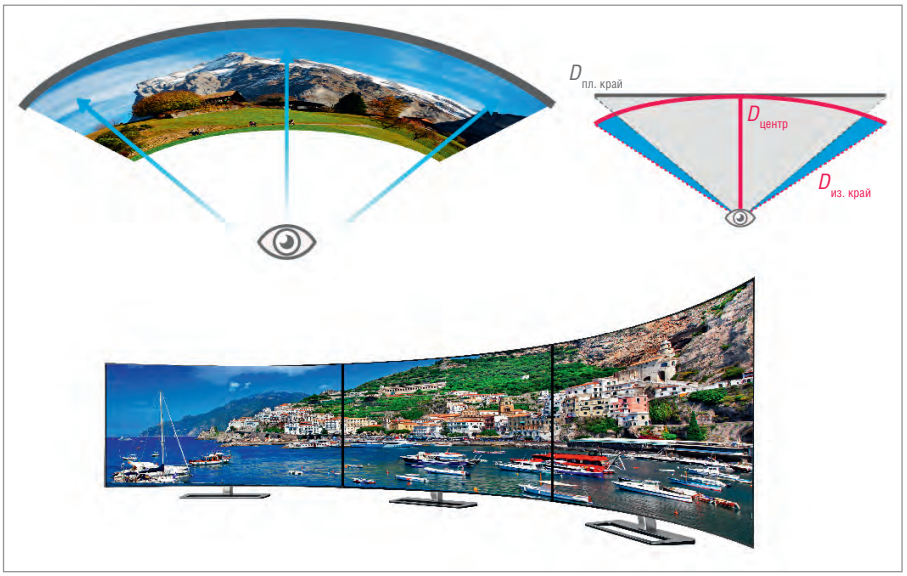



**Рис. 5. Иллюстрация изогнутой ЖК-панели**

разработала 5,5″ ЖК-панель для смартфонов с PPI > 538, которая в полной мере обеспечила качество отображения графики и видео.

## Изогнутые дисплеи

Изогнутый дизайн дисплеев соответствует особенностям зрения человеческих глаз. Изогнутый экран предлагает более широкие углы обзора и улучшает впечатления от просмотра. Он также обеспечивает неизменную чёткость и изображение без искажений – нет визуальных различий независимо от угла просмотра.

На рис. 5 показано, каким образом возникают искажения на плоских дисплеях и почему на изогнутых формах таких искажений нет. Чтобы избежать искажений, расстояние от точки обзора до центра экрана ($D_{центр}$) должно совпадать с расстоянием от точки обзора до края экрана ($D_{пл.\ край}$ и $D_{из.\ край}$). Чем больше размер экрана/видеостены, тем сильнее проявляются эти искажения.

Изогнутый дизайн также способствует уменьшению усталости глаз зрителя от фокусировки на экране в течение длительных периодов времени и демонстрирует очевидные преимущества дизайна по сравнению с обычными аналогами. Кроме того, фирменная технология ультратонкой изогнутой подсветки AUO также приводит к значительному уменьшению толщины модуля и включает в себя функцию локального затемнения для обеспечения высокого качества изображения. Локальное затемнение реализовано в виде подсвечивания групп светодиодов в зависимости от изображения, то есть на тёмных зонах изображения светодиоды затемняются, а на светлых светят более ярко. Этот механизм даёт лучший уровень чёрного и большую контрастность изображения. На сегодняшний день данный способ подсветки позволяет достичь самых лучших характеристик изображения.

Для различных применений AUO может предложить варианты дисплеев с различной кривизной в зависимости от требуемого угла обзора. Помимо изогнутых ЖК-панелей, компания AUO также разработала изогнутые игровые мониторы и дисплеи для автомобильных применений, которые могут быть адаптированы к обтекаемому интерьеру автомобиля, чтобы максимально вписываться в дизайн салона автомобиля.

## Узкая рамка дисплея

Узкая рамка дисплея – современный тренд в дизайне ЖК-дисплеев последних поколений. Фирменная технология AUO GOA (Gate on Array) позволила интегрировать схемы управления (драйверы строк и столбцов) в подложку ЖК-матрицы. Технология GOA значительно уменьшает количество микросхем драйверов, тем самым достигается сверхузкий дизайн ЖК-панели и расширяется рабочее поле до максимального значения при той же разрешающей способности (рис. 6). Технология GOA применяется в конструкциях широкоформатных ЖК-панелей AUO и ЖК-панелей настольных мониторов для обеспечения эффекта отсутствия рамки дисплея.

Дисплеи AUO для видеостен имеют ширину рамки всего 1,8 мм, и когда они собраны в видеостену, то пользователь видит единое изображение с едва заметными разделителями.

На рынке мобильных устройств производители стремятся к созданию так называемого безрамочного дизайна своих изделий. Технология LTPS от AUO не только обеспечивает более высокое разрешение, но и уменьшает объём пространства, необходимого для схем управления (схемы драйверов) и тем самым максимально удовлетворяет ожидания потребителей по качеству и внешнему виду изображения.

## Сенсорные решения

В линейке дисплеев AUO присутствуют модели с интегрированными сенсорными функциями, то есть установка сенсорного экрана выполняется непосредственно в процессе производства ЖК-панели. К преимуществам сенсорных панелей AUO относятся тонкие и лёгкие конструкции, исключительные оптические характеристики и упрощённые производственные процессы изготовления ЖК-панелей. Разработаны различные сенсорные решения для планшетов, ноутбуков, смартфонов и промышленных применений.

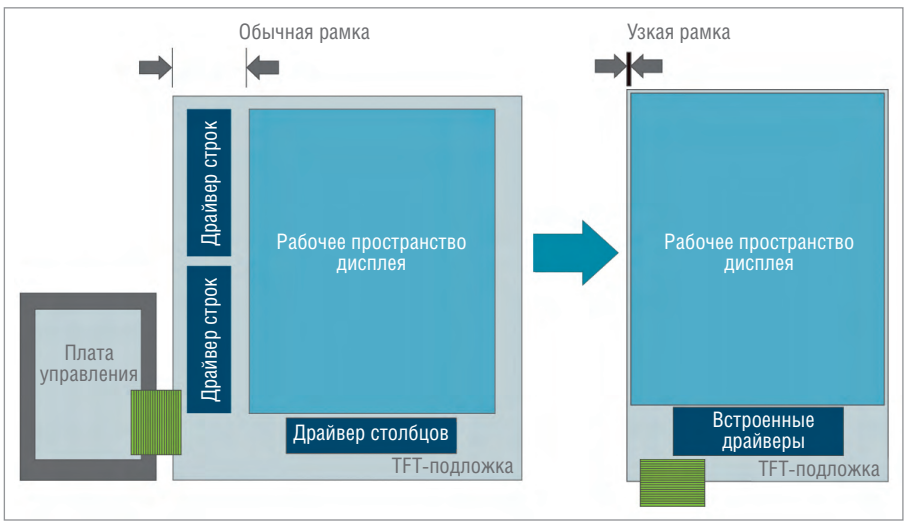



**Рис. 6. Переход от дисплея с обычной рамкой к «безрамочному» варианту**

ADVANTIX intellect

# ОТКАЗОУСТОЙЧИВОЕ РЕШЕНИЕ ДЛЯ КРИТИЧЕСКИ ВАЖНЫХ ПРИЛОЖЕНИЙ

intel Technology Provider Platinum 2015

## КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- «Нулевое» время простоя — обеспечение непрерывности работы приложений без потери данных и транзакций
- «Нулевое» администрирование — решение является простым в эксплуатации и не требует высоких затрат на обслуживание
- Предотвращение простоев, а не восстановление после сбоев
- Уровень доступности 99,999%, что соответствует 5,25 минуты простоя в год

## AdvantiX Intellect FT-BOX

Microsoft Linux SCADA

WWW.ADVANTIX-PC.RU

ProSoft®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

УЗНАТЬ БОЛЬШЕ

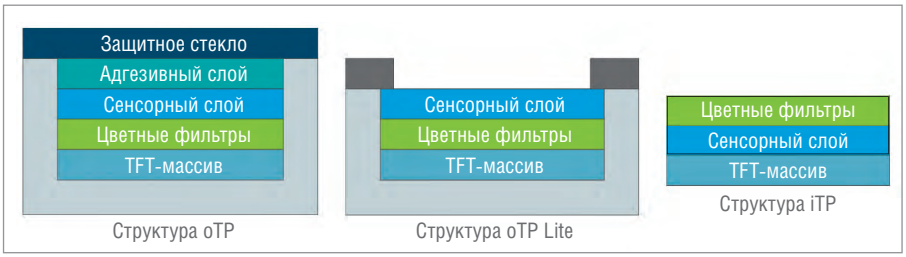



**Рис. 7. Варианты сенсорных решений AUO**

Для ноутбуков компания AUO создала интегрированное сенсорное решение oTP (On-Cell Touch Panel) и его облегчённую версию – oTP Lite.

oTP предлагает конструкцию со встроенным мультисенсорным слоем от края до края (дизайн "edge-to-edge") с высоким разрешением и высоким коэффициентом пропускания. Этот сенсорный слой наносится непосредственно на ЖК-панель, затем устанавливаются поляризатор и защитное стекло. Основные плюсы этой технологии: повышается реагирование на касания, улучшается цветопередача, искажения изображения сводятся на нет. Технология oTP также совместима с профессиональными средствами рисования (стилусами, маркерами и т.п.), что даёт большую точность рисования.

Технология oTP Lite отличается от oTP тем, что в ней отсутствует защитное стекло, она предназначена для более лёгких и тонких устройств. Дисплеи с oTP Lite соответствуют стандартам VESA, они позволяют разработчикам легче реализовать сенсорные функции в изделиях.

На рис. 7 показаны решения AUO в части интегрированных сенсорных дисплеев. Помимо решения oTP компания AUO предлагает iTP (In-Cell Touch). iTP – это решение, в котором сенсорный слой и схемы управления дисплеем интегрированы в производственный процесс создания ЖК-дисплея, но тут сенсорный слой встраивается в цветные фильтры, располагаясь прямо под крайним слоем стекла на экране, тем самым исключается необходимость применения среднего слоя стекла. Такой подход значительно упрощает процесс производства сенсорных панелей и позволяет создавать более тонкие дисплеи. К примеру, сенсорный дисплей 15″ формата Full HD, выполненный по технологии iTP, становится почти на 1 мм тоньше, и его вес сокращается на 200 г.

Согласно подсчётам аналитического агентства DisplaySearch, поставки дисплеев, выполненных с интегрированными сенсорными технологиями, в период 2014–2017 гг. во всём мире превысили отметку 90 млн штук. В основном эти дисплеи применяются в смартфонах начального и среднего уровня. По прогнозу в 2018 году показатель отгрузок достигнет значения 130 млн устройств.

## Сферы применения дисплеев AUO

Компания AUO выпускает продукцию, которая применяется практически во всех возможных сегментах и отраслях, где необходимы средства отображения (рис. 8). Постоянные исследования и разработки, внедрение новых технологий и долгосрочные капиталовложения привели AUO к сильному и стабильному положению на этом рынке. Результаты работы компании неоднократно отмечены различными наградами, призами и премиями различных международных конкурсов, таких как Gold Panel Awards, Taiwan Corporate Sustainability Awards и Golden Wingspan Award.

### ЖК-телевизоры

AUO лидирует в телевизионной отрасли с безрамочными ЖК-телевизорами (Advanced LCD TV), которые включают в себя весь набор традиционных технологий: разрешение UHD 4K, изогнутый дизайн, HDR, локальное затемнение, а также технологию квантовых точек – Quantum Dots (QD).

Технология QD позволяет улучшить цветовой диапазон дисплея, яркость и контрастность без повышения энергопотребления. Основа технологии QD – это специализированные цветные плёнки, расположенные в блоке светодиодной подсветки ЖК-дисплея (рис. 9). На этих плёнках находятся флуоресцентные полупроводниковые нанокристаллы, которые светятся, когда подвергаются воздействию тока или света и испускают только один цвет, определяемый их размером: красные точки размером до 7 нм (150 атомов) в диаметре, зелёные точки около 3 нм (30 атомов), синие точки – самые маленькие, размер их ядра составляет около 2 нм (15 атомов). Из-за крошечных размеров синие частицы очень уязвимы и сложны для работы, и по этой причине их обычно исключают из технологии, заменяя пустыми точками. Для получения синего цвета в QD-дисплеях используется подсветка синего цвета, а не белая, как у классических дисплеев. Синий свет пропускается через пустые пиксели для генерации синего цвета, в то время как красные и зелёные точки отвечают за красный и зелёный цвета.

По характеристикам QD-дисплеи находятся на уровне устройств, выполненных по технологии OLED, но затраты на производство матриц гораздо ниже [2].

Насыщенность цвета превышает 100% стандарта NTSC, что позволяет отображать точную и более широкую цветовую гамму с богатой градацией даже в мельчайших деталях.

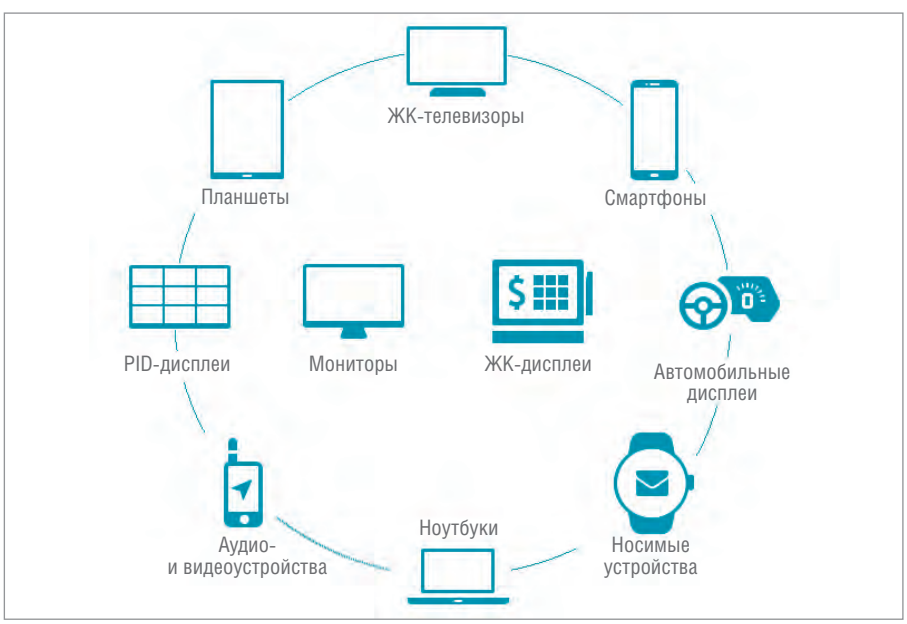



**Рис. 8. Области применения дисплеев AUO**

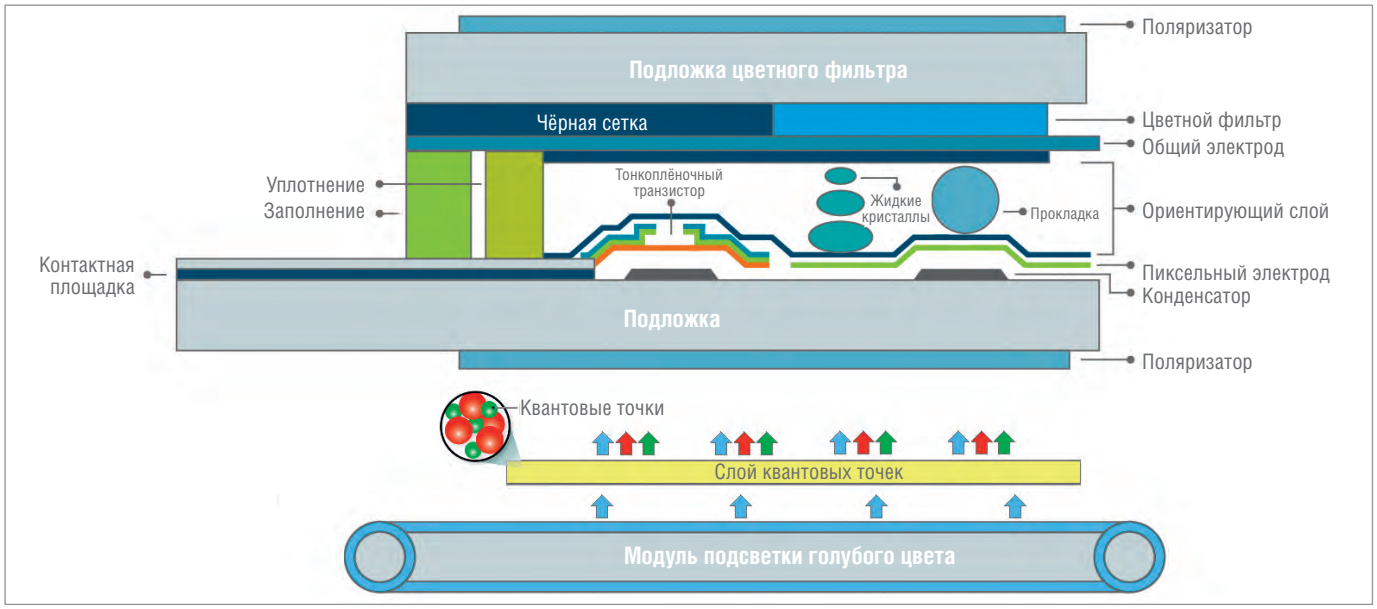



**Рис. 9. Структура QD-дисплея**

Технология HDR с высоким коэффициентом контрастности на QD-дисплеях обеспечивает большую глубину цвета и более тонкие детали на тёмном и ярком фоне.

Телевизоры AUO на базе QD-дисплеев также имеют широкий угол обзора, быстрое время отклика и высокую цветопередачу благодаря эффективной светодиодной подсветке.

В табл. 1 представлены модели телевизоров производства компании AUO на сегодняшний день и некоторые их параметры. Показано, что в зависимости от размеров экрана AUO применяет те или иные технологии для удовлетворения потребностей и желаний потребителей. С ростом диагонали экрана появляются модели с повышенной частотой обновления изображения, а также модели с изогнутым и безрамочным дизайном.

## Информационные дисплеи

AUO предлагает широкий набор информационных дисплеев (PID – Public Information Display), включая рекламные панели, интерактивные электронные панели, двухсторонние и прозрачные дисплеи, зеркальные ЖК-панели, экраны транспортной информации и различные видеостены. Разнообразная продукция подходит как для внутреннего, так и для наружного применения, обладая такими характеристиками, как высокие надёжность, разрешение и яркость, крайняя узкая рамка, светодиодная подсветка и низкое энергопотребление.

PID-дисплей для применений вне помещения обладает сверхвысокой яркостью, которая способствует выводу чётких изображений даже под прямыми солнечными лучами. Специальная конструкция поляризатора также позволяет пешеходам в поляризованных солнцезащитных очках считывать информацию с экрана.

Двухсторонний PID-дисплей конструктивно представляет собой два ЖК-дисплея с объединённой подсветкой. Такие дисплеи характеризуются малой толщиной и небольшим весом.

Прозрачные дисплеи – это новый тип средств отображения информации, они наиболее востребованы в рекламно-торговых и развлекательных секторах. На таком дисплее видно не только информацию на экране, но и предметы за дисплеем, как за обычным стеклом. Задний поляризатор в этих дисплеях в отличие от классических ЖК-дисплеев имеет другую ориентацию, обеспечивающую прозрачное состояние пикселей в выключенном состоянии, что создаёт эффект прозрачности.

ЖК-дисплеи с управляемым зеркальным режимом позволяют создавать популярные нынче рекламные носители, в которых совмещены два режима – обычный дисплей и режим зеркала. В режиме дисплея на экране отсутствует отражение от окружающих предметов, а в зеркальном режиме обеспечена высокая степень зеркальности. Зоны дисплея и зеркала можно комбинировать и смешивать, создавая таким образом различные интерактивные решения [3].

## Решения для настольных мониторов

Направление настольных ЖК-мониторов компании AUO включает в себя обычные настольные, игровые, профессиональные и изогнутые дисплеи.

ЖК-дисплеи AUO для профессиональных настольных мониторов обладают такими характеристиками, как форматы UHD 4K (3840×2160) и WQHD (3440×1440), широкая цветовая гамма и безрамочная конструкция. Эти дисплеи хорошо подходят для профессионального графического дизайна, визуального редактирования, медицинского, игрового и промышленного использования. AUO может похвастаться самой полной линейкой игровых дисплеев

*Таблица 1*

**ЖК-телевизоры AUO с указанием характеристик дисплеев и конструкций**

| Диагональ | Формат | Разрешение | Частота обновления | Изогнутый дизайн | «Безрамочный» дизайн |
|---|---|---|---|---|---|
| 19,5″ | HD | 1366×768 | 60 Гц | – | – |
| 32″, 39″ | HD | 1366×768 | 60 Гц | – | – |
| | Full HD | 1920×1080 | | | |
| 43″, 50″ | Full HD | 1920×1080 | 60 Гц | 50″ UHD 4K | – |
| | UHD 4K | 3840×2160 | | | |
| 55″, 65″ | Full HD | 1920×1080 | 60/120 Гц | Да | Да |
| | UHD 4K | 3840×2160 | | | |
| 75″, 85″ | UHD 4K | 3840×2160 | 120 Гц | Да | 75″ |

с прекрасными значениями характеристик, например, с высокой частотой обновления 240 Гц, большими размерами и высоким разрешением.

В бытовом сегменте AUO предлагает мониторы с диагональю экрана от 17 до 27″ и разрешением от 1280×1024 до 2560×1440. Модели мониторов более 21″ обладают плоскими безрамочными корпусами. В зависимости от модели монитора применяются ЖК-матрицы, изготовленные по технологии TN, AHVA или AMVA.

Так как на рынке ЖК-дисплеев появилось огромное количество различных технологических и маркетинговых обозначений типов матриц, то нужно пояснить, что именно производит компания AUO (рис. 10).

**TN** (Twisted Nematic – скрученные нематические кристаллы) – самая старая и простая технология производства ЖК-матриц, которая используется до сих пор ввиду своей дешевизны. Нематические кристаллы выстроены в матрице друг за другом в виде спирали. При отсутствии напряжения кристаллы поворачивают ось поляризации света на 90°, он оказывается в одной плоскости со вторым поляризатором и проходит через него – получается белый пиксель. При подаче напряжения на электроды спираль кристаллов сжимается, ось света не поворачивается и поглощается вторым поляризатором – получается чёрный пиксель. Для создания оттенков серого напряжением меняется положение кристаллов и тем самым свет частично проходит через фильтры. Основное достоинство TN-матриц – время отклика на настоящий момент считается одним из лучших.

**AHVA** (Advanced Hyper-Viewing Angle, дословно «продвинутые гипереуглы обзора») – это вариант IPS-матрицы от компании AUO. В этих матрицах изменено расположение управляющих электродов (направителей) и самих жидких кристаллов (они не образуют спираль и при приложении напряжения поворачиваются все разом). Для получения чёрного пикселя к матрице не прикладывается напряжение, жидкие кристаллы не поворачиваются и свет не проходит, так как поляризаторы повёрнуты перпендикулярно друг к другу. При приложении напряжения жидкие кристаллы в матрице поворачиваются перпендикулярно своему начальному положению и пропускают свет, образуя белый пиксель. К достоинствам этих матриц относятся глубокий чёрный цвет, повышенная контрастность, большие углы обзора и частота обновления экрана.

MVA-матрица от AUO имеет название **AMVA** (Advanced MVA – продвинутое многодоменное вертикальное выравнивание). В AMVA конструктивно изменены подложки – на них имеются выступы, которые и образуют домены из жидких кристаллов, а также электроды подведены к обеим подложкам. Домены переключаются одновременно, но кристаллы в них наклоняются в противоположных направлениях. При отсутствии напряжения кристаллы выстраиваются перпендикулярно подложке, будет чёрный пиксель. При наличии напряжения кристаллы поворачиваются на нужный угол и изменяют поляризацию света. При смене величины напряжения будет меняться угол наклона кристаллов и изменится оттенок серого вплоть до белого (при максимальном значении напряжения). Эта технология обеспечивает чрезвычайно высокие коэффициенты контрастности, в результате чего просмотр изображения становится более удобным. Матрицы AMVA имеют большую глубину чёрного цвета. Кроме того, энергопотребление ниже из-за изменённого модуля подсветки и высокой пропускной способности ячеек матрицы, что позволило уменьшить количество используемых светодиодов.

## ЖК-дисплеи для ноутбуков

ЖК-дисплеи производства AUO на сегодня самые распространённые на рынке ноутбуков. Многие крупные производители используют дисплеи AUO в своих изделиях, среди них ASUS, IBM, Dell, MSI и даже такие «монстры» как LG, Toshiba и Samsung, иногда устанавливают в свои ноутбуки дисплеи AUO, хотя имеют дисплеи собственного производства отличного качества. Причина этого – широкий модельный ряд, качество и отличные характеристики дисплеев AUO.

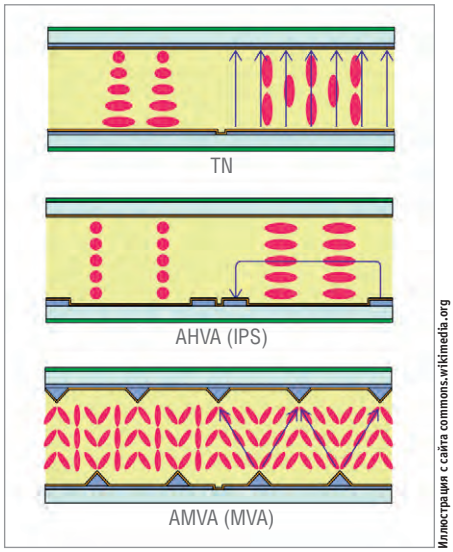



Иллюстрация с сайта commons.wikimedia.org

**Рис. 10. Типы матриц, выпускаемых компанией AUO**

AUO предлагает полную линейку LTPS-дисплеев с разрешением UHD 4K для вывода детализированных и ярких изображений, с узкими рамками для увеличения активной области дисплея, а также с более низкими значениями энергопотребления, они подходят для бытовых, профессиональных и игровых ноутбуков. Компаиня AUO также разработала серию a-Si ЖК-дисплеев для различных применений.

Для игровых ноутбуков AUO выпускает AHVA ЖК-дисплеи формата UHD 4K, в которые интегрирована технология ультравысокой частоты обновления и быстрого времени отклика, чтобы обеспечить отличное качество изображения и производительность в динамике.

В поставках AUO также присутствует oTP-дисплей (ЖК-панель с интегрированным сенсорным экраном) как оптимальное решение для сенсорных ноутбуков.

## Дисплейные решения для планшетов

Дисплеи AUO для планшетов эстетичны, а также обладают высоким разрешением, ультратонким дизайном, лёгким весом, широким углом обзора и низким энергопотреблением, обеспечивают удобство в использовании.

Для планшетов AUO предлагает комплексные дисплейные решения, включая интегрированные сенсорные функции, технологию AHVA и высокоэффективную светодиодную подсветку.

В линейке планшетных дисплеев AUO есть разнообразные варианты – от 6,4 до 11,6″, с различными разрешениями экрана и сенсорными функциями.

## ЖК-дисплеи для различного оборудования

Типовые ЖК-дисплеи AUO обладают рядом существенных достоинств: высокое разрешение, яркость и контрастность, широкие углы обзора, расширенный диапазон рабочих температур, длительный срок службы и низкое энергопотребление. Поэтому они нашли широкое применение в различных областях: в автоматизации производства, систем безопасности, медицинского оборудования, в сфере транспортной информации, в различных тер-

nVent

Schroff®

# NOVASTAR

## Дизайн • Функциональность • Практичность


## ИнNOVAционный шкаф для 19″ электронного оборудования

- Аудио- и видеотехника
- Лабораторные измерения
- Испытания и контроль

### Технические характеристики

- 19-дюймовый разборный каркас из алюминиевого профиля
- Два класса нагрузки: Slim-line и Heavy-Duty
- Ширина всего 553 мм
- Высота от 360 (6U) до 2200 мм (47U)
- Глубина от 550 до 880 мм
- Боковой Т-образный паз для крепления консолей и пультов
- Легкое перемещение на роликовых опорах

ProSoft®
WWW.PROSOFT.RU

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

**МОСКВА**
(495) 234-0636
info@prosoft.ru

**САНКТ-ПЕТЕРБУРГ**
(812) 448-0444
info@spb.prosoft.ru

**ЕКАТЕРИНБУРГ**
(343) 356-5111
info@prosoftsystems.ru

УЗНАТЬ БОЛЬШЕ

миналах, игровых автоматах, рекламных вывесках, наружных дисплеях и т.п.

При необходимости AUO может интегрировать в эти дисплеи такие технологии, как мультисенсорный экран и изогнутый дизайн.

В настоящее время AUO предлагает более 60 моделей ЖК-дисплеев с различными размерами (от 4,3 до 32″) и характеристиками. Примеры доступных моделей с указанием основных характеристик приведены в табл. 2. Отметим основные особенности:

- долгий срок жизни моделей – до 6 лет;
- взаимозаменяемость при снятии с производства;
- расширенный диапазон рабочих температур (модели для уличного применения);
- хорошие потребительские характеристики (углы обзора, яркость, палитра);
- срок службы от 30 000 до 50 000 часов;
- варианты с интегрированными сенсорными экранами.

## Решения для аудио- и видеоустройств

AUO предоставляет высококачественные AHVA-дисплеи и заказные решения на их основе для широкого ассортимента аудио- и видеоустройств. Эти дисплеи обладают такими техническими преимуществами, как высокая разрешающая способность, тонкий дизайн и лёгкий вес, низкое энергопотребление и мультисенсорные функции.

Для устройств наружного применения AUO предлагает трансфлективные ЖК-дисплеи с низким энергопотреблением и читаемостью изображения при ярком солнечном свете.

Трансфлективный ЖК-дисплей по принципу работы представляет собой гибрид обычного ЖК-дисплея и дисплея типа «электронные чернила» (E-Ink). В конструкцию такого дисплея под слой жидких кристаллов добавлена специальная полимерная плёнка – трансфлектор (отражающий слой). Яркость этого дисплея складывается из двух составляющих: собственная подсветка + внешний свет, отражённый трансфлектором.

Впечатляющее качество изображения можно обеспечить как на открытом воздухе, так и в помещении. Изображения на экране стали хорошо читаемыми при сильном освещении даже на энергосберегающих дисплеях (с пониженной яркостью собственной подсветки).

Примеры таких аудио- и видеоустройств:

- аппаратура навигации;
- различные печатающие устройства (терминалы оплаты, системы контроля въезда/выезда, чековые станции);
- портативные системы видеонаблюдения;
- различные носимые устройства.

## Дисплеи для автомобильной промышленности

Уже давно прошли времена, когда автомобиль мог похвастаться лишь своей аудиосистемой с красивой съёмной панелью. Современные автомобили оснащаются различными мультимедийными центрами, информационными индикаторами и дисплеями, а также разнообразными развлекательными системами для пассажиров.

Компания AUO также не стоит в стороне и в части поставок дисплейных решений для автомобилей. Как и в других сегментах, доступен полный набор автомобильных дисплеев с высоким разрешением, широкой цветовой гаммой, большими углами обзора, низким отражением (антибликовые покрытия), вибростойкостью, коротким временем отклика даже при низкой температуре и высокой устойчивостью к погодным условиям. В модельном ряде стандартных серийных изделий AUO присутствуют дисплеи от 3,5″ (240×320) до 12″ (1920×720) с контрастностью 1000:1 и яркостью до 700 кд/м$^2$.

*Таблица 2*

**Примеры модельного ряда ЖК-дисплеев AUO**

| Примеры модельного ряда ЖК-дисплеев AUO | | | | | | |
|---|---|---|---|---|---|---|
| Модель | Размер | Разрешение | Контрастность | Яркость кд/м$^2$ | Диапазон рабочих температур | Интерфейс |
| G043FW01 V0 | 4,3″ | 480×272 | 400:1 | 450 | 0…+70°C | TTL |
| G057VTN01.0 | 5,7″ | 640×480 | 800:1 | 530 | –30…+85°C | TTL |
| G070VW01 V0 | 7″ | 800×480 | 700:1 | 400 | –30…+85°C | LVDS |
| G101EVN01.3 | 10,1″ | 1280×800 | 1300:1 | 500 | –30…+80°C | LVDS |
| G133HAN01.0 | 13,1″ | 1920×1080 | 1000:1 | 400 | 0…+70°C | LVDS |
| G150XVN01.0 | 15″ | 1024×768 | 1500:1 | 300 | –10…+70°C | LVDS |
| G170ETN02.1 | 17″ | 1280×1024 | 1000:1 | 800 | –30…+85°C | LVDS |
| G190EG02 V0 | 19″ | 1280×1024 | 2000:1 | 600 | 0…+50°C | LVDS |
| G230HAN01.1 | 23″ | 1920×1080 | 5000:1 | 300 | 0…+60°C | LVDS |
| G320ZAN01.0 | 32″ | 3840×2160 | 5000:1 | 700 | 0…+50°C | V-by-One |


Иллюстрация с сайта pxhere.com

**Рис. 11. Пример реализации информационной панели с использованием ЖК-дисплея свободной формы**

Компания AUO накопила огромный опыт в создании автомобильных дисплеев высокого класса для различных применений, начиная от комбинации автомобильных приборов, центрального информационного дисплея, «умного» зеркала заднего вида, головного дисплея и до развлекательных систем в автомобиле.

Помимо стандартных решений AUO предлагает дисплеи свободной формы, изогнутого дизайна и с интегрированными сенсорными функциями. Используя дисплеи AUO, можно реализовать все виды телематики и усовершенствованные системы помощи водителю с полным набором решений систем отображения, чтобы водители могли легко получить всю информацию об автомобиле и существенно повысить безопасность, а пассажиры наслаждались в поездке различными развлекательными системами (рис. 11).

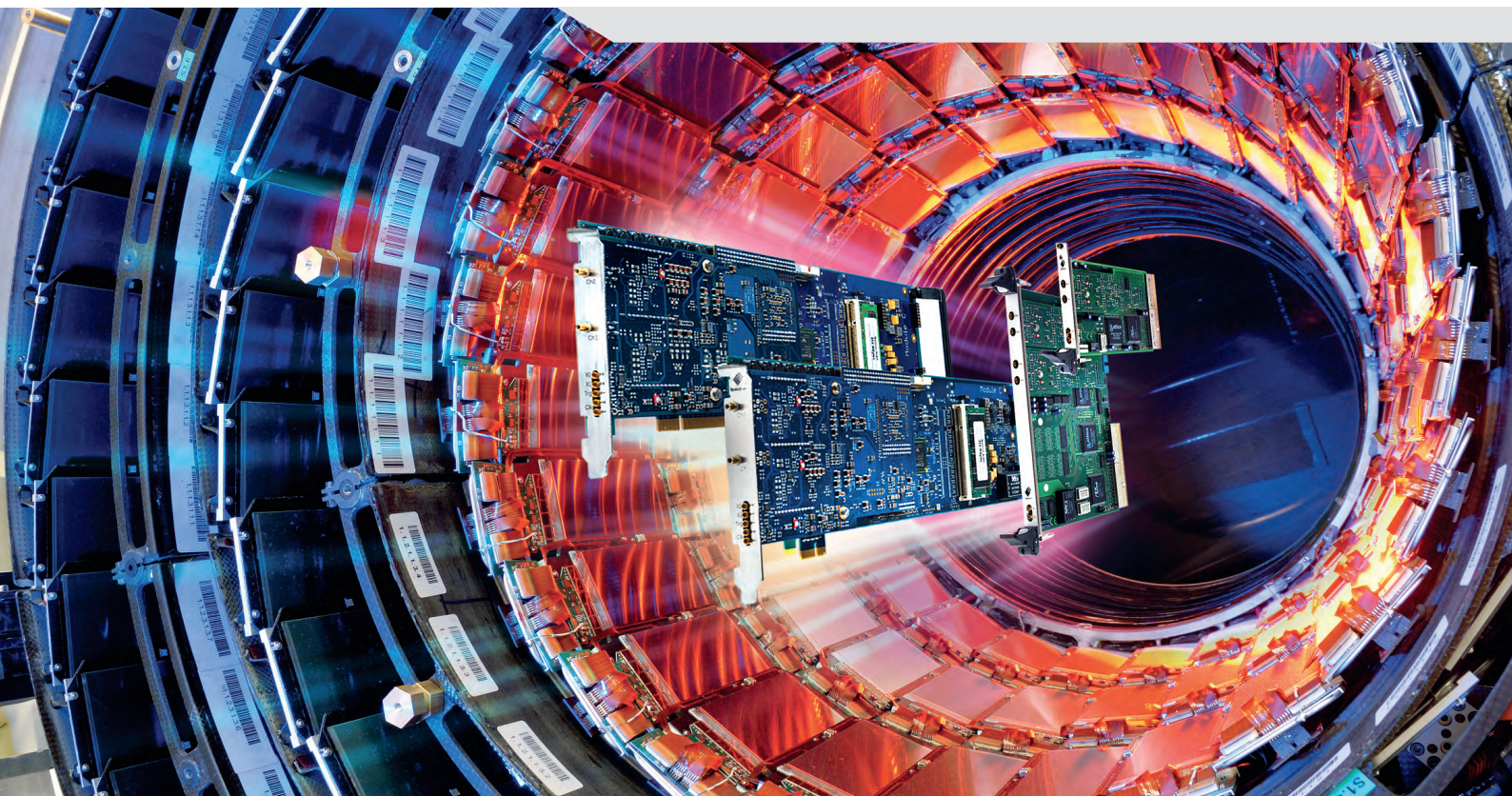
## Дисплеи для производителей телефонов и смартфонов

Следуя тенденции растущего спроса на смартфоны с крупными экранами, компания AUO разработала линейку дисплеев для таких смартфонов – у них большие экраны и сверхвысокие разрешения. Использование совокупности современных решений позволило AUO занять одно из лидирующих мест на рынке ЖК-дисплеев для телефонов и смартфонов.

Также компания AUO разработала и успешно реализует дисплеи с соотношением сторон 18:9, чтобы довести до максимума соотношение экрана и кор-

SPECTRUM

# *Высокоскоростные инструментальные платы Spectrum*



## Для широкого спектра решений по сбору данных и генерации сигналов

### PCI/PCI-X и PCI Express

- Свыше 200 моделей плат
- До 16 синхронных каналов
- Разрешение от 8 до 16 бит
- Частота опроса до 1 ГГц
- Встроенная память до 4 Гбайт
- Тактирование и многомодульная синхронизация

### 6U CompactPCI

- Около 80 вариантов модулей
- До 16 каналов
- Разрешение до 16 бит
- Частота опроса до 500 МГц

### 3U PXI

- Более 45 моделей
- Соответствие стандарту PXI
- Межмодульная синхронизация
- Тактирование 10 МГц
- Память до 512 Мбайт

### Программное обеспечение


- Собственное ПО SBench 6
- Поддержка ОС Windows, Linux
- Разработка систем сбора и записи данных по ТЗ заказчика
- Индивидуальное консультирование по выбору оборудования для конкретных применений

### LXI-системы сбора сигналов

- Более 60 моделей
- Соответствие стандарту LXI
- Число каналов 2–48
- Частота опроса до 500 МГц
- Разрешение от 8 до 16 бит
- Полоса частот от 100 кГц до 250 МГц

Иллюстрация с сайта pxhere.com

**Рис. 12. «Умные» часы (Smart Watch) с использованием круглого AMOLED-дисплея**

пуса телефона и значительно увеличить площадь дисплея. Согласно отчёту маркетинговой компании Sigmaintell, в 2017 году общемировые поставки дисплеев формата 18:9 достигли более 200 млн штук, при этом компания AUO вошла в тройку крупнейших производителей этих устройств вместе с Samsung Display и Tianma Micro-electronics. В прогнозах на 2018–2019 годы указывается, что не менее 40% всех выпускаемых смартфонов составят модели с полноэкранными дисплеями формата 18:9.

## Решения для различных носимых устройств

Уникальные характеристики AMOLED-дисплеев служат для обеспечения высоких потребительских свойств, таких как разрешающая способность, ультратонкий размер и малый вес, а также весьма низкое потребление энергии. Всё это позволяет использовать продукты AUO в популярных нынче носимых изделиях – в «умных» часах и устройствах виртуальной реальности.

Для «умных» часов были разработаны энергосберегающие AMOLED-дисплеи круглой формы сверхтонкой конструкции с высоким разрешением, обладающие всеми достоинствами дисплеев AUO. Эти круглые дисплеи с областью отображения по всей поверхности и узким дизайном рамки позволяют создавать наручные часы классического внешнего вида (рис. 12).

Виртуальная реальность (VR) – новая тенденция в развитии технологий нынешнего и следующего поколений. Устройство VR представляет собой носимый перед глазами дисплей для создания изображения и трекинг-систему, которая отслеживает изменение положения головы, таким образом, картинка на экране всегда соответствует направлению взгляда человека. Для устройств VR AUO предлагает AMOLED-дисплеи с набором всех своих фирменных технологий и уникальных характеристик. Высокая насыщенность цвета, превосходный коэффициент контрастности и большая яркость позволяют создать высококачественные устройства VR, обеспечивающие эффект полного погружения в виртуальную реальность.

## Инновационные решения в области солнечной энергии

Помимо своего основного профиля – средств отображения, с 2008 года компания AUO занимается разработками и внедрениями в области солнечной энергии.

AUO предлагает своим клиентам по всему миру инновационные решения в сфере солнечной энергетики с фирменными технологическими преимуществами, всесторонним обслуживанием

и интегрированной сервисной платформой. Компания AUO создала комплексное предложение, состоящее из эффективных и интегрированных решений, включающих поставку модулей солнечной электростанции, наладку, эксплуатацию и обслуживание, а также управление энергопотреблением.

Чтобы лучше помочь заказчикам в эксплуатации и обслуживании электростанций, AUO создала интегрированную сервисную программно-аппаратную платформу для обеспечения множества функций, включая мониторинг мощности электростанции в режиме реального времени, мгновенное обнаружение проблем и своевременное оповещение о них (рис. 13).


**Рис. 13. Комплекс предложений AUO в сфере солнечной энергии**

AUO оценивается многими консалтинговыми компаниями в области энергетики (такими как BNEF и EuPD Research) как один из ведущих разработчиков фотоэлектрических преобразователей (PV-модулей), входящий в десятку лучших производителей.

AUO предлагает различные PV-модули: монокристаллические, поликристаллические и набирающие в последние годы популярность PV-модули по технологии PERC (Passivated Emitter Rear Contact – диэлектрический слой на тыльной части солнечного элемента) с КПД от 16% и более 20%. Все модули обладают PID-устойчивостью (токи утечек сведены к минимуму), огнестойкостью и другими усиленными характеристиками, что позволяет безопасно внедрять их в самых разнообразных условиях.

У AUO есть превосходные возможности и обширный опыт работы с полным набором услуг по созданию и сопровождению солнечной электростанции. Компания является экспертом на всех этапах разработки проекта, обладает обширным опытом в области проектирования и строительства электростанций и интегрированной платформой для долгосрочного технического обслуживания.

AUO владеет самым большим количеством солнечных электростанций коммунального назначения различного масштаба на Тайване, от государственных организаций и зданий, до фабрик и заводов. Компания обладает богатым практическим опытом в проектировании и создании под ключ крупных солнечных электростанций, в том числе на фабричных крышах и больших высотах. Солнечные электростанции установлены на крышах всех фабрик AUO на Тайване. В настоящее время идёт активная работа по развитию солнечной энергетики с целью помощи клиентам в ис-

пользовании коммерческих офисов, фабрик, общественных зданий и объектов животноводства для создания новых источников «зелёной» энергии и сокращения выбросов углекислого газа.

## Заключение

Как мы видим, компания AUO является производителем качественной продукции и надёжным партнёром в области средств отображения информации. Дисплейные решения AUO способны удовлетворить все потребности различных сфер и отраслей, от бытового применения до использования в тяжёлых условиях эксплуатации.

Долгий срок жизни дисплеев AUO и своевременный выпуск новых моделей взамен снимаемых с производства позволяет закладывать их в долгосрочные проекты различной направленности. Широта номенклатуры изделий, возможность поставки от одного устройства и ценовая политика AUO делают продукцию весьма привлекательной, как для крупных производителей, так и для мелкосерийных проектов различных системных интеграторов. ●

## Литература

1. LTPS – низкотемпературная поликремневая технология. Что такое LTPS TFT ЖКИ? [Электронный ресурс] // Режим доступа : http://www.gaw.ru/html.cgi/txt/lcd/tech/ltps.htm.
2. Чем отличается Nano Cell от QLED [Электронный ресурс] // Режим доступа : http://ultrahd.su/video/nano-cell-qled-otlichiya.html.
3. Самарин А., Наймушин А. TFT ЖК-панели компании AUO для общественных информационных дисплеев // Компоненты и технологии. – 2014. – № 1.

**Автор – сотрудник фирмы ПРОСОФТ**
**Телефон: (812) 448-0444**
**E-mail: info@spb.prosoft.ru**

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

## ЛЭТИ и ПРОСОФТ: совместная подготовка кадров для технологического прорыва

29 марта на кафедре систем автоматического управления (САУ) СПбГЭТУ «ЛЭТИ» состоялось торжественное открытие модернизированной учебно-научной лаборатории «Промышленные системы управления и автоматизации».

Символическую красную ленту перерезали проректор по международной деятельности СПбГЭТУ «ЛЭТИ» Виктор Анатольевич Тупик и основатель компании ПРОСОФТ Сергей Александрович Сорокин.

Лаборатория включает в себя восемь индивидуальных исследовательских комплексов для изучения основ работы с программируемыми логическими контроллерами (ПЛК), SCADA-системами и распределёнными устройствами ввода/вывода. Кроме того, лаборатория оснащена стендом с макетом производственного комплекса для изучения основ управления технологическим процессом, диагностики и поиска неисправностей в автоматизированных системах управления.

– На новом оборудовании студенты познакомятся с основами построения автоматизированных систем управления технологическими процессами, научатся создавать алгоритмы управления промышленными объектами и связывать программируемые логические контроллеры с системами верхнего уровня, – сообщил доцент кафедры систем автоматического управления **Денис Михайлович Филатов**.

Современное российское оборудование компании ПРОСОФТ было предоставлено вузу на бесплатной основе в рамках программы импортозамещения. Оно заменило устаревшие аппаратные средства, которые использовались ранее.

Модернизация лаборатории позволит повысить практико-ориентированную подготовку магистрантов второго курса факультета электротехники и автоматики, обучающихся по направлению «Управление в технических системах». В перспективе на базе лаборатории планируется организация платных курсов повышения квалификации для программистов и инженеров, которые используют в своей работе FASTWEL I/O – модульный программируемый логический контроллер (ПЛК) отечественного производства.

– Среди вузов, с которыми мы сотрудничаем, СПбГЭТУ «ЛЭТИ» занимает особое место. Руководство университета полностью поддерживает наши инициативы и быстро внедряет их в учебный процесс. Уверен, лаборатория «Промышленные системы управления и автоматизации» будет в значительной степени способствовать повышению уровня подготовки выпускников ЛЭТИ, – считает основатель компании ПРОСОФТ **Сергей Александрович Сорокин**.

Договор между СПбГЭТУ «ЛЭТИ» и компанией ПРОСОФТ был подписан в 2017 году. Документ предполагает использование продуктов партнёра университета в образовательном процессе, создание совместного учебно-научного центра, участие преподавателей и аспирантов ЛЭТИ в разработке программного обеспечения компании ПРОСОФТ. В перспективе стороны планируют развивать взаимодействие в сферах силовой электроники, производства элементной базы радиоэлектронных систем и СВЧ-электроники, а также в области Delta Design – первой современной отечественной системы автоматизированного проектирования, реализующей сквозной цикл проектирования электроники. ●

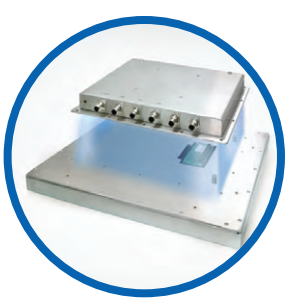
Открытие лаборатории «Промышленные системы управления и автоматизации»

Оборудование лаборатории

# Серия AEx

## во взрывозащищённом исполнении, удовлетворяющая требованиям ТР ТС 012 и ATEX для зоны 2

- Корпуса серии AEx из нержавеющей стали устойчивы к вибрации, ударам, коррозии, низкой и высокой температуре
- Модели имеют степень защиты IP66 и оснащаются надёжными и безопасными резьбовыми коннекторами
- Модульная конструкция позволяет выбрать тип изделия: дисплей, встраиваемый или панельный компьютер
- Серия сертифицирована по нормам:
  2Ex nA ic IIC T4 Gc X, CE / FCC Class A,
  ATEX Zone 2 Ex nA ic IIC T4 Gc, Class I,
  Divizion 2, Group ABCD T4, ANSI / SA 12,12.01-2013
  CSA Std. C22.2 №. 213-1987 / №. 61010



# Зачем нужны промышленные стандарты?

Сергей Солдатов

**Как проверить, что в сложную промышленную систему не установили некачественную деталь? Как не допустить применения не соответствующего отраслевым требованиям оборудования? Как гарантировать совместимость техники разных поставщиков? На подобные вопросы можно дать один ответ: требуйте соответствия стандартам. Зачем они, кто их разрабатывает и как контролируется их выполнение, рассказано в данной статье.**

Каждая отрасль придерживается ряда стандартов, которые гарантируют, что промышленные компоненты производятся единообразно и взаимодействуют без как-либо сложностей. Например, стандарты обеспечивают возможность звонить и получать доступ в сеть Интернет с любого современного мобильного телефона, слушать музыку и смотреть телевизор независимо от производителя аппаратуры. Существует несколько десятков тысяч стандартов, которые затрагивают почти каждый аспект нашей повседневной жизни.

Стандарты, а также другие связанные термины, такие как сертификаты, разрешения, технические регламенты, особенно важны при изготовлении, продаже или использовании определённых компонентов в промышленной сетевой инфраструктуре [1]. Они направлены на то, чтобы различные продукты и компоненты, производимые разными производителями, работали вместе и отвечали определённым экологическим требованиям или требованиям безопасности (рис. 1) – либо для определённого сегмента рынка, либо для определённой страны/региона. В России и ряде стран ближнего зарубежья стандарты могут охватывать не только производство и само изделие, но и документацию, монтаж и ввод в эксплуатацию [2].


Иллюстрация с сайта www.eurasiancommission.org

**Рис. 1. Сферы, регулируемые стандартами**

## Промышленные стандарты – что это?

Стандарты публикуются в документах, в которых устанавливаются спецификации и процедуры, направленные на повышение надёжности продуктов, материалов и услуг. Они могут быть либо нормой, либо требованием и затрагивают широкий круг вопросов, от повышения эффективности продуктов/компонентов до их совместимости и взаимодействия с другими продуктами/компонентами для обеспечения безопасности работников предприятий и конечных потребителей.

Когда производители разрабатывают свои изделия в соответствии с определёнными стандартами, разработка упрощается, а выход на рынок ускоряется. В конечном счёте стандарты стимулируют разработку и внедрение технологий, которые меняют нашу жизнь и работу.

## Как создаются стандарты?

Стандарты разрабатываются различными стандартизирующими организациями, такими как IEEE (Institute of Electrical and Electronics Engineers), IEC (International Electrotechnical Commission) или ISO (International Organization for Standardization), которые оценивают реализуемость и практическую необходимость потенциального стандарта, а затем разрабатывают стандарт [1]. Потом он распространяется по производителям и потребителям и после принятия поддерживается стандартизирующей организацией. Такие организации зачастую являются некоммерческими и негосударственными и существуют на взносы членов и компаний, аккредитованных проводить от имени данных организаций сертификацию.

Стоит отметить, что описанный здесь формат стандарта относится к стандартам *де-юре*, или основанным на консенсусе участников. Это означает, что члены организации по стандартизации пришли к формальному и официальному соглашению по его содержанию. С другой стороны, существуют стандарты *де-факто* – они широко распространены и используются в промышленности без формального процесса рассмотрения, выполняемого организациями по стандартизации. Эти стандарты обычно устанавливаются при активном использовании продуктов или услуг, которые давно вышли на новый рынок, например, формат DVD или раскладка клавиатуры QWERTY.

Стандарты де-факто и де-юре также называют проприетарными и открытыми соответственно. Собственные (де-факто) стандарты, как правило, развиваются из доминирующей технологии, разработанной и используемой одной компанией, например, Microsoft Windows.

Государственные структуры также занимаются стандартизацией и осуществ-

ляют регулирование в области технических стандартов [3]. В России Федеральный закон «О техническом регулировании» от 27.12.2002 № 184-ФЗ является основополагающим нормативным актом, регулирующим права и обязанности субъектов в отношениях, возникающих при разработке, применении и соблюдении требований к продукции, процессам производства, эксплуатации, хранения, перевозки, реализации и утилизации в обязательном порядке и на добровольной основе. Закон устанавливает, что государство берёт на себя обязанность по регулированию безопасности продукции. Это подразумевает контроль её эксплуатационных и потребительских характеристик, причём ответственность за качественную и дизайнерскую составляющую полностью ложится на производителя.

Стоит упомянуть и третий класс стандартов – стандарты предприятия. Эти стандарты могут иногда выходить за пределы традиционных отраслевых стандартов, детализируя некоторые требования, например, условные графические обозначения на мнемосхемах на АРМ и щитах автоматики или требования к маркировке оборудования и кабелей, процедурам пусконаладочных работ, ввода в эксплуатацию. Особенно это характерно для энергогенерирующих и энергопередающих предприятий [4, 5]. Необходимость разработки подобных стандартов объясняется обилием поставщиков для таких предприятий, а также необходимостью обеспечения надлежащего уровня совместимости, технической поддержки и, что ещё важнее, преемственности систем при модернизации.

## Примеры использования стандартов

Как уже было сказано, в мире существует множество различных стандартов. Ряд наиболее известных промышленных стандартизирующих организаций и некоторые их стандарты перечислены в табл. 1.

Далее приведены примеры использования стандартов.

### Стандарт Wi-Fi

Семейство стандартов IEEE 802.11 (часто называется Wi-Fi) является прекрасным примером известного, ориентированного на рынок беспроводных локальных сетей стандарта [1]. Изначально он создавался для соединения беспроводных кассовых аппаратов, но превратился в стандарт, который оценили и другие потребители, большинство из которых пользуются мобильными устройствами.

Wi-Fi является основой беспроводных сетевых приложений по всему миру, он обеспечивает беспроводной доступ в Интернет в офисах и домах, в аэропортах и поездах, на промышленных объектах и заводах (рис. 2), и число устройств, кото-

*Таблица 1*

**Наиболее известные промышленные стандартизирующие организации**

| Организация/название | Задачи организации | Примеры |
|---|---|---|
| **Европейские стандарты (EN)** | Разработка EN. EN – это документы, которые были ратифицированы одной из трёх европейских организаций по стандартизации (ESO): CEN, CENELEC или ETSI | EN 50155 обеспечивает совместимость систем железных дорог и охватывает электронное оборудование, используемое на подвижно́м составе для железнодорожных применений |
| **EtherCAT Technology Group (ETG)** | ETG совместно с производителями устройств EtherCAT, поставщиками и пользователями продвигает технологию EtherCAT и обеспечивает её открытость. ETG является официальным партнёром МЭК | EtherCAT и Safety over EtherCAT – это стандарты IEC (IEC 61158 и IEC 61784) |
| **Международная электротехническая комиссия (МЭК, IEC – International Electrotechnical Commission)** | МЭК является международным стандартизирующим органом по электротехническим продуктам, системам и услугам | IEC 61850-3 позволяет взаимодействовать интеллектуальным электронным устройствам в системах автоматизации электрических подстанций |
| **IEEE (Institute of Electrical and Electronics Engineers)** | IEEE – крупнейшая в мире профессиональная техническая организация, специализирующаяся на продвижении технологий посредством публикаций и конференций, активно занимающаяся внедрением стандартов и ведущая образовательную деятельность | IEEE 802.11 представляет собой набор спецификаций для реализации беспроводных локальных сетей, работающих в нескольких частотных диапазонах |
| **Международная организация по стандартизации (ISO – International Organization for Standardization)** | ISO – это независимая неправительственная международная организация, которая продвигает общепризнанные промышленные и коммерческие стандарты во всём мире. ISO разрабатывает добровольные, основанные на консенсусе участников организации международные стандарты | ISO 14000 – это семейство стандартов по созданию системы экологического менеджмента для минимизации негативного воздействия на окружающую среду |
| **Национальная ассоциация производителей электрооборудования (NEMA – National Electrical Manufacturers Association)** | NEMA является крупнейшей торговой ассоциацией производителей электрооборудования в США. NEMA опубликовала более 600 стандартов, руководств по их применению и технических документов | NEMA TS-2 охватывает оборудование регулирования движения транспорта, используемое для безопасного перемещения пешеходов и движения автотранспорта |
| **ODVA (Open DeviceNet Vendors Association)** | ODVA была основана в 1995 году, это глобальная организация по торговле и стандартизации, членами которой являются поставщики устройств для промышленной автоматизации | ODVA контролирует технологии и стандарты для EtherNet/IP, DeviceNet, CompoNet, ControlNet, Common Industrial Protocol (CIP) |
| **Организация пользователей PROFIBUS (PNO)** | PROFIBUS Nutzerorganisation eV (PROFIBUS User Organization, или PNO) состоит из 25 региональных ассоциаций, включая поставщиков средств автоматизации и услуг, а также конечных пользователей, которые совместно работают над созданием новых стандартов | PNO контролирует сертификаты и стандарты, связанные с PROFINET, PROFIBUS, PROFIsafe, PROFIdrive & Encoder, PROFIenergy, IO-LINK и интеграцией полевых устройств (FDI) |
| **UL (Underwriters Laboratories)** | UL – глобальная независимая научная компания в области безопасности, которая разработала более 1500 стандартов. Стандарты UL охватывают дизайн, производство, маркетинг и покупку товаров, решений и инноваций | Стандарт UL 60950-1 применим к информационно-технологическому оборудованию, предназначенному для использования в качестве телекоммуникационного оконечного оборудования и средств сетевой инфраструктуры, с целью снижения риска получения травмы или повреждения |

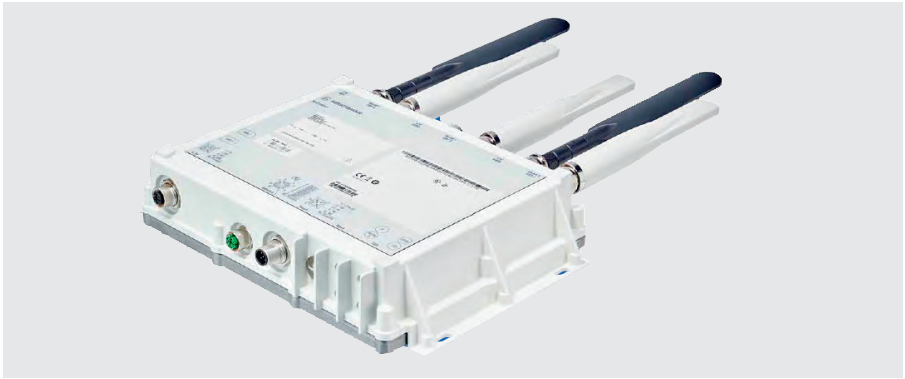


Рис. 2. Промышленная Wi-Fi-точка доступа Hirschmann BAT450-F

Рис. 3. Кабель Belden серии MarineTuff для морского и судового применения

рые подключены по беспроводной связи, быстро растёт. Значимость стандарта существенно возросла с появлением новых приложений, таких как интеллектуальные сети и системы мониторинга состояния беспроводной сети.

## Сертифицированные кабели для морского и судового применения

Активное бурение морского шельфа для добычи нефти и газа в глубоководных районах моря потребовало создания новых кабелей, которые смогли бы обеспечивать электропитание и контроль глубоководного оборудования. Компания Belden специально для этих целей разработала безгалогеновые мало дымящие кабели MarineTuff (рис. 3), способные противостоять жёстким условиям эксплуатации на самых суровых морских глубинах [6].

Для подтверждения исключительных характеристик кабели прошли сертификацию более чем по десяти стандартам: ABS (American Bureau of Shipping), IEEE 45, IEEE 1580, IEC 60092-350, UL 2225, UL 1277 TC-ER и др. Осуществив такую обширную сертификацию, производитель избавил заказчиков от необходимости сертифицировать каждую закупку.

Стоит отметить, что указанные кабели подходят как для прокладки внутри морского судна, так и снаружи. А для повышения уверенности заказчиков Belden предлагает 10-летнюю гарантию на данные кабели.

## Автоматические транспортировочные роботы

Современное автомобильное производство должно обеспечивать высокое качество продукции и в то же время учитывать потребности конкретного клиента [7]. Один из способов решения – использование автоматических транспортных систем/роботов на предприятии (AGVs – Automated Guided Vehicles), рис. 4. Для эффективной работы такие системы должны строиться с использованием беспроводных сетей стандарта 802.11n/ac, использовать стандартные промышленные протоколы PROFINET, EtherNet/IP, IO-Link, EtherCAT и др.

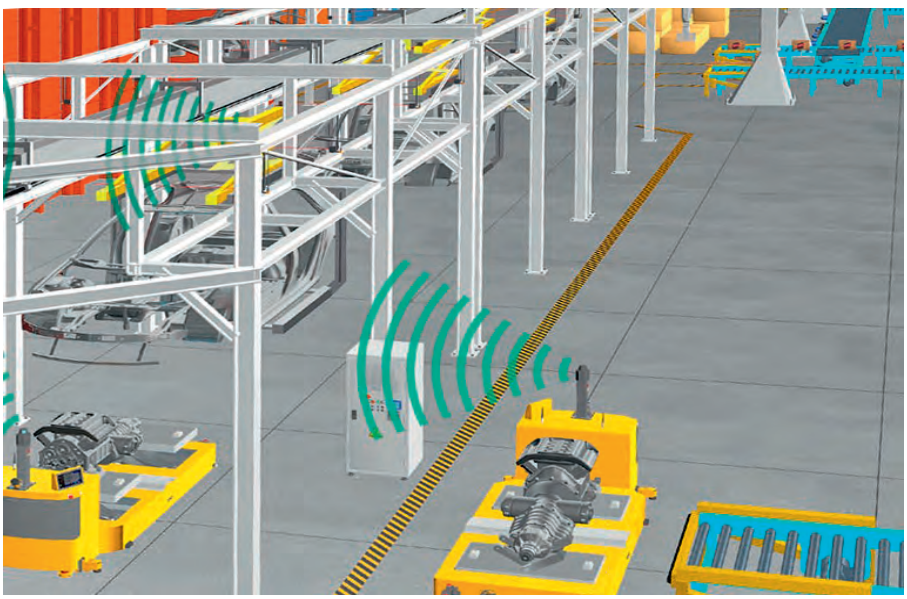


Рис. 4. Автоматическая транспортная система с беспроводной связью

Для обеспечения безопасности персонала на предприятиях должна использоваться только сертифицированная кабельная продукция, например, фирмы Belden, а с учётом высокой подвижности манипуляторов современных роботов данные кабели обязаны сохранять работоспособность при большом количестве деформаций.

Таким образом, эффективность и качество современного автомобильного производства напрямую зависят от использования сертифицированных и стандартизированных компонентов.

## Упаковка продуктов питания

Все уже привыкли покупать продукты питания не на развес, а в красочных упаковках, с конкретным объёмом и весом. Но для того чтобы упаковать продукты, необходима слаженная работа множества машин и промышленных компонентов. Рассмотрим один из них – соединители и распределительные коробки (рис. 5). Многие производители, в частности, компания Belden, производят соединители и распределительные коробки, сертифицированные для использования на пищевом производстве [8]. Специфика пищевых производств – обилие различных пищевых химических веществ (например уксус), экстремально низкие или высокие температуры, пыль от измельчённых продуктов и многое другое. Сертифицированные компоненты должны

Рис. 5. Кабели со смонтированными разъёмами для пищевых производств

# Анализ технологических показателей в реальном времени

## Решения на базе программных продуктов ICONICS

## ЧТО?

- Управление эксплуатацией оборудования
- Снижение затрат
- Энергоменеджмент

## КАК?

- Диагностика состояния оборудования с возможностью прогнозирования сбоев. Учёт наработки, экспертные карты, вероятностный анализ
- Анализ нештатных режимов. Частота возникновения, поиск взаимосвязи, анализ времени реакции персонала
- Анализ потребления энергоресурсов. Данные о потреблении в реальном времени, сравнение с идеальной моделью и плановыми показателями, сравнение с историческими данными, индикаторы энергоэффективности. Поддержка анализа в рамках энергоменеджмента по ГОСТ 50001:2011

ICONICS

PortalWorX Productivity Analytics Facility AnalytiX Energy AnalytiX Alarm Analytics

НОРВИКС ТЕХНОЛОДЖИ

Тел.: +7 (495) 232-1817
Факс: +7 (495) 232-1649
Эл. почта: info@norvix.ru

Официальный партнёр компании ПРОСОФТ
www.norvix.ru

переносить все негативные воздействия и не выделять в процессе своей эксплуатации вредных для человека веществ.

## Каким критериям должны удовлетворять сертифицируемые компоненты?

Сертификаты на компоненты требуются для многих критичных или уязвимых применений, что особенно актуально для промышленности [1]. В частности, есть ряд жёстко регулируемых отраслей: транспорт, энергетика и промышленное производство. Чтобы получить сертификат для использования в этих отраслях, обычно выполняются следующие шаги:

1) тестирование продукта в реальных приложениях;
2) оценка результатов теста по полученным данным;
3) решение о том, должен ли продукт получать сертификат;
4) продолжение оценки продукта, чтобы он соответствовал заданным критериям, а затем периодическая сертификация по мере необходимости.

Таким образом, сертификация – это не разовая процедура, а постоянный процесс, выполняемый в течение всего жизненного цикла компонента. Только так можно гарантировать заказчику, что изделие независимо от даты производства будет иметь надлежащее качество.

## Кто сертифицирует промышленные продукты?

Одной из лидирующих и самых результативных сертифицирующих компаний является UL (Underwriters Laboratories) [1]. Коммерческое и промышленное подразделение UL обеспечивает сопровождение продукта совместно с производителями на протяжении всего жизненного цикла, начиная с разработки продукта и далее, включая создание прототипа, функциональное тестирование, сертификацию и заканчивая инспекцией предприятия, с периодическими аудитами и постоянным контролем в полевых условиях.

Такие сертифицирующие компании, как UL, выявляют проблемы, определяют потребности производителей и помогают снизить риски. Когда потребитель видит, что продукты и услуги сертифицированы, он может быть уверенным, что они были разработаны в соответствии или даже с превышением требований конкретных отраслевых стандартов.

## Стандартизация и выход на международный рынок

Ещё одним важным моментом является обеспечение того, чтобы технологический процесс и инфраструктура производства соответствовали требованиям любой страны, в которой производитель будет работать. Многие страны или регионы имеют свои собственные очень строгие нормативы и положения. Международные компании, которые работают сразу в нескольких странах, должны уделить вопросу стандартизации особое внимание, чтобы решить его эффективно, просто и экономично. В случае выполнения стандартов определённого региона на изделие наносится соответствующая маркировка. Например, в Европе от производителя может потребоваться маркировка CE или сертификация DNV GL, и компания должна её обеспечить. В странах Евразийского экономического союза, куда входит и Россия, требуется выполнение собственных технических регламентов, соответствующие им продукты маркируются знаком EAC.

## Вывод

Стандарты, сертификаты и технические регламенты помогают обеспечить совместимость промышленных компонентов, а также их безопасность и надёжность.

Прежде чем выбирать какие-либо промышленные сети или решения для подключения к ним, заказчик или интегратор должны ответить на ряд вопросов.

- Какие стандарты нужно учитывать или каких нужно придерживаться? Каковы плюсы и минусы открытых или проприетарных стандартов, как на краткосрочную, так и на долгосрочную перспективу?
- Какие сертификаты необходимы для продуктов и решений, которые закупаются/интегрируются? Для каких случаев использования, условий окружающей среды и т.п. они сертифицированы?
- Где будут использоваться компоненты или решения? Какие сертификаты и разрешения нужны для обеспечения норм и стандартов или подачи документов для получения разрешения на использование продуктов в конкретных приложениях или выхода на рынок?

Стандарты, сертификаты и разрешения являются частью одного и того же процесса, направленного на обеспечение должного уровня производительности и совместимости, как у потребителей, так и у производителей. ●

## Литература


1. Chris Long. A Guide to Industrial Standards, Certifications and Approvals [Электронный ресурс] // Режим доступа : https://www.belden.com/blog/industrial-ethernet/a-guide-to-industrial-standards-certifications-and-approvals?hsCtaTracking=a4d6a87d-ecd3-4dab-9a84-05d91e81984b|012aea2a-96c7-4bbd-b8cc-fa66d0640521et/a-guide-to-industrial-standards-certifications-and-approvals?hsCtaTracking=a4d6a87d-ecd3-4dab-9a84-05d91e81984b|012aea2a-96c7-4bbd-b8cc-fa66d0640521.
2. Техническое регулирование и стандартизация [Электронный ресурс] // Режим доступа : http://www.eurasiancommission.org/ru/act/texnreg/deptexreg/tr/Pages/default.aspx.
3. Техническое регулирование [Электронный ресурс] // Режим доступа : http://www.cntd.ru/tehnicheskoe_regulirovanie.html.
4. Стандарт организации ОАО «ФСК ЕЭС» : СТО 56947007-29.130.20.104-2011. Типовые технические требования к КРУ классов напряжения 6–35 кВ [Электронный ресурс] // Режим доступа : http://www.fsk-ees.ru/upload/docs/47-26_sto_56947007-29.130.20.104-2011_izm.pdf.
5. Техническая политика ОАО «МРСК Центра» [Электронный ресурс] //Режим доступа : https://www.mrsk-1.ru/docs/tech_politic.pdf.
6. MarineTuff™ Certified Belden® Instrumentation, Control and VFD Cables [Электронный ресурс] // Режим доступа : https://www.belden.com/hubfs/resources/technical/solution-brochures/marinetuff-certified-belden-instrumentation-control-and-vfd-cables-capabilities-bulletin.pdf.
7. Automotive Manufacturing – Communication Systems for Shop Floor Application [Электронный ресурс] // Режим доступа : https://info.belden.com/hubfs/resources/technical/solution-brochures/automotive-manufacturing-communication-systems-for-shop-floor-application.pdf.
8. Line Card – Food and Beverage [Электронный ресурс] // Режим доступа : http://info.belden.com/hubfs/resources/technical/solution-brochures/food-and-beverage-line-card.pdf.

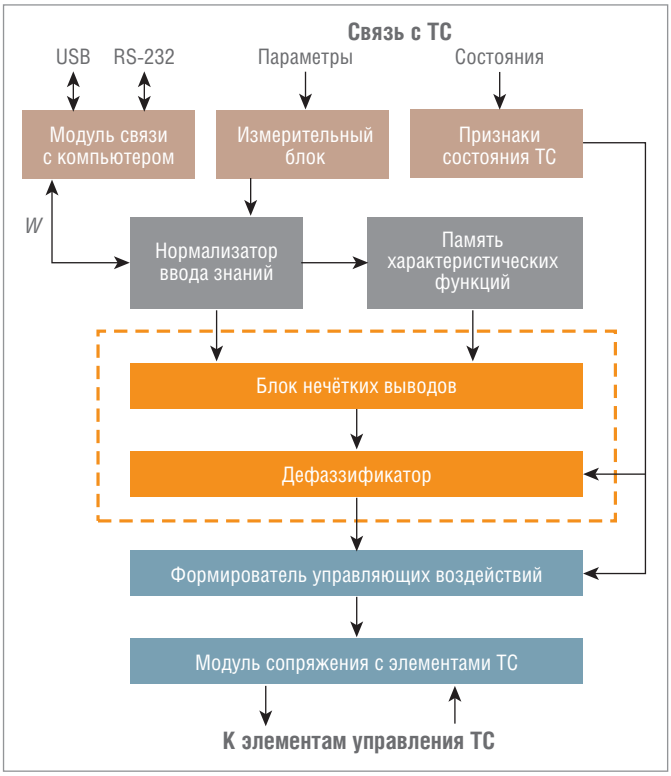

**E-mail: ssa-company@mail.ru**

Александр Клевцов, Данила Зимогляд

# Основы структурно-функциональной организации встроенных и автономных нечётких систем управления

При решении задач оптимизации потребления электроэнергии (ЗОПЭ) структурно-функциональное построение нечётких систем управления (НСУ) исходит из конкретных условий потребления электроэнергии и принципов функционирования определённой технической системы, будь то компрессорная или насосная станция, устройство преобразования электроэнергии, система питания, мощное пусковое устройство или статический компенсатор реактивной мощности. К основным аспектам работы при определении структуры и функций НСУ следует отнести:

- детальный анализ принципа функционирования технической системы, потребляющей электроэнергию;
- изучение технологической задачи, реализуемой с помощью данной технической системы;
- определение возможности реального снижения электропотребления за счёт оптимизации режимов работы электрооборудования без ухудшения выходных параметров;
- проведение сравнительной комплексной оценки реализации решения ЗОПЭ с помощью традиционных алгоритмов управления, основанных на построении чётких структур: экстремальное или адаптивное управление, прямой поиск и т.д.;
- определение возможности решения ЗОПЭ на основе располагаемых аппаратно-программных ресурсов управляющей системы, находящейся в эксплуатации;
- разработка структуры и функций встраиваемой или автономной НСУ в случае отсутствия возможности реализации в рамках существующей архитектуры аппаратно-программных средств.




**Условные обозначения:** *W* – канал ввода знаний (нечёткой информации); ТС – техническая система.

**Рис. 1. Обобщённая структурная схема нечёткой системы управления**

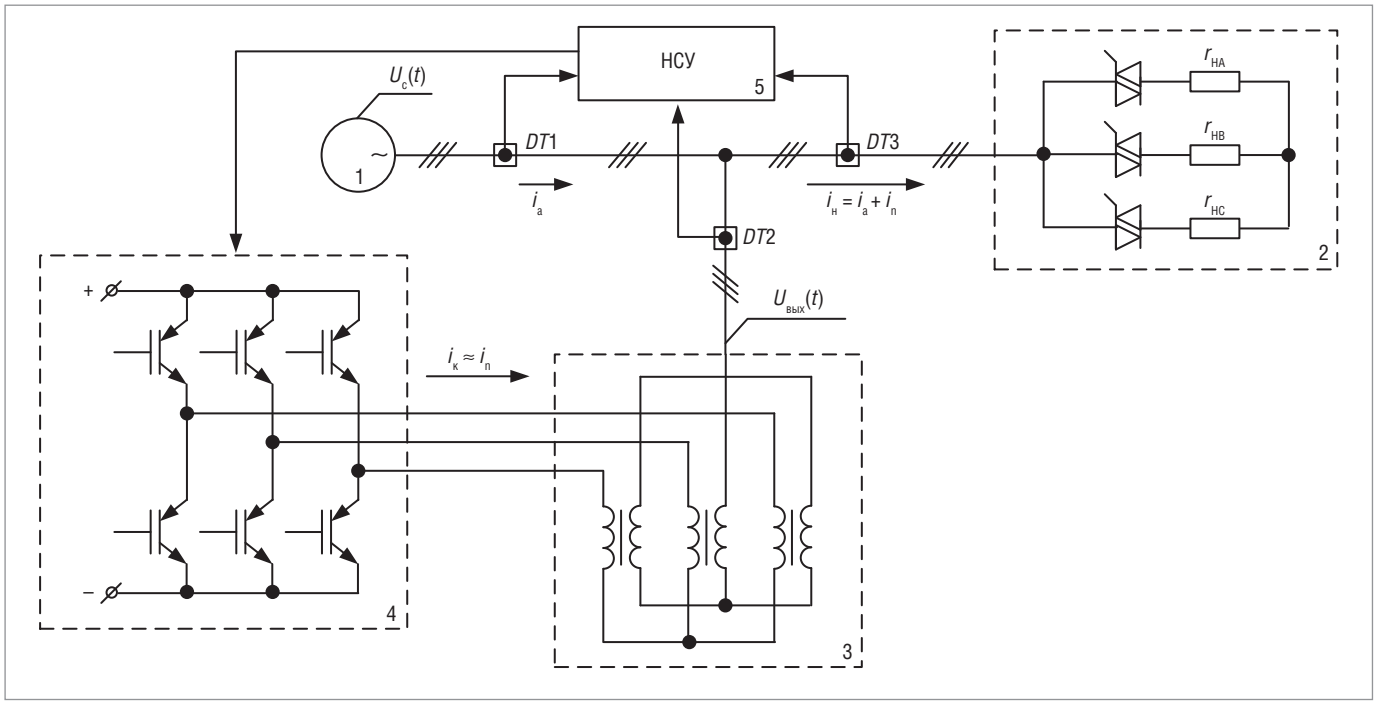
Информационной базой для проведения последней работы должен послужить свод продукционных правил, разработанных для конкретной задачи оптимизации потребления электроэнергии.

На рис. 1 представлена обобщённая структурная схема нечёткой системы управления, отдельные блоки которой, в зависимости от характера взаимодействия с элементами технической системы, могут быть представлены многообразными вариантами исполнения.

В плане реализации измерительный блок является устройством сбора и согласования сигналов различных типов, включая термопары, аналоговые сигналы в диапазоне ±10 В с одновременной оцифровкой. Примечательным и коренным отличием от логического или вычислительного устройства, предназначенного для выполнения программы чёткого (детерминированного) управления, является наличие в структуре НСУ блока нечётких выводов и дефаззификатора (от англ.”defuzzification” – формирователя управляющего воздействия по конечному результату нечёткого вывода).

## Статические компенсаторы неактивных составляющих

Рассмотрим функционально-алгоритмическое построение средств оптимизации потребления электроэнергии на примере нечёткого управления статическим компенсатором неактивных составляющих мощности с полной компенсацией гармонических составляющих тока нагрузки. Известно, что желаемой формой потребляемого тока для силовой трёхфазной сети (ТС) переменного тока является синусоидальная, когда коэффициент мощности любой ТС будет максимально приближен к единице, что даст возможность сэкономить на эксплуатационных затратах и повысить энергетические показатели. В связи со стремительным развитием силовой электроники перспективными устройствами для решения данной




**Условные обозначения:** 1 – питающая система; 2 – электротехническая установка; 3 – блок развязывающих трансформаторов; 4 – компенсационный источник напряжения; 5 – нечёткая система управления; $U_с$ – напряжение питающей сети; $U_{вых}$ – выходное напряжение источника питания; $i_а$ – активная составляющая тока нагрузки; $i_к$ – компенсационный ток; $i_п$ – пассивная составляющая тока нагрузки; $i_н$ – ток нагрузки; $r_{НА}$, $r_{НВ}$, $r_{НС}$ – сопротивление электротехнической установки по каждой фазе; *DT*1, *DT*2, *DT*3 – датчики тока

**Рис. 2. Структурная схема статического компенсатора неактивных составляющих**

задачи становятся статические компенсаторы неактивных составляющих (СКНС).

На рис. 2 приведён вариант упрощённой структурной схемы СКНС. Питающая система 1 нагружена электротехнической установкой 2, например, трёхфазным регулятором мощности. Выход компенсатора 4, представляющего собой мостовой трёхфазный инвертор на IGBT-транзисторах, включается через развязочные (разделительные) трансформаторы 3 параллельно между питающей сетью и нагрузкой. Информация о мгновенных значениях тока нагрузки $i_н$, компенсационного тока $i_к$, тока питающей сети $i_а$ с помощью датчиков тока *DT*1, *DT*2, *DT*3 поступает в НСУ. Электромагнитные процессы в этой схеме отражает дифференциальное уравнение:

$$u_с(t) = u_{вых}(t) - L\frac{di_к}{dt},$$

где $u_с(t)$ – мгновенное значение напряжения питающей сети; $u_{вых}(t)$ – мгновенное выходное напряжение компенсационного источника питания 4.

Ток нагрузки состоит из активной составляющей тока нагрузки и пассивной составляющей, представляющей ток гармонических составляющих, который может определяться [1] как:

$$i_п(t) = i_н(t) - i_а(t) = i_н(t) - \frac{S_н}{U_с^2}u_с(t)\cos\varphi_н = i_н(t) - \frac{P_н}{U_с^2}u_с(t),$$

где $U_с$ – действующее значение напряжения сети, $P_н$ – активная мощность нагрузки.

Условием полной компенсации пассивной составляющей тока нагрузки $i_п(t)$ является:

$$i_к(t) = -i_п(t).$$

Тогда

$$u_{вых}(t) = L\frac{di_н(t)}{dt} + L\frac{P_н du_с(t)}{U_с^2 dt} + u_с(t).$$

Данное выражение и определяет напряжение компенсационного источника, при котором обеспечивается требуемое значение компенсационного тока при заданных параметрах силовой схемы: активной мощности нагрузки $P_н$, действующего напряжения сети $U_с$, индуктивности вторичной обмотки разделительного трансформатора $L$.

## Решение задачи компенсации неактивных составляющих с использованием алгоритма нечёткого управления

Если в реальном времени производить вычисление выходного напряжения $u_{вых}(t)$ и формировать аналоговый сигнал управления ШИМ-модулятора, то для этого потребуются значительные вычислительные ресурсы, что и определяет высокую цену.

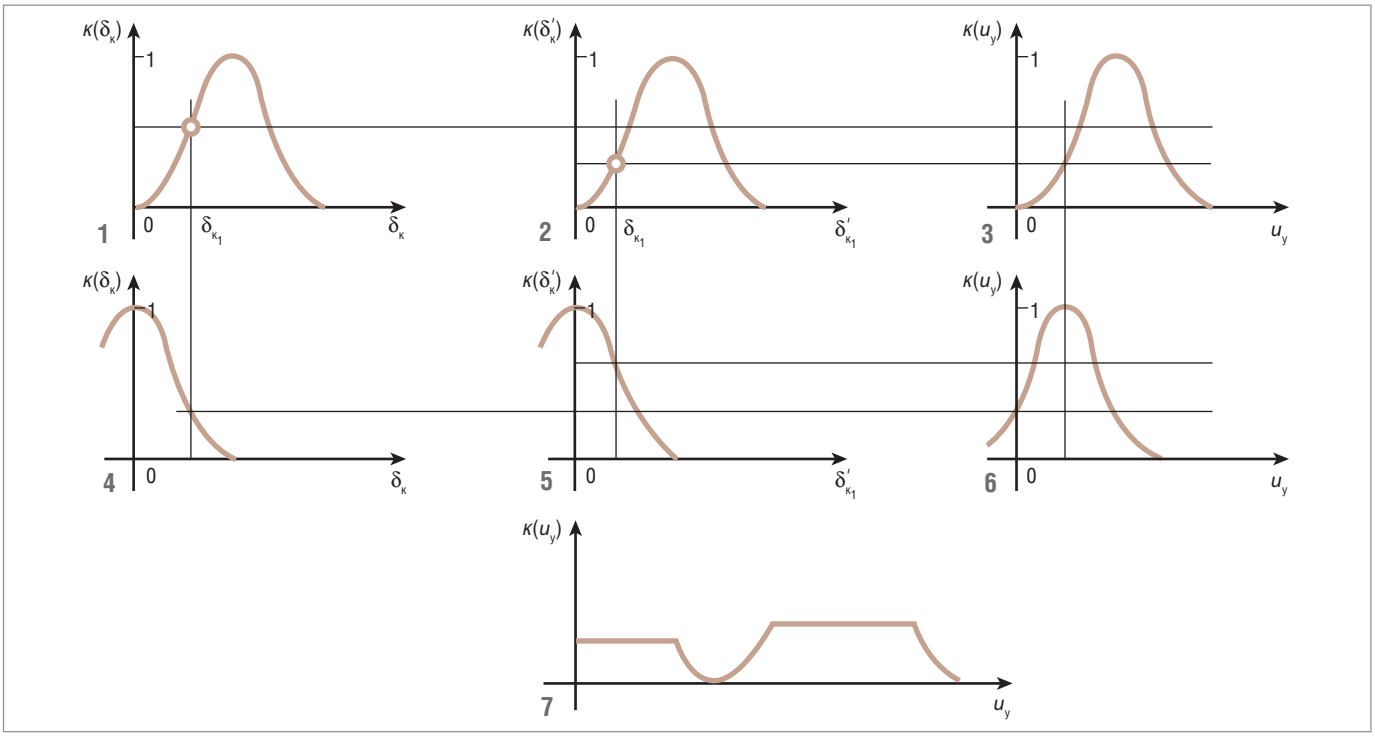
Как будет выглядеть решение с использованием алгоритма нечёткого управления?

Переменной, характеризующей состояние системы, является значение пассивной составляющей $i_п$, которое определяется НСУ в каждом цикле, исходя из измеренных текущих значений тока нагрузки $i_н$ и напряжения сети $U_с$. Для управления выходным напряжением $u_{вых}(t)$ компенсационного источника НСУ используются значения ошибки компенсации $\delta_к = i_к - i_п$ и производной $\delta'_к$.

Уровень активной мощности нагрузки $P_н$ также определяется в каждом цикле по замеренным мгновенным значениям напряжения сети $U_с$ и тока нагрузки $i_н$.

В данном случае просматриваются два правила:

- если ошибка $\delta_к$ и её производная $\delta'_к$ не равны нулю, то управляющий сигнал $u_у$ в компенсационном источнике также не равен нулю, то есть, если $\delta_к \neq 0$ и $\delta'_к \neq 0$, то $u_у \neq 0$;
- если ошибка $\delta_к$ и её производная $\delta'_к$ равны нулю, то управляющий сигнал $u_у$ в компенсационном источнике также равен нулю, то есть, если $\delta_к = 0$ и $\delta'_к = 0$, то $u_у = 0$.




Условные обозначения: $u_у$ – управляющий сигнал; $\delta_к$ – ошибка компенсации; $\delta'_к$ – производная ошибки компенсации; $\kappa(\delta_к)$ – относительное значение функции принадлежности ошибки компенсации; $\kappa(\delta_к)$ – относительное значение функции принадлежности производной ошибки компенсации; $\kappa(u_у)$ – относительное значение функции принадлежности управляющего напряжения $u_у$.

**Рис. 3. Иллюстрация формирования нечёткого вывода: 1…7 – фазы формирования вывода**

На рис. 3 показана примерная иллюстрация формирования нечёткого вывода по алгоритму Мамдани [1]. В данном примере использована типовая форма функции принадлежности – гауссовская (gaussmf), причём каждая из входных величин ($\delta_к$, $\delta'_к$) представлена набором функций принадлежности, перекрывающих их возможный диапазон изменений (рис. 4).

По конкретному значению ошибки $\delta_к$, измеренной в цикле, сделаны два частных вывода (см. графики 3 и 6 на рис. 3), по которым сформирован окончательный нечёткий вывод для данного момента времени. Вывод получен по ранее упомянутому в [1] принципу MIN-MAX: выход на нечёткое множество каждого правила «обрезается», затем «обрезанные» выходные функции (графики 3 и 6 на рис. 3) объединяются операцией максимума (график 7 на рис. 3). Операция дефаззификации (получение конкретного значения) управляющего напряжения для компенсационного источника определяется НСУ любым из известных методов [2], например, центроидным или наибольшего максимума (LOM – Largest of Maximums).

Очевидно, что требования к аппаратным ресурсам НСУ для управления источником компенсационного напряжения в основном сосредоточены в измерительных возможностях микроконтроллера и в наличии сравнительно небольшой энергонезависимой памяти, необходимой для хранения дискретного представления функций принадлежности с определённым шагом квантования.

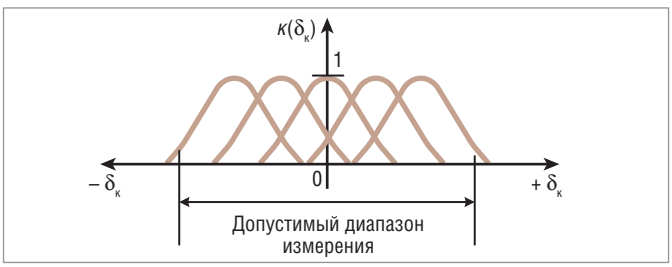
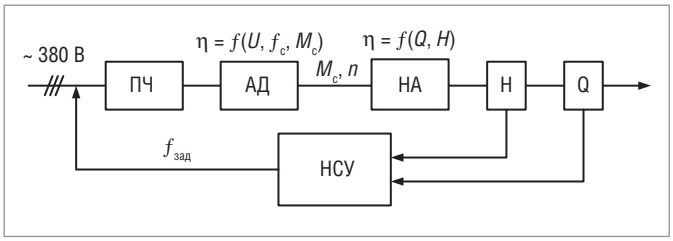



**Рис. 4. Набор функций принадлежности $\kappa(\delta_к)$ в допустимом диапазоне измерений: $\delta_к$ – ошибка компенсации**

## Увеличение КПД электрооборудования за счёт нечёткого управления

В настоящее время существуют комплексные системы экстремального управления, позволяющие производить в реальном времени поиск рабочей точки с максимальным КПД насоса при минимуме суммарных потерь энергии в электроприводе и поддержании требуемой постоянной производительности. При их реализации часто не учитывалось то обстоятельство, что работа при максимальном КПД насоса не всегда сопровождается минимальными потерями в электроприводе. Кроме этого, важной особенностью таких систем является то, что для обеспечения их работоспособности необходимо постоянное согласование шагов и амплитуд поиска минимальных потерь в двигателе ($\Delta t$, $\Delta U$ – шаг времени и выходного напряжения источника питания соответственно) и максимума КПД ($\Delta h$, $\Delta f_с$ – шаг изменения напора и частоты напряжения сети соответственно). При этом контур поиска максимума КПД должен адаптироваться к колебаниям частоты вращения электродвигателя в окрестностях точки минимальных потерь при условии непрерывного изменения. В этом случае техническая реализация такого двухконтурного регулятора не может быть простой и по стоимости будет составлять достаточно весомую часть в общем балансе затрат на создание технических средств управления насосными агрегатами.

В качестве альтернативы рассмотрим вариант системы на базе нечёткого алгоритма оптимизации, в основе которого сочетание возможностей встроенной в преобразователь частоты (ПЧ) функции оптимизации потерь в приводном асинхронном двигателе (АД) и нечёткого регулятора КПД насоса (рис. 5).




**Условные обозначения:** ПЧ – преобразователь частоты; АД – асинхронный электродвигатель привода насосного агрегата; НА – насосный агрегат; Н – датчик напора; Q – датчик производительности; НСУ – контроллер нечёткой системы управления; $f_{зад}$ – заданная частота сети; $f_c$ – частота сети; $U$ – напряжение питания; $M_c$ – статический момент на валу; $n$ – число оборотов вала электродвигателя в минуту; η – КПД.

**Рис. 5. Вариант структурной схемы организации нечёткого управления насосным агрегатом**

Задачей системы является обеспечение максимально возможного КПД насосной установки при условиях обеспечения минимальных потерь в АД и поддержания необходимой производительности.

При соответствующей инициализации ПЧ и включении штатной функции энергосберегающего управления с момента ввода в работу встроенный контроллер ПЧ производит оценку мощности нагрузки на валу АД и в случае её изменения управляет выходным напряжением $U_{АД}$ таким образом, что обеспечивается только требуемая мощность потребления электроэнергии при частоте $f_{зад}$ (рис. 5). В то же время контроллер нечёткой системы управления производит в соответствии с алгоритмом нечёткого управления пошаговую корректировку уровня задания частоты вращения АД ($f_{зад}$) таким образом, чтобы рабочая точка соответствовала максимальному КПД насоса с минимальным потреблением электроэнергии при требуемой постоянной производительности.

Алгоритм основан на анализе и выборе в реальном времени оптимального сочетания характеристик и физических параметров, характеризующих режим работы насосного агрегата: напор, производительность, зависимость КПД от гидравлического сопротивления. При этом в полной мере используются возможности функции энергосберегающего управления промышленных преобразователей частоты насосных серий.

## Выводы

На сегодняшний день для оптимизации потребления электроэнергии весьма перспективны решения, основанные на совместном использовании энергосберегающих функций типового промышленного оборудования (преобразователей частоты, устройств плавного пуска, управляющих средств различных технологических комплексов и т.д.) и возможностей автономных специальных устройств, реализующих алгоритмы нечёткого управления [3, 4]. В качестве автономных НСУ могут применяться бюджетные встраиваемые промышленные платформы на базе широко используемых в настоящее время различных серий микроконтроллеров (STM32, Pic, Atmel и т.д.), сочетающих достаточно высокую производительность, функциональность, низкое энергопотребление с относительно низкой ценой. Не исключается применение практически любого программируемого логического контроллера, обладающего достаточными аппаратно-программными ресурсами и соответствующей конфигурацией. За последние 10 лет ООО «НПП «АКИС» реализован ряд проектов по снижению потребления электроэнергии на основе использования НСУ в различных отраслях промышленного производства, с которыми можно ознакомиться на сайте компании «АКИС». ●

## Литература

1. Клевцов А.В. Оптимизация потребления электроэнергии. – М. : Перо, 2015.
2. Клевцов А.В. Основы рационального потребления электроэнергии: учеб. пособие. – М. : Инфра-Инженерия, 2017.
3. Клевцов А. Системы нечёткого управления уровнем потребления электроэнергии в промышленном оборудовании // Современные технологии автоматизации. – 2018. – № 1.
4. Клевцов А., Зимогляд Д. Методы создания продукционных правил оптимизации потребления электроэнергии // Современные технологии автоматизации. – 2018. – № 2.

**E-mail: akis_tula@inbox.ru**

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

## Встретимся в Москве: определена тематика осенней выставки «Передовые Технологии Автоматизации – 2018»

*17–19 октября 2018 года в рамках Российской недели электроники и автоматизации свои экспозиции впервые объединят знаковые отраслевые мероприятия – выставки ChipExpo и «ПТА» («Передовые Технологии Автоматизации»), в павильоне «Форум» центрального выставочного комплекса «ЭКСПОЦЕНТР».*

В этом году деловая программа мероприятия ещё глубже раскроет самые насущные и острые вопросы автоматизации промышленности с помощью IIoT-технологий, робототехники, облачных сервисов. Вот круг тем, который будет охвачен докладчиками – ведущими специалистами компаний, занятых разработкой, производством и дистрибуцией новейшего оборудования и программного обеспечения для АСУ ТП и встраиваемых систем:

- кибербезопасность на промышленном предприятии;
- промышленный Интернет вещей (IIoT);
- промышленная автоматизация на пути к Industry 4.0;
- встраиваемые системы.

В рамках деловой программы запланирована дискуссия между докладчиками и приглашёнными ключевыми экспертами рынка об интересующих всех вопросах развития отрасли, вызовах и возможностях, которые сулит эпоха Industry 4.0.

Свои технологии и решения для всех уровней промышленной автоматизации ведущие компании рынка представят в следующих разделах:

- автоматизация промышленного предприятия;
- автоматизация технологических процессов;
- бортовые и встраиваемые системы;
- измерительные технологии;
- робототехника и мехатроника;
- облака, IoT, Big Data в промышленности.

Экспозиция будет сформирована с учётом тематики деловой программы, чтобы гости «ПТА» получили комплексное представление о заинтересовавших их продуктах и решениях и ответы на все возникшие вопросы.

Также в этом году вновь будет предоставлена возможность поучаствовать в технологических турах – специализированных тематических экскурсиях на стенды компаний-участниц. ●

Нина Кузьмина

# Реализация TCP- и UDP-сокетов на контроллере FASTWEL CPM723-01 в среде разработки CODESYS V3

## Введение

В распределённых системах управления обмен данными является одним из ключевых моментов работы системы.

Новый контроллер модульной линейки FASTWEL I/O CPM723-01 (рис. 1) позволяет отправлять и получать данные по промышленному протоколу Modbus TCP на базе протокола TCP/IP с использованием двух портов Ethernet и по протоколу Modbus RTU/ACSII на базе последовательных сетей RS-485/RS-232 с помощью коммуникационных модулей NIM741/NIM742. Кроме того, система исполнения контроллера CPM723-01 поддерживает механизм сетевого обмена данными между контроллерами, принадлежащими одной подсети, средствами специального протокола прикладного уровня CODESYS V3 [1]. Но иногда возникает необходимость использования протоколов низкого уровня, которые позволяют обмениваться большим количеством сообщений между различными устройствами с помощью стека TCP/IP. Также на базе данного стека можно создавать протоколы более высокого уровня модели OSI (рис. 2) [2].

TCP/IP основывается на соединениях, устанавливаемых между двумя устройствами, обычно называемыми *клиентом* и *сервером*. Взаимодействие между устройствами в рамках стека TCP/IP осуществляется с помощью связки IP-адреса и порта. Пара адрес и порт образует *сокет* (от английского socket – «гнездо») [3]. Сокет является программным интерфейсом, который обеспечивает обмен данными между устройствами на низком уровне (рис. 3). Различают сокет клиента и сокет сервера.

Рис. 1. Новый контроллер модульной линейки FASTWEL I/O CPM723-01

Для протокола версии IPv4 IP-адреса записываются в 32-битной форме, представляемой в виде mmm.nnn.ppp.qqq – адрес, разбитый на четыре поля, разделённых точками, по одному байту в поле, например, 192.168.102.101 [2]. Номер порта задаётся в диапазоне от 0 до 65535.


Рис. 2. Пример протоколов стека TCP/IP в соответствии с моделью OSI

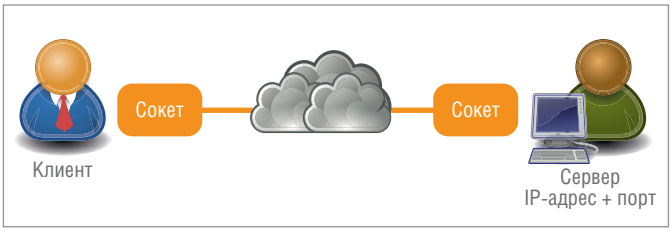



Рис. 3. Общение с помощью сокетов

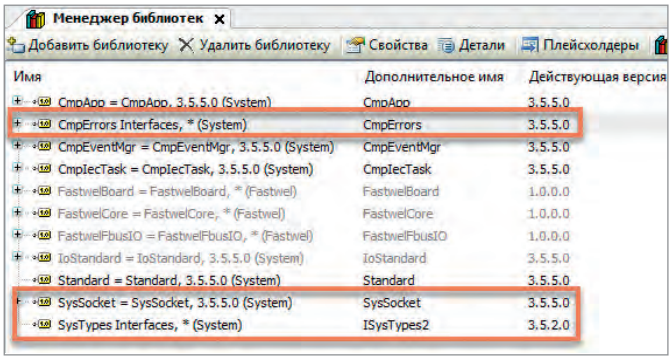



Рис. 4. Библиотеки CODESYS V3, используемые для реализации сокетов

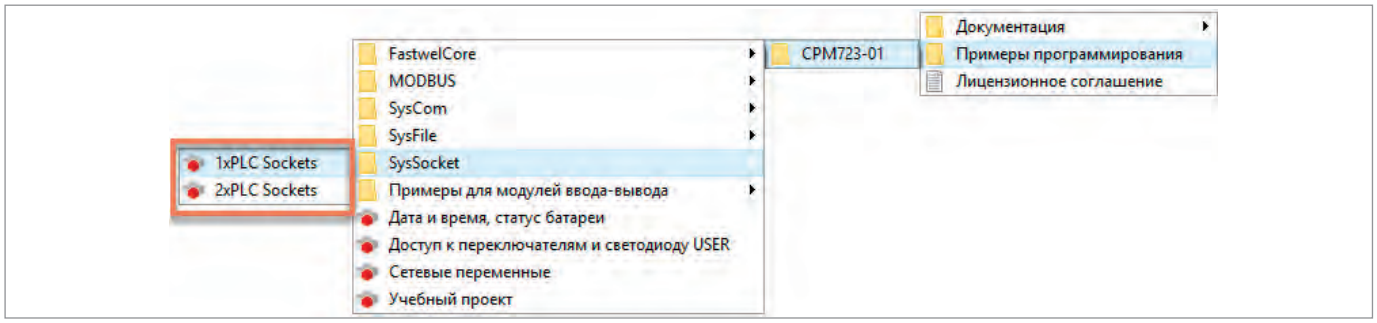



**Рис. 5. Примеры для библиотеки SysSocket на базе контроллера CPM723-01**

Для организации общения клиент должен знать IP-адрес и номер порта сервера, по которым он подключается к удалённому устройству. В рамках стека протоколов TCP/IP различают два типа сокетов – TCP и UDP [4]. Также TCP-сокеты называют *потоковыми*, а UDP – *датаграммными*.

## Реализация сокетов в CODESYS V3

### Системные библиотеки

Реализовать работу TCP- и UDP-сокетов на базе контроллера CPM723-01 можно с помощью системной библиотеки *SysSocket*. Эта библиотека включена в комплект поставки среды разработки CODESYS V3 и позволяет создавать сокеты на всех устройствах, поддерживающих данную платформу (рис. 4).

В качестве дополнительных библиотек в проект должны быть включены *CmpErrors* и *ISysTypes2 Interfaces* (рис. 4).

Библиотека *ISysTypes2 Interfaces* необходима для создания системных идентификаторов *hServer* и *hClient*, представленных типом *RTS_IEC_HANDLE*. Кроме того, некоторые функции *SysSocket* возвращают результат (переменная *result*) в виде кодов ошибок, представленных типом *RTS_IEC_RESULT*, которые также декларированы в системной библиотеке *ISysTypes2 Interfaces*.

Тип *RTS_IEC_RESULT* предназначен для передачи приложению кода ошибки вызова системной функции. Перечень кодов ошибок находится в библиотеке *CmpErrors* в списке констант *Errors*.

### Пример сокетов для CPM723-01

Текущая версия пакета адаптации CODESYS V3 для контроллеров FASTWEL 1.0.1.0 (от 29.12.2017) содержит готовые примеры программирования для библиотеки SysSocket (рис. 5): проект для одного контроллера и для двух контроллеров для TCP- и UDP-сокетов, в которых можно посмотреть полностью реализованный код для контроллера. Также готовые примеры реализации сокетов для контроллера CPM723-01 и CODESYS V3 можно скачать по ссылке: ftp://ftp.prosoft.ru/pub/Hardware/Fastwel/Fastwel_IO/AppNotes/AN-0001/.

### TCP-сокеты

TCP-сокеты используют TCP-соединения, в которых на транспортном уровне (рис. 2) обеспечивается надёжная доставка данных. TCP-протокол отвечает за установление и поддержание соединения, сегментацию, доставку и буферизацию данных, упорядочивание и избавление от дублированных TCP-сегментов данных, контроль ошибок и скорости передачи данных [5]. Схема работы простого TCP-сокета [6] представлена на рис. 6.

В процессе обмена данными с помощью сокетов участвуют две стороны: сервер и клиент. Рассмотрим вначале работу серверного TCP-сокета. На рис. 6 слева представлена блок-схема работы простого серверного TCP-сокета. Для удобства использованы функции из библиотеки *SysSocket* среды разработки CODESYS V3.

**Серверный TCP-сокет**

При старте программы, отвечающей за управление сервером, вначале происходит инициализация сокета. Данный процесс осуществляется один раз.

С помощью функции *SysSockCreate()* создаётся системный идентификатор («хэндл» – от английского handle) сокета. Данная функция в качестве входных параметров принимает аргументы, задающие тип и протокол сокета. Для использования TCP-протокола функция *SysSockCreate()* должна получить входные аргументы, как показано в листинге 1.

Далее сокет сервера привязывается к определённому IP-адресу и порту с помощью функции *SysSockBind()*. Для привяз-

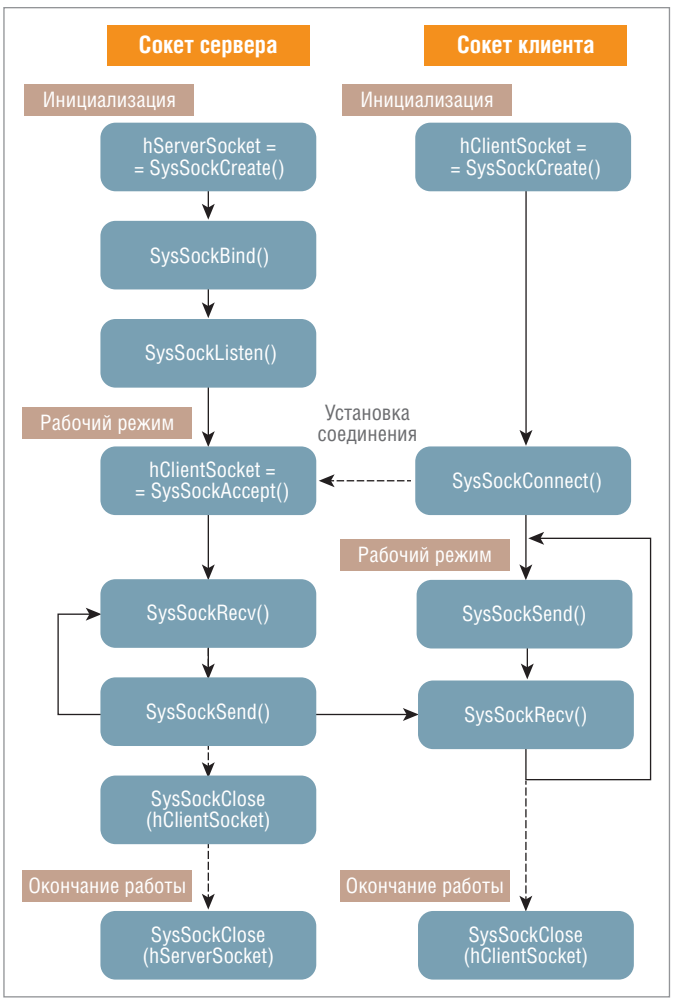



**Рис. 6. Работа простых клиентского (справа) и серверного (слева) TCP-сокетов**

**Листинг 1. Создание серверного TCP-сокета**

```
hServerSocket := SysSockCreate(SOCKET_AF_INET, SOCKET_STREAM, SOCKET_IPPROTO_TCP, ADR(result));
// hServerSocket – системный идентификатор типа RTS_IEC_HANDLE, создаваемый SysSockCreate;
// SOCKET_AF_INET задаёт сетевой протокол версии IPv4
// SOCKET_STREAM определяет тип создаваемого сокета, в данном случае потоковый режим (TCP);
// SOCKET_IPPROTO_TCP определяет протокол сокета, в данном случае TCP;
// ADR(result) – указатель на системный идентификатор (handle) результата функции;
// result имеет тип структуры RTS_IEC_RESULT и содержит коды ошибок, возникающих
// при работе с сокетами
```

**Листинг 2. Задание адреса серверного TCP-сокета**

```
// Задание адреса сокета для подключения к клиенту
// Выбор семейства протоколов: SOCKET_AF_INET соответствует IPv4 serverAddress.sin_family := SOCKET_AF_INET;

// Указывается IP-адрес сервера, с которым будет связан сокет
// IP := '10.0.0.100';
result := SysSockInetAddr(IP,ADR(serverAddress.sin_addr.ulAddr));

// Указывается порт сокета
// port := 503;
serverAddress.sin_port := SysSockHtons(port);
```

**Листинг 3. Связывание серверного TCP-сокета с адресом**

```
result := SysSockBind(hServerSocket, ADR(serverAddress), SIZEOF(serverAddress));
// Дескриптор серверного сокета hServerSocket связывается с адресом сокета serverAddress,
// описываемым структурой SOCKADDRESS.
```

**Листинг 4. Старт прослушивания серверного TCP-сокета**

```
result := SysSockListen(hServerSocket, maxConnections);
// hServerSocket – системный идентификатор серверного сокета;
// maxConnections – максимальное количество входящих соединений, например maxConnections := 3;
```

**Листинг 5. Создание системного идентификатора клиентского TCP-сокета**

```
hClientSocket := SysSockAccept(hServerSocket, ADR(clientAddress), ADR(adressSize), ADR(result));
// hclientSocket – системный идентификатор клиентского сокета;
// clientAddress – структура SOCKADDRESS, где хранится адрес клиента;
// ADR(adressSize) – указатель на размер структуры SOCKADDRESS (тип DINT).
```

**Листинг 6. Получение данных от TCP-клиента**

```
bytesRead := SysSockRecv(hClientSocket, ADR(recvBuffer), SIZEOF(recvBuffer), 0, ADR(result));
// bytesRead – количество полученных байт сообщения. В случае ошибки возвращается 0;
// hClientSocket – системный идентификатор клиентского сокета;
// ADR(recvBuffer) – указатель на переменную, в которой сохраняется принимаемое сообщение;
// SIZEOF(recvBuffer) – размер принимаемого сообщения;
// Вместо 0 могут быть установлены дополнительные опции для приёма сообщений
// (подробнее в описании функции в библиотеке SysSocket);
// ADR(result) – указатель на идентификатор результата.
```

**Листинг 7. Отправка данных TCP-клиенту**

```
bytesSend := SysSockSend(hClientSocket, ADR(sendBuffer), SIZEOF(sendBuffer), 0, ADR(result));
// bytesSend – количество отправленных байт. В случае ошибки возвращается 0;
// hClientSocket – системный идентификатор клиентского сокета;
// ADR(sendBuffer) указатель на переменную, которая содержит отправляемое сообщение;
// SIZEOF(sendBuffer) – размер принимаемого сообщения;
// Вместо 0 могут быть установлены опции приёма сообщений;
// ADR(result) – указатель на идентификатор результата.
```

**Листинг 8. Закрытие TCP-сокета сервера**

```
SysSockClose(hServerSocket);
// hServerSocket – системный идентификатор серверного сокета.
```

ки к определённому IP-адресу функция *SysSockBind()* ссылается на структуру *SOCKADDRESS*, в которой хранится заданный адрес сокета для привязки.

Адрес сокета сервера задаётся один раз при инициализации (листинг 2). Переменная *serverAddress* имеет тип *SOCKADDRESS*. При инициализации необходимо выбрать семейство протоколов, указать IP-адрес (записанный в виде текстовой переменной типа STRING, например, '10.0.0.100') и номер порта (переменная типа WORD, например, 503).

После этого вызывается функция *SysSockBind()*, которая привязывает сокет к данному адресу (листинг 3).

При успешной привязке к адресу функция *SysSockListen()* включает прослушивание входящих соединений (ожидание подключений клиентов к серверу). Функцией *SysSockListen()* также определяется максимальное количество подключений к серверу (листинг 4). Например, если максимальное количество подключений равно 3 и все три клиента уже подключились к серверу, то четвёртому будет отказано в подключении.

Как только сервер включает режим прослушивания, он переходит в рабочий режим и ждёт входящие соединения от клиентов. Когда клиент подключается к сокету сервера, с помощью функции *SysSockAccept()* создаётся системный идентификатор клиентского сокета *hClientSocket* и соединение считается открытым (листинг 5).

Сообщения принимаются серверным сокетом с помощью функции *SysSockRecv()*. В данной функции задаётся указатель на переменную, куда будут сохраняться принимаемые сообщения (листинг 6).

После приёма сообщений сервер может отправить ответ. Это осуществляется с помощью функции *SysSockSend()*. В данной функции задаётся указатель на переменную, в которой хранятся отправляемые данные (листинг 7).

После успешных приёма и передачи данных возможны несколько вариантов поведения программы.

1. Программа может закрыть клиентское соединение. В этом случае в следующих циклах программы сервер будет ожидать подключения с новым клиентом. Такой режим работы не является эффективным, так как контроллеру придётся во время каждого цикла закрывать клиентское соединение и подключать нового клиента (или того же самого, что и в предыдущем цикле).
2. Программа может не закрывать клиентский сокет, а сохранить установленное соединение. В этом случае, один раз установив соединение, клиент будет постоянно отправлять и получать данные от сервера. Такой режим работы более эффективный, но может возникнуть ситуация, когда все клиентские соединения будут заняты и новый клиент не сможет подключиться к серверу. Решить данную ситуацию можно различными способами. Один из вариантов – наблюдать за последним временем активности клиентских сокетов и отключать самое старое соединение в случае, если в очереди обнаружился новый клиент (рис. 7).

В рабочем режиме серверный сокет всегда остаётся открытым. Закрытие серверного сокета может происходить при внешнем событии или при возникновении критических ошибок.

Ошибки при создании и работе сокетов отображаются в системном идентификаторе *result*, который имеет тип структуры *RTS_IEC_RESULT*. Обозначение кодов ошибок описано в системной библиотеке *CmpErrors Interfaces* в глобальных константах *Errors* (рис. 8).

Закрывает сокетное соединение функция *SysSockClose()* (листинг 8).

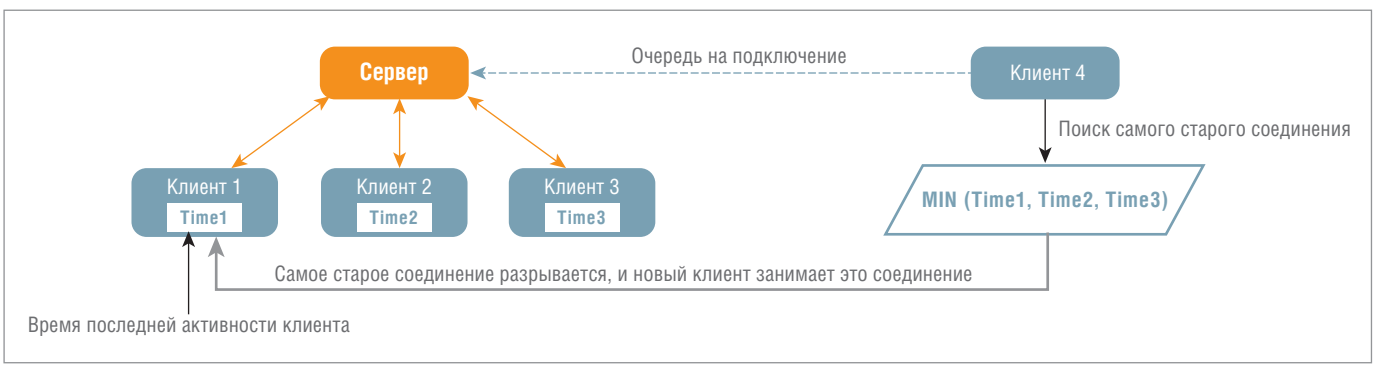



**Рис. 7. Обработка подключения нового клиента**

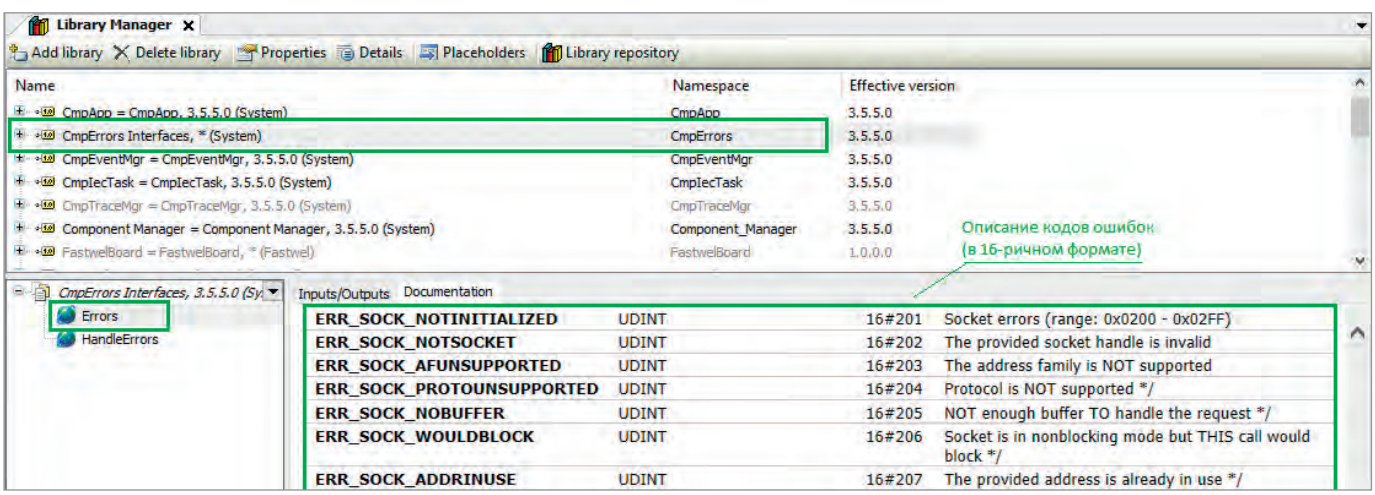



**Рис. 8. Расшифровка кодов ошибок работы сокетов**

**Клиентский TCP-сокет**

Схема работы клиентского сокета отображена на рис. 6 справа. Так же как и в случае серверного сокета, клиентский сокет вначале создаётся функцией *SysSockCreate()*, в результате которой создаётся системный идентификатор сокета (листинг 9).

Для подключения клиент должен знать IP-адрес и порт сервера, который хранится в переменной *clientAddress* (листинг 10).

После этого клиент переходит в рабочий режим и начинает обмениваться данными с сервером (листинг 11).

Обмен данными между клиентом и сервером осуществляется с помощью функций *SysSockSend()* и *SysSockRecv()*. Данные функции отправляют сообщения серверу и получают от него ответ (листинг 12).

После обмена данными сокет может быть закрыт с помощью *SysSockClose()* (листинг 13).

Однако, с точки зрения циклического обмена данными реального времени, закрытие сокета при каждом цикле нецелесообразно. Поэтому после успешной установки соединения обмен данными осуществляется в бесконечном цикле, до тех пор пока по какой-то причине не появляется необходимость закрыть сокет.

**Особенности TCP-сокетов**

Использование TCP-сокетов позволяет приложениям клиента и сервера обмениваться данными почти прозрачно, не заботясь о поддержании сетевого соединения, доставке пакетов по сети, порядке передачи пакетов и буферизации. TCP-сокеты гарантируют доставку сообщений и правильный порядок пакетов, а также пересылают пакеты повторно, если подтверждение о передаче не приходит в течение определённого промежутка времени [4]. Таким образом, использовать TCP-сокеты уместно там, где необходима гарантированная доставка данных.

Несмотря на многие преимущества, TCP-сокеты имеют и негативные стороны. Например, необходимость поддержания TCP-соединения уменьшает пропускную способность обмена данными в распределённых системах. Также в системах обмена данными реального времени повторная передача потерянных пакетов может привести к тому, что система получит данные, которые утратили свою актуальность.

## UDP-сокеты

Все перечисленные недостатки TCP-сокетов связаны с особенностью TCP-протокола. Если в системе присутствие дан-

Листинг 9. Создание клиентского TCP-сокета

```
hClientSocket := SysSockCreate(SOCKET_AF_INET, SOCKET_STREAM, SOCKET_IPPROTO_TCP,ADR(result));
// hClientSocket – системный идентификатор клиентского сокета;
// SOCKET_AF_INET задаёт сетевой протокол IPv4;
// SOCKET_STREAM определяет тип сокета, в данном случае потоковый сокет (TCP);
// SOCKET_IPPROTO_TCP определяет протокол сокета, в данном случае TCP;
// ADR(result) – указатель на системный идентификатор (handle) результата функции.
```

Листинг 10. Задание адреса для подключения клиентского TCP-сокета к TCP-серверу

```
// Задаётся адрес сокета для подключения
// Выбор семейства протоколов: SOCKET_AF_INET соответствует IPv4
clientAddress.sin_family := SOCKET_AF_INET;

// Задание порта сокета для подключения
// port := 503;
clientAddress.sin_port:=SysSockHtons(port);

// Задание IP-адреса сервера
// IP := '10.0.0.100';
result := SysSockInetAddr(IP, ADR(clientAddress.sin_addr));
```

Листинг 11. Подключение клиентского сокета к серверу

```
result := SysSockConnect(hClientSocket, ADR(clientAddress), SIZEOF(clientAddress));
// hClientSocket – системный идентификатор клиентского сокета;
// ADR(clientAddress) – указатель на структуру SOCKADDRESS с адресом сокета сервера;
// SIZEOF(clientAddress) – размер структуры адреса сокета.
```

Листинг 12. Обмен данными между TCP-клиентом и TCP-сервером

```
bytesSend := SysSockSend(hClientSocket, ADR(sendMessage), SIZEOF(sendMessage), 0,ADR(result));
bytesRecv := SysSockRecv(hClientSocket, ADR(recvMessage), SIZEOF(recvMessage), 0, ADR(result));
// hClientSocket – системный идентификатор клиентского сокета;
// ADR(sendMessage/recvMessage) – указатель на отправляемое/полученное сообщение;
// SIZEOF(sendMessage/recvMessage), размер отправленного/полученного сообщения;
// ADR(result) – указатель на системный идентификатор (handle) результата функции.
```

Листинг 13. Закрытие клиентского TCP-сокета

```
SysSockClose(hClientSocket);
// где hClientSocket – системный идентификатор серверного сокета.
```

PROSOFT® SYSTEMS

# УСТРОЙСТВО СИНХРОНИЗАЦИИ ВРЕМЕНИ ИСС

## точка отсчета в информационной системе

ИСС-1.1

ИСС-1.3

ИСС-2.1

- Прием сигналов от глобальных навигационных спутниковых систем ГЛОНАСС и GPS
- Формирование сигналов точного времени в форматах 1PPS, IRIG-B, IEEE 1344, 10 МГц, NMEA
- Поддержка сетевых протоколов синхронизации времени
- Диапазон рабочих температур от –40 до +60°С
- Абсолютная погрешность 200 нс относительно UTC

Серия включена в Государственный реестр средств измерений 21.05.2018 под номером 71235-18

Инженерная компания ООО «Прософт–Системы»
620102, г. Екатеринбург, ул. Волгоградская, 194а
prosoftsystems.ru

тел.: +7 (343) 3-565-111,
факс: +7 (343) 3-100-106
info@prosoftsystems.ru

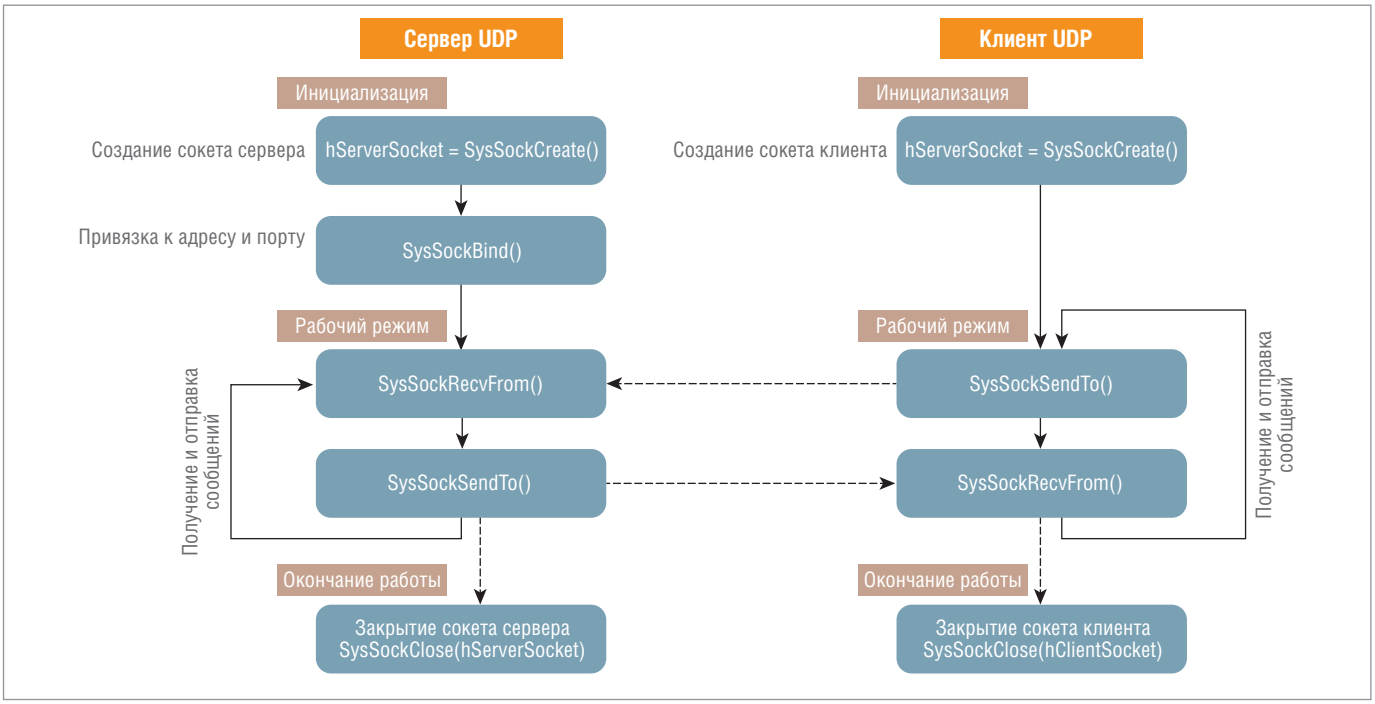



**Рис. 9. Схема работы простых UDP-сокетов: серверного (слева) и клиентского (справа)**

ных факторов крайне нежелательно, а гарантированность доставки сообщений не является критичным требованием, то в качестве альтернативы TCP-сокетов могут использоваться UDP-сокеты.

UDP-сокеты устроены проще, чем TCP. В качестве транспортного уровня используется протокол UDP, который не требует установления соединения и подтверждения приёма [4]. Информация пересылается в предположении, что принимающая сторона её ожидает. Датаграммные сокеты не контролирует ничего, кроме целостности полученных датаграмм. Несмотря на это, UDP-сокеты нашли своё применение в системах, где на первом месте стоит именно актуальность данных и их быстрая доставка, а не гарантия доставки каждого сообщения.

Например, сервер в ответ на запросы клиента передаёт по сети текущие значения некоторого параметра, а клиент формирует управляющий сигнал на основе принятых значений. Если клиент опрашивает сервер быстрее, чем скорость изменения параметра, то потеря одного-двух UDP-сообщений от сервера существенно не повлияет на качество формирования управляющего сигнала. В случае использования TCP потерянный пакет будет автоматически передан повторно, что может привести к получению клиентом неактуального значения параметра, а значит, к ошибке формирования управляющего сигнала.

На рис. 9 представлена схема работы простых серверных и клиентских UDP-сокетов.

**Серверный UDP-сокет**

Так же как в случае TCP-сокетов, системный идентификатор UDP-сервера создаётся с помощью функции *SysSockCreate()* (листинг 14).

После создания сокет сервера привязывается к определённому IP-адресу и порту с помощью функции *SysSockBind()*. В отличие от TCP, UDP-сокет не включает прослушивание входящих соединений, а сразу подготавливается к получению данных по сети (листинг 15).

Для получения данных по UDP используется функция *SysSockRecvFrom()* (в отличие от *SysSockRecv()* для TCP-сокетов). Её главная особенность в том, что она не просто принимает данные от клиента, но и записывает адрес и порт клиента в специальную структуру для хранения адреса *SOCKADDRESS*, чтобы в дальнейшем сервер знал, куда отправлять ответное сообщение (листинг 16).

Ответное сообщение отправляется с помощью функции *SysSockSendTo()*, которая аналогична *SysSockSend()* для TCP-протокола, но в качестве аргумента принимает ссылку на адрес структуры *SOCKADDRESS*, где хранится записанный ранее адрес клиента (листинг 17).

После отправки данных сокет сервера снова переходит к функции *SysSockRecvFrom()* и остаётся открытым. Но в случае необходимости серверный сокет можно закрыть аналогично TCP-сокету (листинг 8):

**Клиентский UDP-сокет**

Клиент UDP работает аналогично клиентскому сокету TCP, за исключением использования функций *SysSockSendTo()* и *SysSockRecvFrom()* для отправки и получения сообщений (рис. 9).

Функция *SysSockCreate()* создаёт системный идентификатор сокета. Так же как и в случае сервера, для клиента необходимо создать потоковый сокет (листинг 18).

В отличие от TCP-сокетов, при использовании UDP-протокола клиентский сокет не устанавливает соединения с сервером, а сразу после создания клиентского сокета переходит к обмену данными с помощью функций *SysSockSendTo()* и *SysSockRecvFrom()* (листинг 19).

После обмена данными сокет может быть закрыт с помощью *SysSockClose()* (листинг 13).

Однако, с точки зрения циклического обмена данными реального времени, каждый раз закрывать и открывать сокет заново неэффективно. Поэтому после успешной установки соединения обмен данными осуществляется в бесконечном цикле.

## Дополнительные настройки сокетов

На рис. 6 показана работа простых серверного и клиентского TCP-сокетов. Но на деле такая простая схема имеет некоторые ограничения и недостатки.

**Блокирующий режим**

По умолчанию некоторые функции библиотеки *SysSocket* являются *блокирующими*. Это значит, что вызов функции не возвращает управление программному коду до тех пор, пока он не выполнится. Блокирующими функциями являются *SysSockAccept()*, *SysSockSend()*, *SysSockRecv()*, *SysSockSendTo()*, *SysSockRecvFrom()* и так далее.

Например, сервер включает прослушивание входящих соединений с помощью неблокирующей функции *SysSockListen()*, сразу после которой идёт вызов *SysSockAccept()*. И до тех пор пока в очереди установленных соединений не появится хотя бы одно подключение, программа не будет исполняться дальше. Такой режим работы также называется синхронным.

Естественно, такое поведение программы не является безопасным, и при циклическом вызове программы в ПЛК может сработать сторожевой таймер или произойти выход в безопасный режим – контроллер будет считать, что программа зависла.

**Листинг 14. Создание серверного UDP-сокета**

```
hServerSocket := SysSockCreate(SOCKET_AF_INET, SOCKET_DGRAM, SOCKET_IPPROTO_UDP, ADR(result));
// hServerSocket – системный идентификатор сокета сервера;
// SOCKET_AF_INET – семейство, соответствующее сетевому протоколу IPv4;
// SOCKET_DGRAM – тип создаваемого сокета (датаграммный сокет для UDP);
// SOCKET_IPPROTO_UDP – протокол сокета UDP;
// ADR(result) – указатель на идентификатор результата (RTS_IEC_RESULT).
```

**Листинг 15. Связывание серверного UDP-сокета с адресом**

```
result := SysSockBind(hServerSocket, ADR(serverAddress), SIZEOF(serverAddress));
// Дескриптор серверного сокета hServerSocket связывается с адресом сокета;
// serverAddress, заданным структурой SOCKADDRESS.
```

**Листинг 16. Получение данных от UDP-клиента**

```
bytesRead := SysSockRecvFrom(hServerSocket, ADR(recvBuffer), SIZEOF(recvBuffer), 0,
                         ADR(clientAddress), SIZEOF(clientAddress),ADR(result));
// hServerSocket – системный идентификатор сокета сервера;
// bytesRead – количество полученных байт, в случае ошибки возвращается 0;
// hServerSocket – системный идентификатор клиентского сокета;
// ADR(recvBuffer) – указатель на переменную, в которую запишется получаемое сообщение;
// SIZEOF(recvBuffer) – размер принимаемого сообщения;
// Вместо 0 могут быть установлены опции приёма сообщений;
// ADR(clientAddress) – указатель на структуру SOCKADDRESS, в которую запишется адрес клиента;
// ADR(result) – указатель на идентификатор результата.
```

**Листинг 17. Отправка данных UDP-клиенту**

```
bytesSend := SysSockSendTo(hServerSocket, ADR(sendBuffer), SIZEOF(sendBuffer), 0,
                         ADR(clientAddress), SIZEOF(clientAddress),ADR(result));
// ADR(sendBuffer) и SIZEOF(sendBuffer) – указатель на отправляемое сообщение
// и размер отправляемого сообщения;
// ADR(clientAddress) – указатель на структуру, в которой записан адрес сокета клиента.
```

**Листинг 18. Создание клиентского UDP-сокета**

```
hClientSocket := SysSockCreate(SOCKET_AF_INET, SOCKET_DGRAM, SOCKET_IPPROTO_UDP, ADR(result));
// hClientSocket – системный идентификатор клиентского сокета;
// SOCKET_AF_INET – семейство, соответствующее сетевому протоколу IPv4;
// SOCKET_DGRAM – тип создаваемого сокета (датаграммный сокет для UDP);
// SOCKET_IPPROTO_UDP – протокол сокета (UDP);
// ADR(result) – указатель на идентификатор результата (RTS_IEC_RESULT).
```

**Листинг 19. Обмен данными между UDP-клиентом и UDP-сервером**

```
bytesSend := SysSockSendTo(hClientSocket, ADR(sendMessage), SIZEOF(sendMessage), 0,
                         ADR(clientAddress), SIZEOF(clientAddress), ADR(result));

bytesRecv := SysSockRecvFrom(hClientSocket, ADR(recvMessage), 256, 0,
                         ADR(clientAddress), SIZEOF(clientAddress), ADR(result));
// hClientSocket – системный идентификатор сокета сервера;
// bytesRead, bytesRecv – количество полученных и отправленных байт,
// в случае ошибки возвращается 0;
// ADR(clientAddress) – указатель на структуру SOCKADDRESS, в которую запишется адрес клиента;
// ADR(result) – указатель на идентификатор результата.
```

Листинг 20. Включение неблокирующего режима

```
result := SysSockIoctl(hSocket, SOCKET_FIONBIO, ADR(mode));
// hSocket – системный идентификатор сокета клиента или сервера;
// ADR(mode) – указатель на переменную, включающую опцию (значение переменной равно 16#1).
```

Листинг 21. Дополнительные настройки работы сокета

```
result := SysSockSetOption(hSocket, SOCKET_SOL, SOCKET_SO_REUSEADDR, ADR(mode), SIZEOF(mode));
// hSocket – системный идентификатор сокета клиента или сервера;
// SOCKET_SOL – уровень протокола, соответствующий уровню сокетов;
// SOCKET_SO_REUSEADDR – опция, позволяющая связать сокет с локальным адресом,
// который уже используется на другом открытом сокете;
// ADR(mode) – указатель на переменную, включающую опцию (значение переменной 16#1).
```

Листинг 22. Работа с несколькими клиентами

```
result := SysSockSelect(maxConnections+1, ADR(readSet), ADR(writeSet), ADR(exceptSet),
                                                ADR(timeSelect), ADR(socketReady));
// maxConnections+1 – количество проверяемых дескрипторов. В качестве аргумента
// устанавливается максимальное количество соединений + 1;
// ADR(readSet), ADR(writeSet), ADR(exceptSet) – указатель на набор дескрипторов
// (SOCKET_FD_SET), которые следует проверять на готовность к чтению, записи и
// наличию исключительных ситуаций;
// SysSockSelect() является блокирующей функцией, она возвращает управление, если
// хотя бы один из проверяемых сокетов готов к выполнению соответствующей операции;
// ADR(timeSelect) – указатель на интервал времени timeSelect, по прошествии которого
// функция вернёт управление в любом случае;
// timeSelect имеет структуру SOCKET_TIMEVAL и задаёт максимальное время, которое
// функция SysSockSelect будет ожидать для получения ответа;
// ADR(socketReady) – указатель на количество сокетов, готовых к работе, которое
// возвращает функция SysSockSelect.
```

Для того чтобы использовать функции в неблокирующем режиме, необходимо после создания сокета *SysSockCreate()* вызвать функцию *SysSockIoctl()* с входным аргументом *SOCKET_FIONBIO* (листинг 20), которая является командой перевода сокета в неблокирующий режим. При неблокирующем (асинхронном) режиме функция возвращает управление программе вне зависимости от того, закончена операция приёма/передачи или нет (рис. 10).

Также дополнительные настройки работы сокета можно сделать с помощью функции *SysSockSetOptions()*, например, включить возможность повторного использования порта (листинг 21).

**Подключение нескольких клиентов**

Серверный TCP-сокет, работающий согласно схеме на рис. 5, подходит для обмена данными в режиме точка–точка, когда существует одно входящее клиентское соединение. В случае если к серверу будет подключаться несколько клиентов, может возникнуть путаница с принимаемыми и отправляемыми сообщениями, а также может появиться очередь на ожидание подключения.

Для того чтобы эффективно работать с несколькими клиентами, используется *SysSockSelect()* (листинг 22). Данный метод проверяет состояние нескольких идентификаторов сокетов одновременно. Сокеты можно проверять на готовность к чтению, записи или на наличие исключительных ситуаций, то есть ошибок.

Если хотя бы один сокет клиента готов, например, к отправке данных, *SysSockSelect()* сообщит об этом программе и соединение с данным клиентом будет установлено. Схема работы серверного сокета с использованием *SysSockSelect()* показана на рис. 10.

Функция *SysSockSelect()* является блокирующей, она возвращает управление, если хотя бы один из проверяемых сокетов готов к выполнению соответствующей операции. Но в качестве настройки в функции можно указать интервал времени, по истечении которого она вернёт управление в любом случае.

## Особенности использования внешних ресурсов контроллера

При создании сокетов для CPM723-01 необходимо иметь в виду, что система исполнения приложений версии CODESYS V3 не имеет в своём составе подсистемы автоматического учёта и освобождения внешних ресурсов, запрошенных приложением [1]. К таким внешним ресурсам относятся файлы, сокеты и другие системные ресурсы. Для того чтобы был обеспечен повторный доступ к ним, необходимо самостоятельно освобождать полученные системные идентификаторы (в нашем случае *hServerSocket* и *hClientSocket*) в обработчике системного события *PrepareExit*, в котором вызывать действия по освобождению ресурсов, требуемых в программах (рис. 11).

Таким образом, каждый раз перед завершением работы приложения будет закрываться доступ к портам, и при следующем запуске приложения данные порты будут открыты для использования.

## Заключение

TCP- и UDP-сокеты отвечают за обмен данными между различными устройствами и процессами. На базе обмена данными по сокетам можно создавать протоколы стека TCP/IP более высокого уровня.

Обмен по TCP и UDP в контроллере CPM723-01 может потребоваться там, где устройство, с которым необходимо орга-

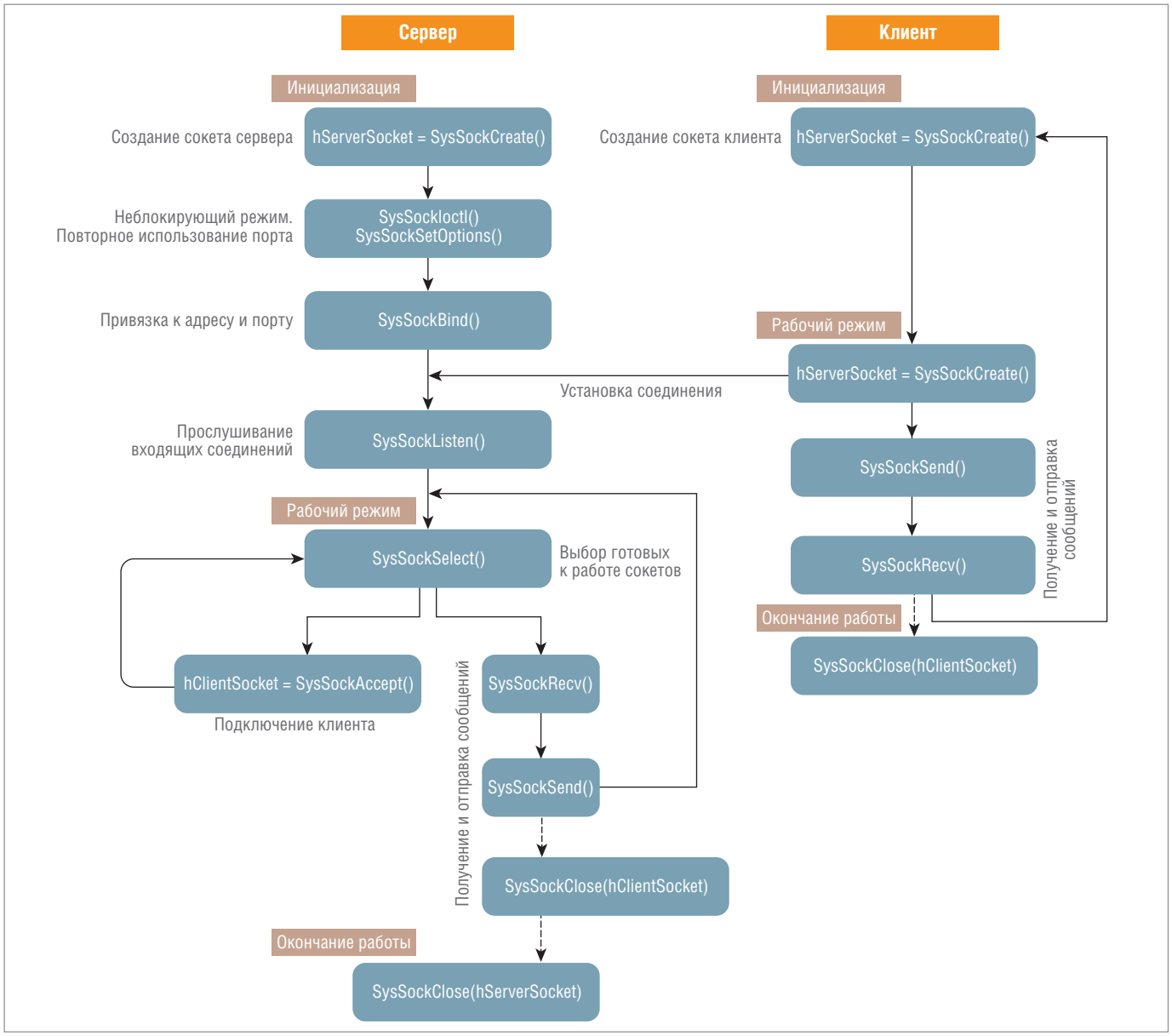



**Рис. 10. Схема работы сокетов с использованием неблокирующих опций и функции SysSockSelect()**

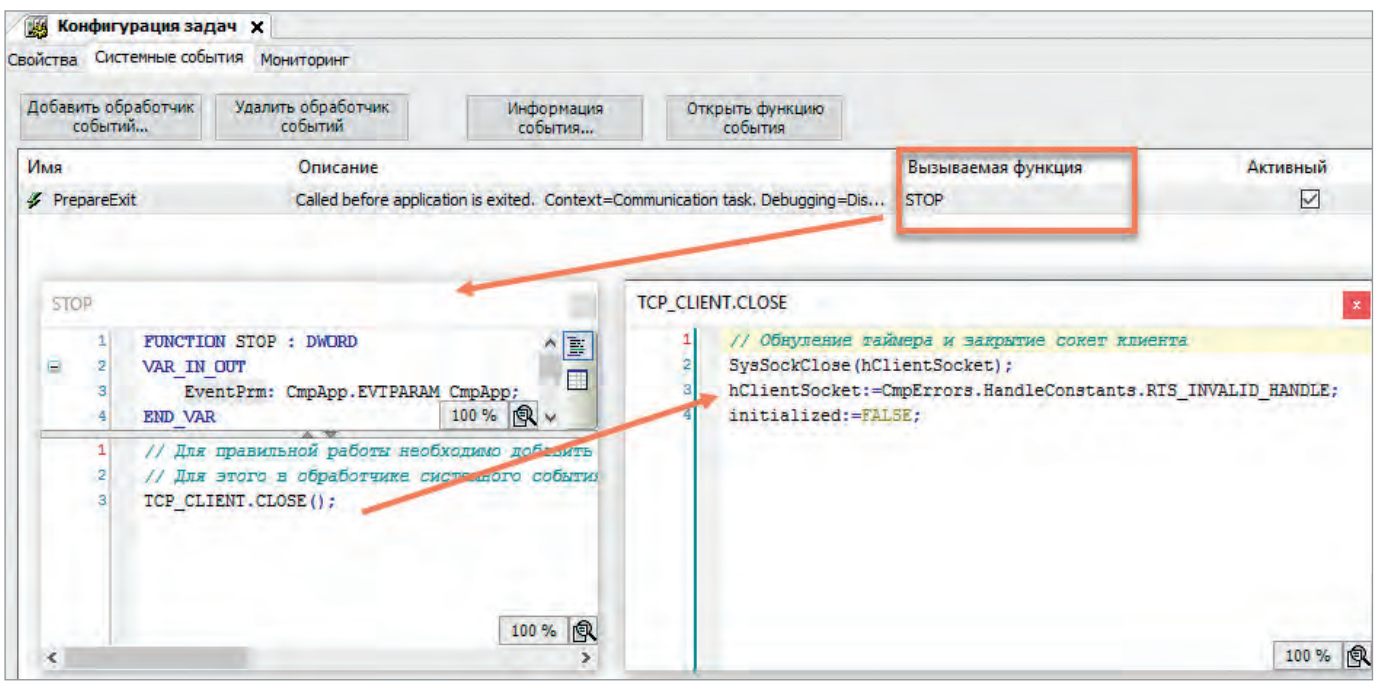



**Рис. 11. Системное событие, освобождающее системные идентификаторы**

низовать связь, не поддерживает промышленный протокол Modbus TCP.

TCP-сокеты необходимы там, где требуется надёжная доставка сообщений, а скорость передачи данных не критична. UDP-сокеты лучше всего использовать там, где требуется эффективность на быстрых сетях с короткими соединениями и данные реального времени, а гарантированность доставки сообщений не нужна [4]. ●

## Литература


1. Система ввода-вывода FASTWEL I/O. Контроллер программируемый CPM723-01.Руководство по конфигурированию и программированию ИМЕС.00300-03 33 02-1. [Электронный ресурс] // Режим доступа : https://tp.prosoft.ru/docs/shared/%D0%A2%D0%B5%D1%85%D0%BF%D0%BE%D1%80%D1%82%D0%B0%D0%BB/Fastwel_IO/Manual/CPM723-01_CDSV3_UM.pdf.
2. Parziale L., Britt D.T., Davis Ch., Forrester J., et al. TCP/IP Tutorial and Technical Overview. – USA : IBM, December 2006.
3. Основы TCP-связи [Электронный ресурс] // Режим доступа : http://www.sbcr.jp/books/img/Linuxnet_02.pdf. – Текст на яп.
4. Fiedler G. UDP vs. TCP. Which protocol is best for games? [Электронный ресурс] // Режим доступа : https://gafferongames.com/post/udp_vs_tcp/.
5. Лейкин А. Протоколы транспортного уровня UDP, TCP и SCTP: достоинства и недостатки // Первая миля. – 2013. – № 5.
6. Network communication under UNIX System Services [Электронный ресурс] // Режим доступа : https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.cbcpx01/ipchap.htm.



**Автор – сотрудник фирмы ДОЛОМАНТ**
**Телефон: (495) 232-1698**
**E-mail: fio@fastwel.ru**


НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

## Новости ISA

4 марта 2018 года на площадке Инженерной школы ГУАП был проведён 2-й этап открытого регионального чемпионата «Молодые профессионалы» (WorldSkills Russia) Санкт-Петербурга по компетенции «Интернет вещей». К участию в соревнованиях были приглашены команды студентов колледжей Санкт-Петербурга и молодые специалисты предприятий города. Возрастная категория от 16 до 22 лет. Чемпионат собрал команды и экспертов по направлению «Интернет вещей» из ведущих средних профессиональных учебных заведений города. Компетенция «Интернет вещей» относится к категории Future Skills (профессии будущего) и направлена на подготовку специалистов по комплексной автоматизации и роботизации производства с использованием самых передовых промышленных технологий. Компетенция создана в 2016 году при поддержке компаний PTC и Fanuc. На церемонии открытия, прошедшей в доброжелательной и деловой атмосфере, к участникам чемпионата с приветствием обратились представитель Регионального координационного центра WorldSkills в Санкт-Петербурге Н.Е. Смирнова и председатель организационного комитета соревнования, начальник Управления информатизации ГУАП, активный член Российской секции ISA А.В. Сергеев.

В период с 16 по 20 апреля в ГУАП прошла 71-я Международная научная студенческая конференция. В рамках мероприятия была проведена XI студенческая конференция ISA. Студенты и аспиранты шести университетов из США, Италии, Испании, Российской Федерации и Индонезии выступили с докладами. Руководил работой конференции профессор университета штата Индиана (США), президент ISA 2009 года Gerald Cockrell. Россию представляли студенты ГУАП Ростислав Шаниязов и Ангелина Добровольская. Решением международного жюри доклады студентов ГУАП признаны лучшими. Студенты и их научные руководители А.В. Сергеев и Н.Н. Майоров награждены почётными дипломами ISA.

Группа компаний (ГК) InfoWatch и ГУАП открыли совместную исследовательскую лабораторию кибербезопасности. Соглашение о создании лаборатории подписали 18 апреля 2018 года на площадке Петербургского цифрового форума ректор ГУАП (президент Российской секции ISA 2014 года) Юлия Анатольевна Антохина и президент ГК InfoWatch Наталья Ивановна Касперская. Помимо подписания соглашения 18 апреля состоялось торжественное открытие лаборатории в Инженерной школе Интернета вещей ГУАП. Лаборатория создана с целью развития инновационной и образовательной деятельности, проведения НИОКР в области защиты информации с использованием технологий, решений, продуктов ГК InfoWatch. Планируется, что лаборатория станет базой для подготовки специалистов по созданной в 2017 году компетенции WorldSkills «Корпоративная защита от внутренних угроз ИБ» в национальном масштабе.

XI студенческая конференция ISA

27–28 апреля 2018 года делегация Российской секции ISA приняла участие в работе Исполкома Европейского совета ISA в Мадриде. На заседании Исполкома обнародованы итоги XIV Европейского конкурса на лучшую студенческую научную работу ISA (ESPC-2018). Студенты и аспиранты ГУАП – члены студенческой секции ISA – в очередной раз показали прекрасные результаты. Золотых медалей удостоены А. Чабаненко, Р. Шаниязов, Б. Акопян, А. Шабанова, М. Шелест, М. Тарала. Серебряные медали вручаются А. Добровольской, Ю. Соколовой, С. Герасимову, А. Виноградову. Бронзовые награды получают Е. Григорьев, Л. Ефимова, Ф. Рыжов, Н. Исакова и Г. Емельянов. Традиционно медали победителям вручены ректором ГУАП, президентом Российской секции ISA 2014 года Ю.А. Антохиной на заседании учёного совета ГУАП 24 мая 2018 года.

Почётными дипломами ISA награждены активные члены Российской секции ISA И.А. Киршина, И.А. Павлов (президент Российской секции ISA 2010 года), Е.Г. Семёнова (президент Российской секции ISA 2011 года), А.С. Будагов (президент Российской секции ISA 2018 года). ●

nVent

Schroff®

# Платформа EuropacPRO — евромеханика высокого полёта


## PROгрессивные блочные каркасы и приборные корпуса

- Безграничное разнообразие конфигураций из унифицированных компонентов
- Современный промышленный дизайн
- Высокая прочность и надёжность
- Доработка под индивидуальные требования

Юрий Широков

# Особенности источников питания и программируемых нагрузок для промышленности и научных исследований

Множество приборов нуждается для работы в источниках тока и напряжения, и сфера применения современных источников питания отнюдь не ограничивается популярными гаджетами и бытовой техникой. Самые совершенные, сложные и дорогостоящие из них применяются в научных исследованиях, промышленности, в составе испытательных стендов и т.п. Там и нашли себе основное применение весьма технологичные устройства – программируемые источники питания. Они созданы на базе накопленных обширных знаний в области электроники и электротехники, а их возможности неизмеримо шире, нежели у бытовых.

В рамках данного обзора мы затронем также тему электронных нагрузок (eLoad). Эти устройства вообще в быту аналогов не имеют и предназначены для выполнения, на первый взгляд, странной задачи – имитации в электрической цепи нагрузки с заданными параметрами путём поглощения строго отмеренной электрической мощности.

## Программируемые источники питания

Программируемые источники питания, как и обычные, обеспечивают на выходе постоянное или переменное напряжение/ток с заданными параметрами. Приборы профессионального класса имеют минимальные значения пульсаций и незначительный коэффициент нестабильности при изменении характеристик подключаемой к ним нагрузки. При этом, как и следует из их названия, они обладают уникальным качеством – возможностью программирования (рис. 1) Под этим качеством подразумевается возможность управлять выходными характеристиками прибора, такими как напряжения и токи в нагрузке, путём подачи внешнего аналогового либо цифрового сигнала или посредством табличного задания параметров, а также получать от источника некоторую мониторинговую информацию.

Современные источники предоставляют такие возможности управления и контроля, как дистанционное включение/отключение, программирование и мониторинг выходных токов и напряжений, мониторинг питающей сети, а также многие другие. Что касается набора интерфейсов, то современные серии программируемых источников могут иметь целый арсенал, включающий порты USB, RS-232/RS-485, аналоговый вход управления 0...5 В, 0...10 В, 4...20 мА, сетевой порт LAN eXtensions for Instrument и прочие. У некоторых моделей имеется также и возможность объединения нескольких источников для совместной работы с использованием шины GPIB (General Purpose Interface Bus).

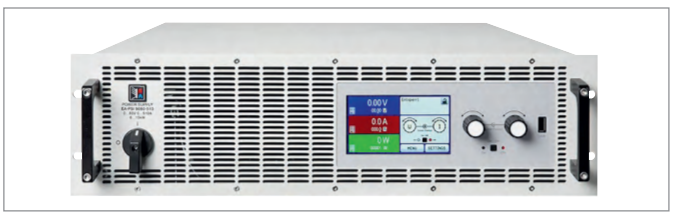


Рис. 1. Программируемый источник питания серии EA PSB 9000 3U

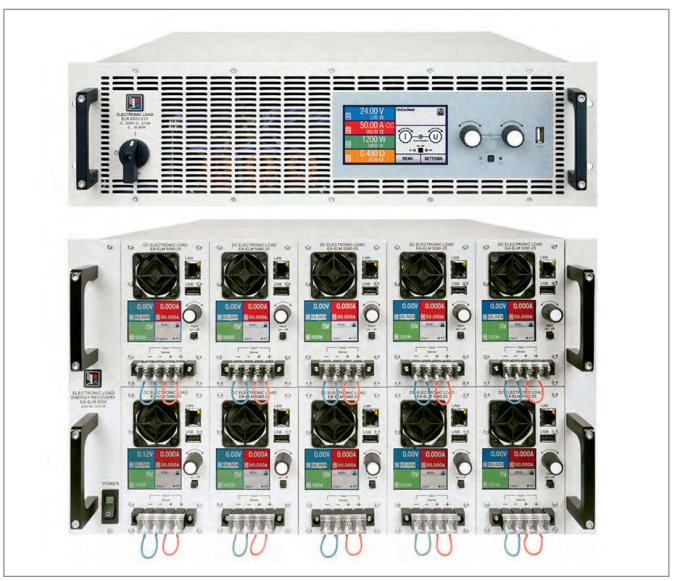


Рис. 2. Электронная нагрузка с рекуперацией энергии ELR 9000 HP 3U

При помощи программируемого источника можно, например, смоделировать поведение реальной АКБ или гальванического элемента в процессе постепенного разряда под нагрузкой, проанализировать в автоматическом режиме работу нагрузки при различных параметрах электропитания, обеспечить сложную и точно заданную выходную характеристику тока и напряжения для научных экспериментов или технологических процессов. Разумеется, такая функциональность крайне востребована в научных и исследовательских центрах и лабораториях, на высокотехнологичных производствах.

## Электронные нагрузки E-Load

Электронная нагрузка представляет собой устройство-противоположность источника питания. Задачей её является имитация поведения реальных приборов и устройств по отношению к источнику питания. E-Load, как правило, обеспечивает

следующие основные режимы: постоянное напряжение (CV), постоянный ток (CC), постоянная мощность (CP), постоянное сопротивление (CR). При помощи устройства E-Load, например, можно смоделировать электродвигатель с его высокими пусковыми токами, а также любую другую нагрузку с нелинейной вольт-амперной характеристикой (рис. 2). Широко применяют электронные нагрузки и для тестирования источников питания. Многие современные электронные нагрузки программируемые и обладают возможностью дистанционного управления. Особо продвинутые модели имеют интерфейс для удалённого управления при помощи компьютера, что позволяет использовать их в составе автоматизированных испытательных стендов, автоматически включающих заданные режимы работы и изменяющих параметры, а также получать и анализировать мониторинговые данные об их состоянии. Всё это востребовано при различных сложных лабораторных испытаниях, проведении тестов устройств и оборудования: солнечных батарей и АКБ, блоков питания, различных генераторов и многого другого. В режиме тестирования батареи, например, она может при помощи E-Load разряжаться постоянным током, постоянной мощностью или постоянным сопротивлением до тех пор, пока не достигнет установленного порога разрядного напряжения. Надо отметить, что типовая электронная нагрузка ещё и обеспечивает постоянный мониторинг напряжения и протекающих через неё токов.

Поскольку электронная нагрузка имитирует реальную, один из ключевых параметров устройства E-Load – рассеиваемая мощность. Таким образом, конструктивное исполнение мощной электронной нагрузки должно гарантировать эффективный теплоотвод. С учётом широкого диапазона доступных мощностей – от сотен Вт до сотен кВт – электронная нагрузка может представлять собой как компактное настольное устройство в приборном корпусе, так и целый отдельно стоящий шкаф с принудительным водяным охлаждением. Бывают и специфические электронные нагрузки, предназначенные для нишевого использования. Например, компания Ericsson использует миниатюрные устройства собственной разработки для тестирования встраиваемых в платы мобильных устройств интегральных DC/DC-преобразователей.

Для обеспечения безопасности работы электронные нагрузки оснащаются также защитой от перегрева и перегрузки по мощности, от переполюсовки и перенапряжения.

В некоторых случаях от электронной нагрузки может потребоваться выступать в роли не поглотителя, а источника энергии. Это нужно, например, при моделировании работы цепей с реактивной (ёмкостной или индуктивной) нагрузкой. Однако такую функциональность имеют далеко не все представленные на рынке модели, и в основном E-Load является управляемым переменным резистором, на котором рассеивается энергия по заданному закону. Упрощённая структура такой электронной нагрузки представлена на рис. 3.

## Комбинирование устройств

На рынке присутствуют также гибридные устройства, представляющие собой источник питания и электронную нагрузку, объединённые в одном корпусе. В последнее время появляются регенеративные электронные нагрузки, способные возвращать поглощённую энергию обратно в сеть с высокой эффективностью. Это особенно актуально, когда рассеиваемая на нагрузке мощность достигает десятков и сотен киловатт. У электронных нагрузок имеется и ещё одно важное применение: их можно использовать совместно с источниками питания в качестве устройств для быстрого управления током. Это позволяет обеспечить высокоскоростное управляемое нарастание/спад импульсов тока, получаемых от источника питания. Такая связка двух приборов зачастую обходится дешевле и обеспечивает более высокие характеристики, нежели специализированный высокоскоростной источник питания.

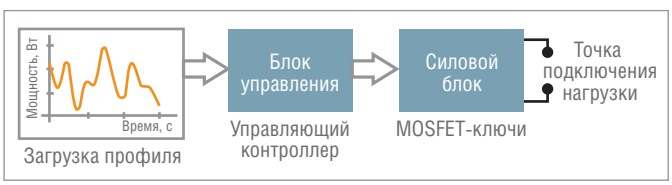



**Рис. 3. Упрощённая структура электронной нагрузки (E-Load)**

## Рынок программируемых источников и электронных нагрузок

Рынок этих весьма востребованных устройств быстро развивается, тем не менее, основные его игроки хорошо известны.

### AMETEK

AMETEK – крупная международная компания, специализирующаяся на производстве электронных приборов и электромеханических устройств. Офисы компании расположены во многих странах, в том числе и в России. Имеет множество подразделений. Подразделение Programmable Power, базирующееся в Сан-Диего (Калифорния), занимается разработкой программируемых источников питания постоянного и переменного тока, электронных нагрузок. Продукция AMETEK применяется в исследовательских и испытательных целях и используется в таких приложениях, как бортовое оборудование, общие НИОКР, проверка на электромагнитную совместимость (ЭМС), производство и тестирование полупроводников, нефтеразведка, симуляция работы различных источников тока (солнечных батарей, аккумуляторов и т.п.), тестирование оборудования и измерения, имитация работы различных силовых электрических шин. Продукция этого подразделения выпускается под брендами Sorensen, ELGAR, California Instruments, AMREL.

### GW INSTEK

Компания основана в 1975 году. В момент основания носила название Good Will Instrument Co., Ltd. Это тайваньский производитель с солидной историей и опытом производства измерительного и испытательного оборудования, а также источников питания. В настоящее время является крупнейшим производителем этого оборудования на Тайване, насчитывающим в своём портфолио более 300 продуктов. Источники питания и электронные нагрузки производства GW INSTEK пользуются заслуженно высокой репутацией среди профессионалов.

### Tektronix

Одна из старейших на рынке компаний, основанная в 1946 году в США. В настоящее время имеет множество представительств по всему миру, включая Россию. Компания настолько известна, что не нуждается в рекомендации: её приборами пользовалось не одно поколение профессиональных электронщиков, учёных-исследователей, производственников, а также специалистов многих других областей. Помимо источников питания и электронных нагрузок постоянного тока компания производит анализаторы спектра, осциллографы, функциональные генераторы, мультиметры.

### TDK-Lambda

Группа компаний TDK основана в 1978 году и специализируется на разработке, производстве и обслуживании импульсных источников питания и периферийных устройств. Ведёт свою историю от японской компании Nippon Electronic Memory Industry Co., Ltd. В 2006 году корпорация TDK приобрела компанию Lambda, и группа компаний получила известное сегодня имя TDK-Lambda. Производственные мощности находятся в Северной Америке, Японии, Южной Корее, Китае, Сингапуре, Израиле, Германии, Франции, Италии, Швеции. В России имеется представительство. TDK-Lambda, одна из именитых компаний на рынке источников питания представляет серию программируемых источников Genesys для монтажа в стойки (1U и 2U), а также серии настольных лабораторных источников Z+ и ZUP.

### EA Elektro-Automatik

Основанная в 1974 году в городе Фирзене Гансом Гельмутом Нольденом как семейная компания, EA Elektro-Automatik развилась в фирму с глобальным присутствием и дилерской сетью по всему миру. Компания EA Elektro-Automatik специализируется на разработке и производстве мощных программируемых источников питания и электронных нагрузок, а также ИБП и зарядных устройств. EA Elektro-Automatik в настоящее время – лидер среди немецких производителей лабораторных источников питания.

Центральный офис компании, как и основное производство, по-прежнему находятся в городе Фирзене. Изделия EA Elektro-Automatik востребованы в области научных разработок, испытаний и измерений, контроля и обеспечения процессов производства. Линейка изделий EA Elektro-Automatik включает:

- программируемые источники питания переменного тока;
- программируемые лабораторные источники питания постоянного тока, в том числе двунаправленные и высоковольтные;
- электронные нагрузки, в том числе программируемые и с функцией рекуперации энергии;
- зарядные устройства для аккумуляторных батарей;
- источники бесперебойного питания переменного и постоянного тока;
- 19″ 3U еврокассетные источники питания.

Программируемые источники питания постоянного тока EA Elektro-Automatik имеют мощность от 100 Вт до 300 кВт при напряжении до 12 000 В и токе до 510 А; электронные нагрузки работают в диапазоне мощностей от 75 Вт до 105 кВт при напряжении до 1500 В и токе до 600 А. Производятся также блоки бесперебойного питания мощностью до 500 Вт с монтажом на DIN-рейку.

Компания может похвастаться существенными техническими новшествами, являющимися плодом собственных разработок, а среди её клиентов такие именитые фирмы, как Airbus, Audi, BMW, Daimler, Opel, Porsche, VW, Siemens, Osram, Kärcher, Black & Decker, Philips и многие другие. Соответствие качества бизнес-процессов стандарту DIN EN ISO 9001:1994 в компании впервые подтверждено службой сертификации TÜV Rheinland ещё в декабре 1998 года, а периодически проводимые повторные аудиты служат гарантией качества и сегодня.

На примере продуктов EA Elektro-Automatik мы и рассмотрим более предметно свойства и применение программируемых источников и электронных нагрузок.

## Программируемые двунаправленные источники питания серии EA-PSB-9000 3U

Эти источники питания обладают следующими характеристиками:

- широкий входной диапазон 360–528 В;
- источник питания и электронная нагрузка интегрированы в едином конструктиве;
- технология рекуперации с высоким КПД;
- мощность от 5 до 240 кВт;
- напряжение от 60 до 1500 В;
- токи от 30 до 360 А;
- множество функций защиты;
- сенсорная TFT-панель управления;
- гальванически изолированный аналоговый интерфейс;
- интегрированный функциональный генератор;
- симуляция работы солнечной батареи.

Все они управляются микропроцессорным блоком. Совмещение в едином конструктиве источника питания и рекуперативной электронной нагрузки позволяет добиваться уникальных характеристик изделий. В частности, приборы обеспечивают стандартную работу в двухквадрантном диапазоне, а также обладают функциональностью Power Sink (ZH) и High Speed (HS), о чём мы расскажем чуть позже. Встроенная электронная нагрузка обеспечивает высокую динамику выходных параметров даже на холостом ходу. Источники этой серии являются автодиапазонными, то есть они способны интеллектуально регулировать выходные токи и напряжения для поддержания максимальной мощности в нагрузке. Приборы снабжены активным корректором коэффициента мощности и рассчитаны на питание от двух- или трёхфазной сети переменного тока. Для защиты от перенапряжения, превышения допустимого тока и мощности в нагрузке доступны соответствующие защитные функции. Превышение заданного порога по любому из параметров вызовет отключение источника. Общий вид устройств приведён на рис. 4.

### Авторанжирование выходных диапазонов

Лабораторные источники питания EA мощностью от 1 кВт и выше имеют автодиапазонный выход. Эта гибкая выходная функция позволяет испытывать гораздо большее число нагрузок с различными номинальными напряжениями в сравнении

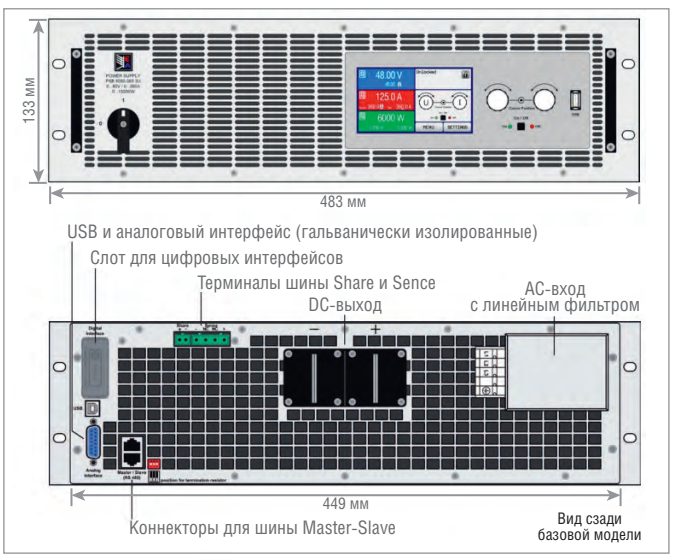



**Рис. 4. Общий вид программируемого источника питания серии EA PSB 9000 3U**

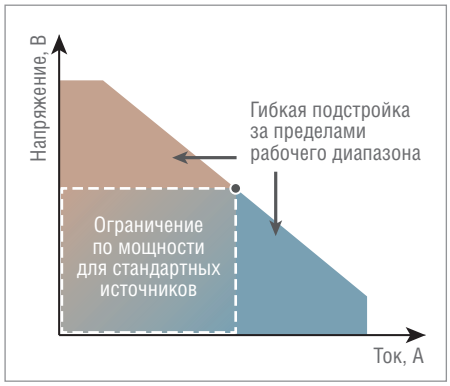



Рис. 5. Авторанжирование рабочих диапазонов

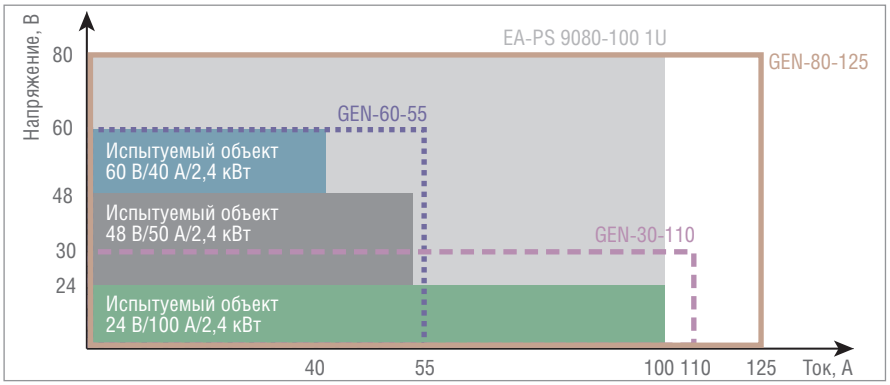



Рис. 6. Иллюстрация преимущества источников с технологией авторанжирования

с традиционными лабораторными источниками питания. Кроме того, в сравнении с традиционными блоками питания автодиапазонные источники питания обеспечивают до трёх раз больше мощности при работе в определённых диапазонах напряжений. Показательным примером «нехорошей» нагрузки является двигатель постоянного тока, работающий от регулируемого источника питания. В данном случае способность программируемого источника обеспечивать повышенный ток при уменьшенном выходном напряжении очень полезна. Эту способность ещё называют автоматическим ранжированием (рис. 5). Для тестирования испытуемого устройства при переменном входном напряжении могут потребоваться несколько источников питания, не обладающих данной функциональностью. В качестве примера, демонстрирующего это преимущество источников EA, рассмотрим задачу тестирования трёх нагрузок с различными параметрами входных токов и напряжений, но потребляющих одинаковую мощность. Тестирование этих нагрузок схематически представлено на рис. 6. Как показано на рисунке, все три нагрузки потребляют мощность 2,4 кВт, но токи и напряжения питания у них различные. Чтобы покрыть всё требуемое поле токов и напряжений, используя, например, обычные источники питания производства TDK-Lambda серии GEN, нам потребуются два разных устройства либо одно с гораздо большим запасом по мощности (10 кВт), а значит, более дорогое. Благодаря наличию функции авторанжирования всего лишь один 3-киловаттный источник EA PS 9080-100 1U легко справляется с поставленной задачей.

## Рекуперация энергии в устройствах E-Load

Новая серия электронных нагрузок постоянного тока ELR с восстановлением энергии обеспечивает уникальные характеристики напряжения, тока и мощности. Эти устройства функционируют в четырёх общих режимах работы: постоянный ток, мощность, напряжение и сопротивление. Кроме того, система управления на основе ПЛИС обеспечивает дополнительные возможности, такие как генератор функций, который по сути является схемой регулирования на основе таблицы для моделирования нелинейных внутренних сопротивлений. Благодаря аппаратуре, управляемой DSP, улучше-

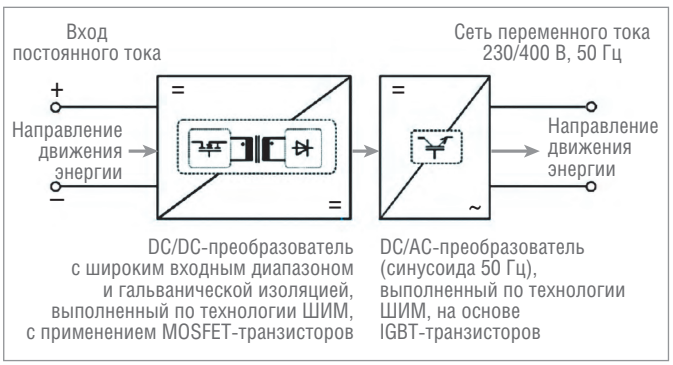



Рис. 7. Процесс обратного преобразования энергии

но время отклика при управлении через аналоговые или цифровые интерфейсы. Несколько устройств серии ELR-9000 могут работать параллельно в конфигурации ведущий-ведомый, что даёт возможность увеличения совокупной мощности до 105 кВт. Но существует одно обстоятельство, которое, несмотря на то что обычные нагрузки могут рассеивать высокую мощность, определяет их существенный недостаток: с повышением уровня мощности рассеивание энергии становится затруднительным и совсем не привлекательным вариантом для некоторых клиентов, поскольку это, безусловно, подразумевает не столь экологичный или «зелёный» подход. Решение, реализованное в устройствах серии ELR, делает нагрузки регенеративными или энергореактивными. Наиболее важной особенностью таких электронных нагрузок является то, что подключение к сети переменного тока используется также в качестве выхода для обратной подачи возвращаемой энергии постоянного тока, которая будет преобразована с эффективностью до 95%. Восстановление энергии позволяет снизить энергозатраты и (что крайне важно) избежать применения дорогостоящих систем охлаждения, требуемых для обычной электронной нагрузки, преобразующей входную энергию постоянного тока в тепло (рис. 7).

## Высокая удельная мощность

Для приборов EA характерна высокая удельная мощность, что позволяет компактно размещать источники и нагрузки в


Рис. 8. Приборы EA обладают высокой удельной мощностью

стойках (рис. 8). В табл. 1 для иллюстрации приведены мощности и габаритные параметры других моделей источников при одинаковой мощности на выходе.

## Встроенный функциональный генератор

Встроенный в модели серии 9000 функциональный генератор позволяет моделировать целый ряд функций применительно к выходным токам или напряжениям источника (рис. 9). Это очень полезная способность для проведения испытаний по сложным сценариям, в том числе тестов на отказоустойчивость электрооборудования, тестов автомобильной электрики, тестов фотоэлектрических установок и топливных элементов (рис. 10). В дополнение к реализованным стандартным функциям можно построить собственную кривую выходного тока или напряжения по 99 произвольно задаваемым отрезкам. Координаты можно загрузить в программируемый источник посредством имеющегося порта USB с флэш-носителя.

## Параллельная работа

Все источники имеют цифровую шину, благодаря которой возможна синхронизация и работа в режиме ведущий-ведомый до 16 источников одинаковых моделей (рис. 11). Параметры параллельной работы можно задать как на панелях самих источников, так и дистанционно посредством программного обеспечения с интуитивно понятным графическим интерфейсом, функционирующего в среде ОС Windows. Вся связка параллельных источников при этом управляется через интерфейс ведущего блока.

## Опциональные интерфейсы

На задней панели источников располагается свободный слот для опционального подключения цифровых интерфейсных модулей. Подключённый модуль распознаётся устройством автоматически и требует лишь минимальной конфигурации. Доступны интерфейсные модули RS-232, CAN, CANopen, Modbus TCP, Profibus, Profinet IO, EtherCAT, Ethernet. Имеется также аналоговый интерфейс (0...5/0...10 В) (рис.12).

## Функция наблюдения за параметрами

Все модели источников снабжены функцией наблюдения (Supervision), позволяющей отслеживать токи и напряжения (а также их изменение во времени) на выходе. При отклонении параметра более чем на заданное значение оператор получит сигнал предупреждения.

## Программное обеспечение

Все приборы, включая источники и электронные нагрузки, работают под управлением ПО EA EasySoft, являющегося набором программных средств для дистанционного мониторинга и управления. Программное обеспечение является бесплатным, но подлежит лицензированию (рис. 13, 14).

*Таблица 1*

**Сравнительные массогабаритные характеристики приборов одинаковой мощности**

| Нагрузки | ELR9080-510 HP | АКИП-1346 | AEL-8816 |
|---|---|---|---|
| Мощность | 15 кВт | 15 кВт | 15 кВт |
| Высота | 3U | 14U | 42U |
| Вес | 32 кг | 170 кг | 300 кг |
| Удельная мощность | 5 кВт/ 1U | 1 кВт/ 1U | 0,35 кВт/ 1U |

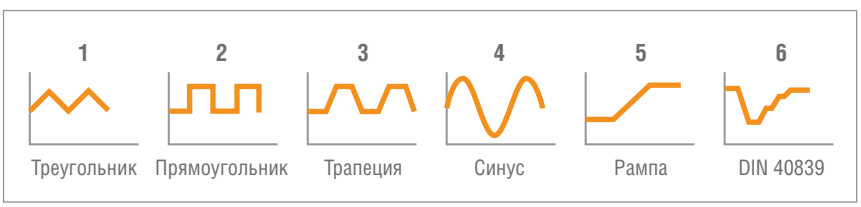



**Рис. 9. Типовые выходные функции тока или напряжения на выходе источников EA**

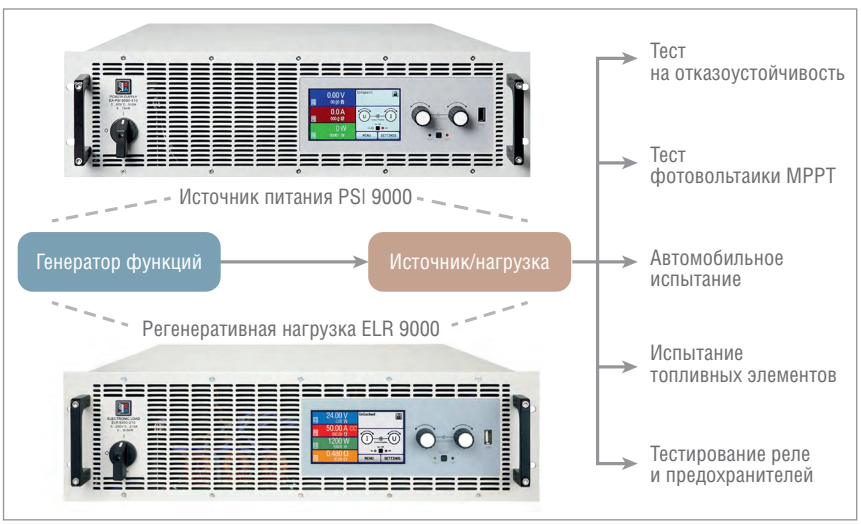



**Рис. 10. Встроенный функциональный генератор расширяет возможности источника**

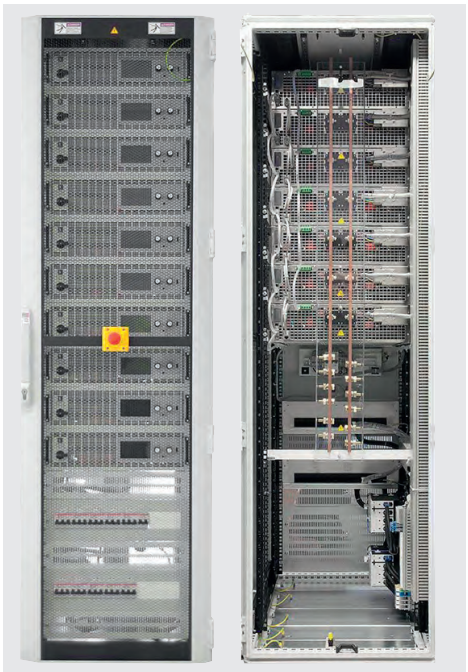


**Рис. 11. Стойка с работающими параллельно источниками питания**

**Рис. 12. Модули опциональных интерфейсов источников EA**


Рис. 13. Интерфейс программы EAsyPower

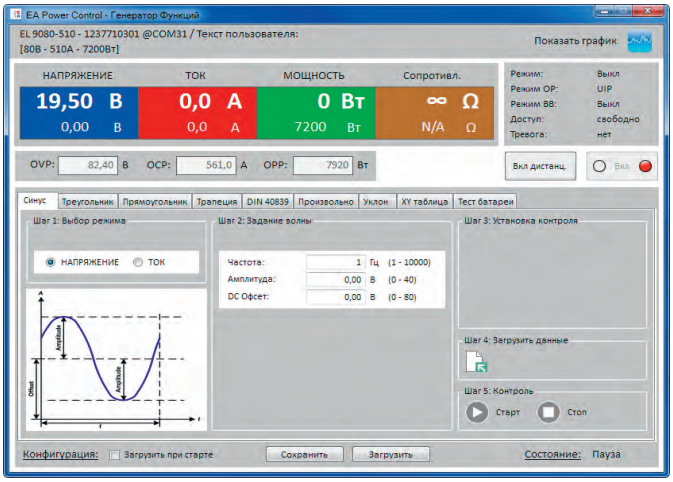



Рис. 14. Интерфейс программы EA Power Control. Генератор функций

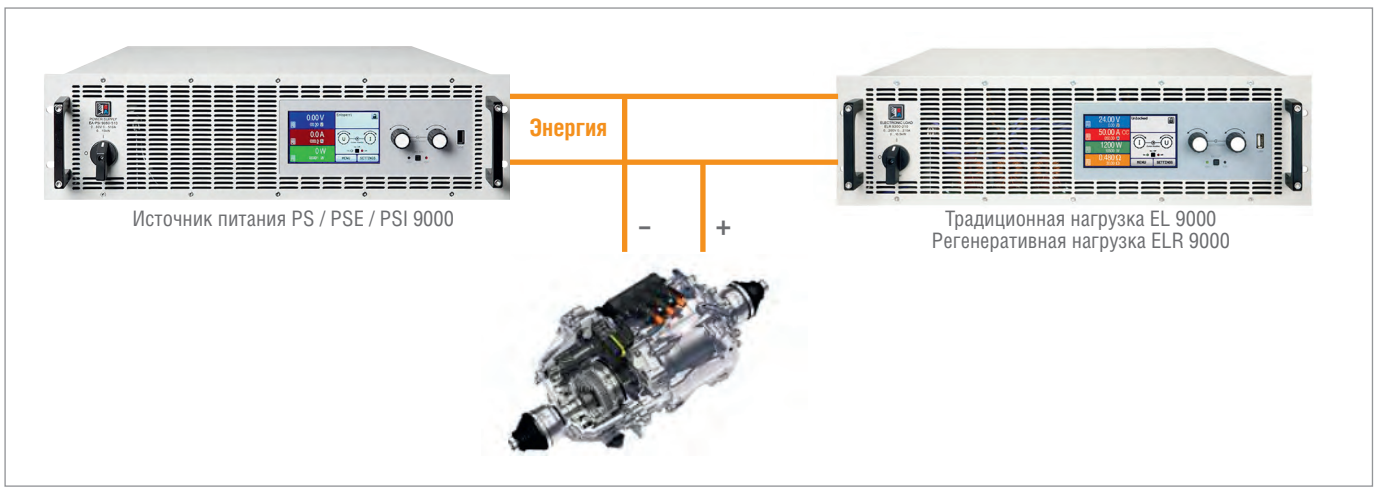



Рис. 15. Двухквадрантное функционирование

## Применение

Многие программируемые источники питания являются высокоточными средствами измерения, поэтому могут использоваться в метрологии для поверки других источников и измерительных приборов, а также в технологических процессах, требующих гарантированной точности задания параметров по установленной программе. Эти импульсные источники питания с регулируемым диапазоном от нуля до номинального значения широко применяются, к примеру, для симуляции работы аккумуляторных батарей автомобилей. С их помощью можно проводить испытания бортового оборудования в условиях, максимально приближенных к естественным, включая имитацию разрядки/зарядки АКБ, «просадки» напряжения на её выходе при резком увеличении нагрузки, работу в связке с автомобильным генератором и электродвигателями с системой рекуперации (торможения), рис. 15. Двухквадрантная схема работы (рис. 16) достигается благодаря совместному функционированию источника и электронной нагрузки, связанных по встроенной шине System Bus. Связанные таким образом приборы могут управляться с компьютера, в то время как в системе ведущим является источник питания. При этом допустима работа в квадрантах I и II (рис. 17) при положительной полярности выходного напряжения источника. Такая схема применима для тестирования широкого спектра реактивных нагрузок (дроссели, катушки индуктивности, моторы постоянного тока, конденсаторные и аккумуляторные батареи, контакторы и т.п.).

А вот для тестирования автомобильного оборудования в реальных условиях предусмотрен даже специальный режим работы источника – функция DIN 40839 (график 6 на рис. 9). Данная функция симулирует поведение аккумуляторной батареи автомобиля во время пуска двигателя. Кривая строится из 5 участков со стандартными значениями выходных напряжений. В этом режиме используется электронная нагрузка, которая и формирует заданную кривую напряжения на выходе при постоянном выходном напряжении источника питания с ограничением тока нагрузки. Серия источников ELR как нельзя лучше подходит для решения описанных задач благодаря встроенной функции Power Sink (поглощение энергии). За данную функцию отвечает опциональный ZH-модуль. Силовые функции Power Sink реализованы в виде каскада мощных MOSFET-транзисторов, на которых может рассеиваться энергия, поступающая в источник в обратном направлении. Структура модуля Power Sink приведена на рис. 18. Силовым модулем управляет встроенная логика, за-

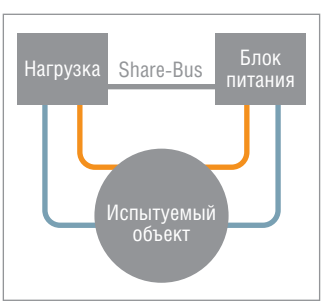



Рис. 16. Подключение источника, испытуемого объекта и нагрузки по двухквадрантной схеме

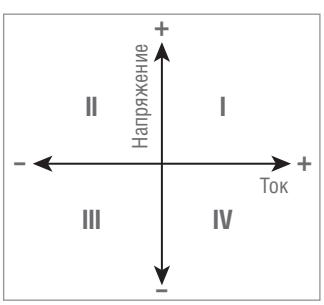



Рис. 17. Условное деление областей работы на квадранты

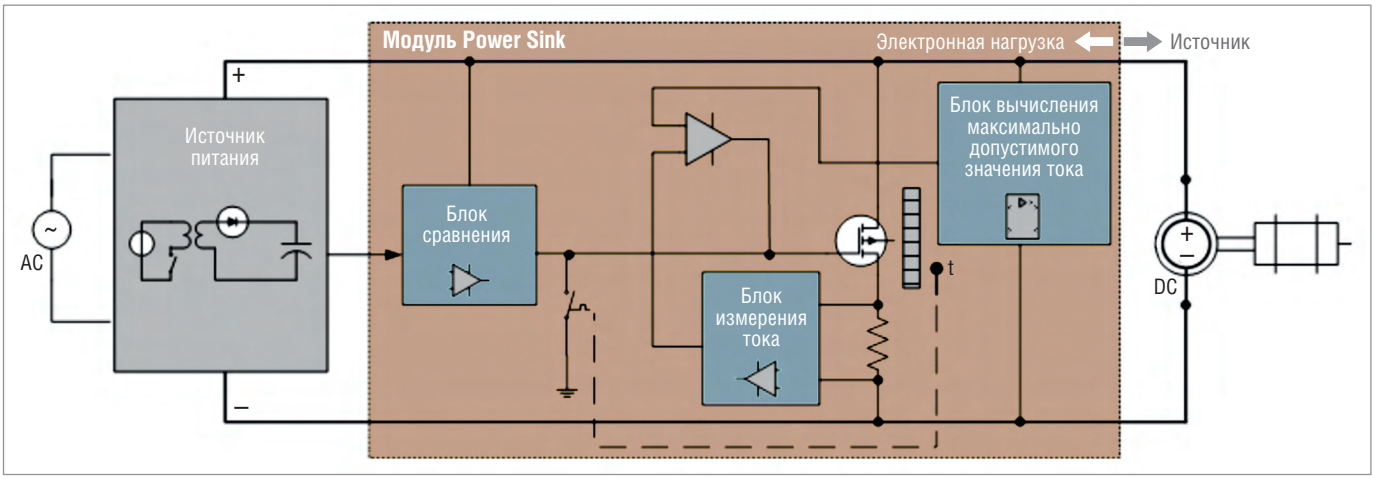



**Рис. 18. Блок-схема модуля Power Sink**

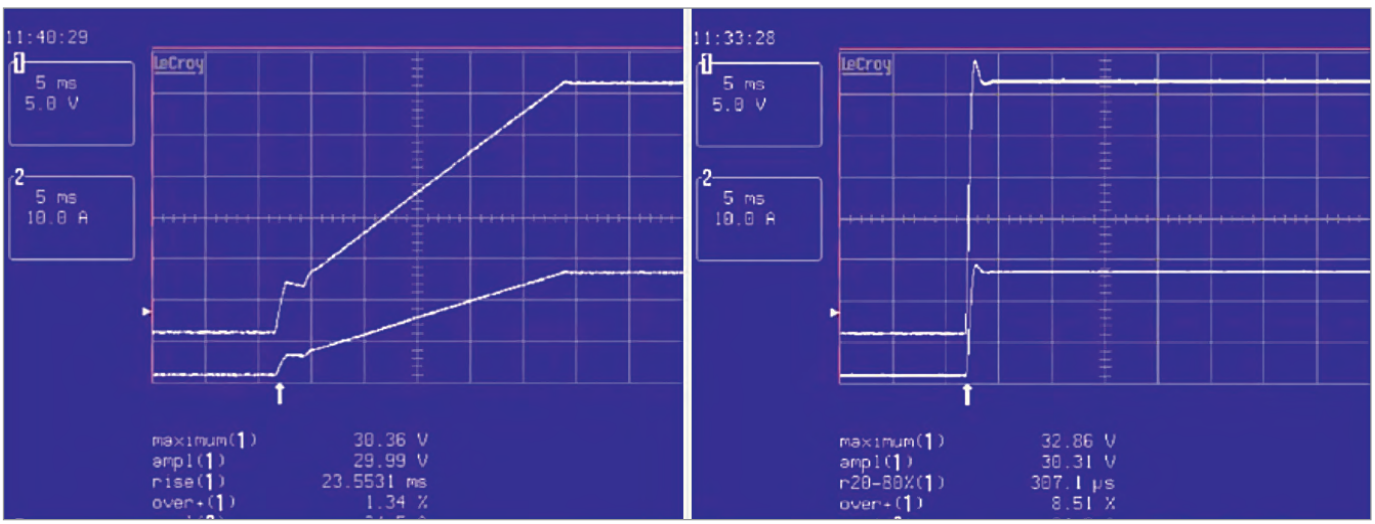



**Рис. 19. Иллюстрация действия опции High Speed: слева – опция отключена, справа – включена**

дачей которой является обнаружение обратного потока энергии и включение электронной нагрузки. Этот же опциональный ZH-модуль может быть использован и для достижения крутого фронта по выходному напряжению на холостом ходу источника. Модуль способен принимать и рассеивать пиковую мощность до 2400 Вт. Если требуется и крутой фронт по нарастанию напряжения на выходе источника, то в некоторых моделях предусмотрена функция High Speed (высокое быстродействие). Функция реализуется также в виде опции (HS) и позволяет за счёт оптимизации ёмкости выходных цепей на порядок снизить время нарастания напряжения на выходе, добиваясь (в комбинации с внешней электронной нагрузкой) нарастания от нуля до 100% менее чем за 1 миллисекунду. При этом надо помнить, что снижение ёмкости выходных цепей источника неминуемо ведёт к повышению уровня пульсаций напряжения на выходе. На рис. 19 приведены сравнительные осциллограммы источников без опции High Speed (слева) и с этой опцией (справа).

Широко применяются программируемые источники в электрохимическом производстве, где обслуживают установки гальванопластики и коррозионной защиты. В электротехническом производстве программируемые источники активно применяются для тестирования производимых электронных компонентов, ячеек аккумуляторных батарей, топливных элементов, электродвигателей. В производстве полупроводников программируемые источники применяются для питания установок выращивания кристаллов, а в такой области, как производство энергосистем на основе солнечных батарей, программируемые источники и нагрузки оказались просто незаменимыми для тестирования оборудования: автономные солнечные энергоустановки немыслимы сегодня без специализированных источников-драйверов. Применение, сходное с автопромом, нашли программируемые источники питания и в авионике, а в научно-исследовательских лабораториях они обеспечивают энергией сложные и требовательные к электропитанию лабораторные установки (например, мощные лазерные установки, плазменные и прочие импульсные генераторы). Сами же производители источников питания широко используют электронные нагрузки для тестирования собственных изделий.

## Заключение

Мы рассмотрели лишь одну линейку изделий, не коснувшись других интересных продуктов, таких как маломощные лабораторные источники, программируемые источники переменного тока, регулируемые источники постоянного тока высокой мощности – до 240 кВт и более. Все они также присутствуют в программе поставок EA Elektro-Automatik. Если у вас возникли вопросы о модельном ряде изделий, их характеристиках или применении, пожалуйста, обращайтесь к официальному дистрибьютору EA Elektro-Automatik в России – компании ПРОСОФТ.

**E-mail: textoed@gmail.com**

# КОМПЛЕКСНЫЕ ПОСТАВКИ ИБП


## ПОСТАВКА, ПУСКОНАЛАДКА, ИНТЕГРАЦИЯ

**Широкий ассортимент ИБП, включая модели:**

- для альтернативной энергетики
- для приложений с нестабильным основным питанием

PROSOFT®
WWW.PROSOFT.RU

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

**МОСКВА**
(495) 234-0636
info@prosoft.ru

**САНКТ-ПЕТЕРБУРГ**
(812) 448-0444
info@spb.prosoft.ru

**ЕКАТЕРИНБУРГ**
(343) 356-5111
info@prosoftsystems.ru

УЗНАТЬ БОЛЬШЕ

# Работа со SCADA-системой GENESIS64: просто о сложном

Ольга Власенко

Одно из качеств хорошей SCADA-системы – гибкость. Рассматриваемые в статье вопросы наглядно показывают, что GENESIS64 в полной мере обладает этим качеством. Вывести нужный бит из тега, настроить форматы отображения даты и времени, создать всплывающее окно и многое другое можно буквально двумя щелчками мыши.

## Вопрос

**Можно ли в GraphWorX64 вывести на экран отдельный бит тега? Например, есть тег с типом Integer, который передаёт значение 8, по битам 1000. Можно ли обратиться к битам этого тега и увидеть, что 4-й бит имеет значение 1?**

## Ответ

Можно использовать функцию *bittest* в редакторе выражений, которая имеет следующий синтаксис:

*x = bittest (number, bitIndex)*,

где *number* – локальная переменная (тег); *bitIndex* – номер бита в теге. Отсчёт битов ведётся с 0 справа.

Например, на экран GraphWorX64 выведена точка процесса, подключённая к OPC-тегу *{{@ICONICS.Siimulator.1\GlobalVariables.Analog1.Value}}*. Тег имеет тип данных 8-bit Interger и передаёт значение 8. Для получения значения 4-го бита выражение имеет вид, представленный на рис. 1.

Результатом выражения будет значение бита на экране (рис. 2).

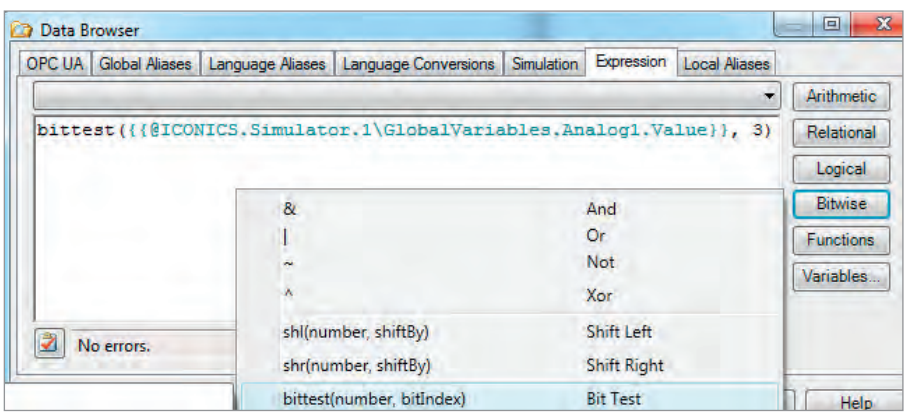



**Рис. 1. Функция *bittest* в редакторе выражений GraphWorX64**

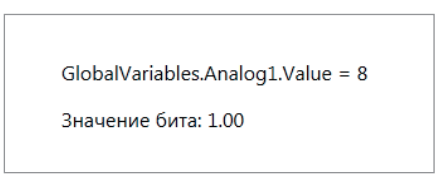



**Рис. 2. Результат, возвращаемый функцией *bittest***

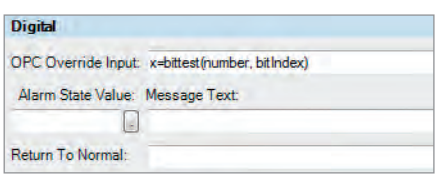



**Рис. 3. Использование функции *bittest* в AlarmWorx64**

## Вопрос

**Как создать битовую аварию? При программировании ПЛК кодировали аварии в одну переменную по битам, всего 16 бит. Теперь в AlarmWorX64 Viewer требуется контролировать нужный бит и, если он выставлен, выводить сообщение об аварии.**

## Ответ

Для решения этой задачи можно использовать описанную функцию *bittest*, указав необходимое выражение в AlarmWorX64 Server на вкладке *Alarms Limit/ Digital* в группе *Digital* в поле *OPC Override Input* (рис. 3). В поле *AlarmState-*

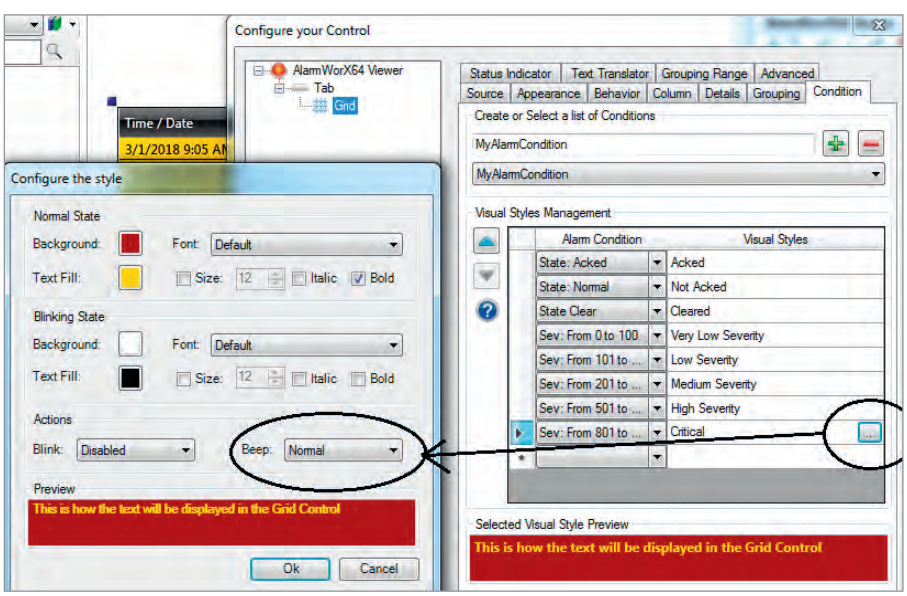



**Рис. 4. Настройка звукового сигнала в AlarmWorX64 Viewer**

*Value* введите 1, а в поле *MessageText* – сообщение об аварии.

### Вопрос

**Какие виды звуковых сигналов можно установить для уведомления об аварии в GENESIS64?**

### Ответ

В приложении для отображения тревог и событий AlarmWorX64 Viewer существует возможность настройки звукового уведомления об авариях для каждого типа тревог. Это выполняется в окне конфигурации свойств AlarmWorX64 Viewer для элемента *Grid* на вкладке *Condition* (рис. 4). Здесь можно включить и настроить длительность звукового сигнала (Normal, Slow, Fast).

В качестве сигнала можно использовать системный звук или загрузить свой звуковой файл – один для всей таблицы. Он прописывается в свойствах самого AlarmWorX64 Viewer на вкладке *Advanced* в параметре *BeepFileLocation* (рис. 5).

Однако следует учесть, что звук аварии будет воспроизводиться только при активном компоненте AlarmWorX64 Viewer, то есть когда он находится на активном слое, не запрещён системой безопасности и виден на экране оператора.

### Вопрос

**Как настроить вывод даты и времени события (тревоги) в русском формате дд.мм.гггг чч:мм вместо мм.дд.гггг (AM/PM) ч:мм для AlarmWorX64 Viewer?**

### Ответ

Для настройки формата времени и даты в таблице тревог AlarmWorX64 Viewer необходимо для элемента *Grid* на вкладке *Advanced* прописать требуемый формат в поле *DataTimeFormat*, например, для нашего случая нужно указать: *dd.MM.yyyy HH:mm* (рис. 6). Отображение столбца время/дата (Time/Date) в AlarmWorX64 Viewer в заданном формате приведено на рис. 7.

### Вопрос

**Что такое точка подключения в GENESIS64, и как правильно подсчитать точки подключения в проекте?**

### Ответ

Точкой ввода-вывода в системе ICONICS GENESIS64 является соединение любого программного компонента GENESIS64 с тегом в OPC-сервере, локальном и/или удалённом, представляющем простейший элемент данных, включая значение на канале ввода-вывода. Одновременное соединение и взаимодействие нескольких приложений с одним и тем же OPC-тегом в сервере OPC рассматривается как одна активная точка. Просмотреть количество подключённых точек можно с помощью приложения MonitorWorX64. Запускается это приложение через главное меню Пуск → ICONICS Licensing → ICONICS.NET Licensing → MonitorWorX Viewer. В режиме исполнения (Runtime) в таблице MonitorWorX64 будут отображены точки, подключённые в проекте в реальный момент времени – именно их количество считается в лицензии (рис. 8).

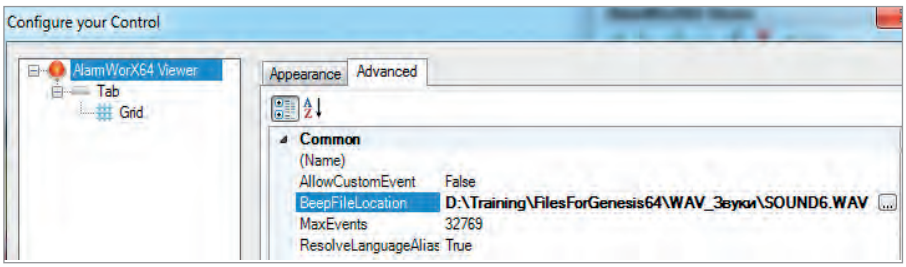



**Рис. 5. Загрузка звукового файла в AlarmWorX64 Viewer**

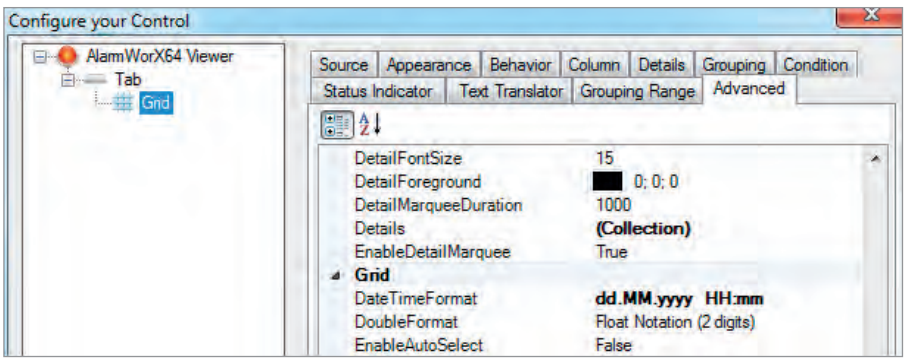



**Рис. 6. Настройка формата время/дата (Time/Date) в AlarmWorX64 Viewer**

| Time / Date | Tag | Priority | Type |
|---|---|---|---|
| 14.03.2018 10:44 | Valve1 | 600 | HI |
| 14.03.2018 10:45 | VCR_Pump Speed | 500 | HI |
| 14.03.2018 10:33 | Tank1 | 900 | LOLO |
| 14.03.2018 10:47 | Tank PSI | 625 | LOLO |
| 14.03.2018 10:45 | Smoke Detector 1 | 900 | Digital |
| 14.03.2018 10:33 | Scale | 700 | LOLO |

**Рис. 7. Отображение столбца время/дата (Time/Date) в AlarmWorX64 Viewer в заданном формате**

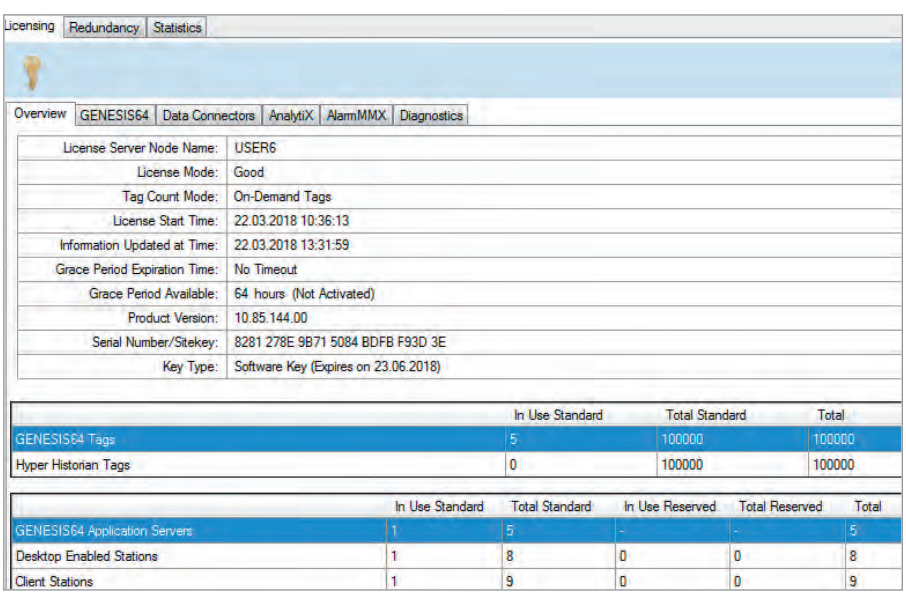



**Рис. 8. Просмотр точек подключения в MonitorWorX**

## Вопрос

**Существует ли возможность при возникновении аварии показывать всплывающее окно с сообщением?**

## Ответ

Для решения этой задачи возможны следующие варианты:

1. Использовать опцию *Default Display* в AlarmWorX64 Server. Для этого необходимо сохранить желаемое сообщение (инструкции оператору, описание технических характеристик объекта, и т.п.) в файле формата .htm и выбрать его через браузер данных в поле *Default Display* при настройке тега тревоги в AlarmWorX64 Server (рис. 9).
   Далее настраиваем в AlarmWorX64 Viewer поле подписки *Server Fields: DEFAULT_DISPLAY* (рис. 10). На вкладке *Column* настраиваем общий вид столбца – его ширину и положение в таблице. Теперь файл с сообщением появится в виде ссылки в столбце *DEFAULT_DISPLAY* в таблице тревог AlarmWorX64 Viewer (рис. 11а), оператор при необходимости может перейти по ссылке к требуемой информации (рис. 11б).
   Если на вкладке *Column* включить опцию *Contains a clickable link* и ввести произвольный текст ссылки или принять по умолчанию общую фразу *Click here*, то ссылка появится во всех строках независимо от того, настроена ли она в AlarmWorX64 Server. Будьте внимательны при использовании данной опции.
2. В качестве альтернативного варианта можно использовать динамику Hide (скрытие) для объектов в GraphWorX64. Наиболее простой вариант – создать графический элемент (или слой, на котором размещены необходимые элементы) с требуемым сообщением, которое будет появляться при выходе значения OPC-тега за предельные границы (рис. 12). В этом случае не надо даже привязываться к серверу тревог.
   Если сообщение необходимо выводить строго при возникновении аварии в соответствии с настройками тега тревог в AlarmWorX64 Server, то динамику Hide можно привязать к атрибуту тега, отвечающего за состояние тревоги *LIM_Active* или к атрибуту квитирования *LIM_Acked*. Атрибут *LIM_Active* равен 1 при наличии тревоги. Атрибут *LIM_Acked* принимает значение 1 при квитировании тревоги оператором (при возврате OPC-тега в нормальное состояние значение 1 сохраняется) и принимает значение 0, когда тревога возникла, но ещё не квитирована.

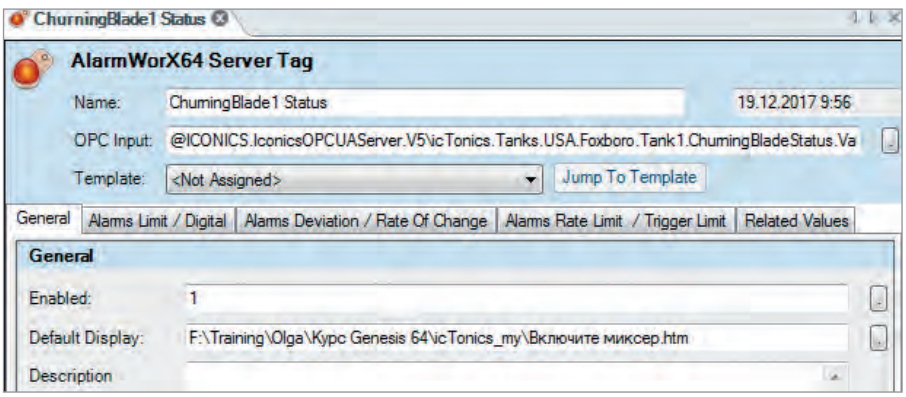



**Рис. 9. Опция *Default Display* в AlarmWorX64 Server**

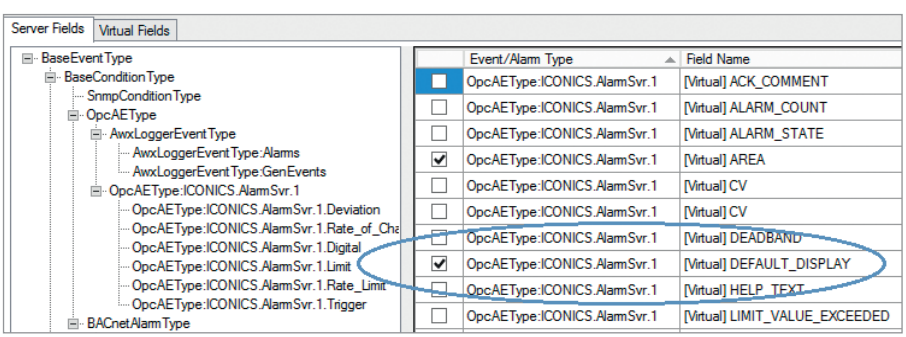
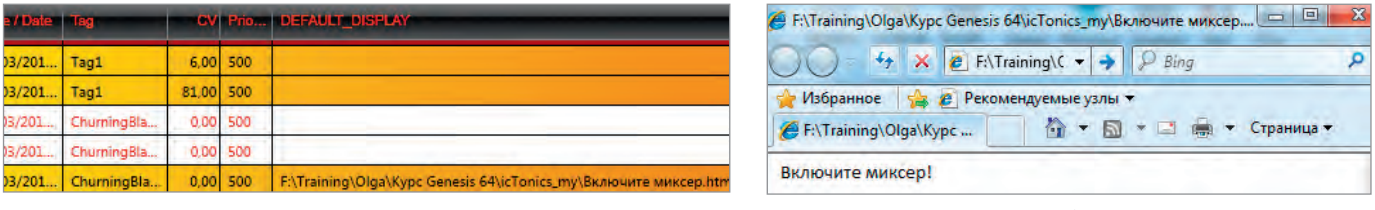



**Рис. 10. Настройка подписки на поле *DEFAULT_DISPLAY***




*а* *б*

**Рис. 11. Ссылка на файл в AlarmWorX64 Viewer: *а* – отображение настроенного столбца *DEFAULT_DISPLAY*; *б* – файл с сообщением в браузере**

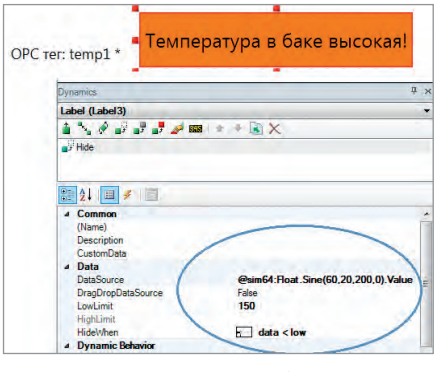



**Рис. 12. Динамика скрытия сообщения по значению OPC-тега**

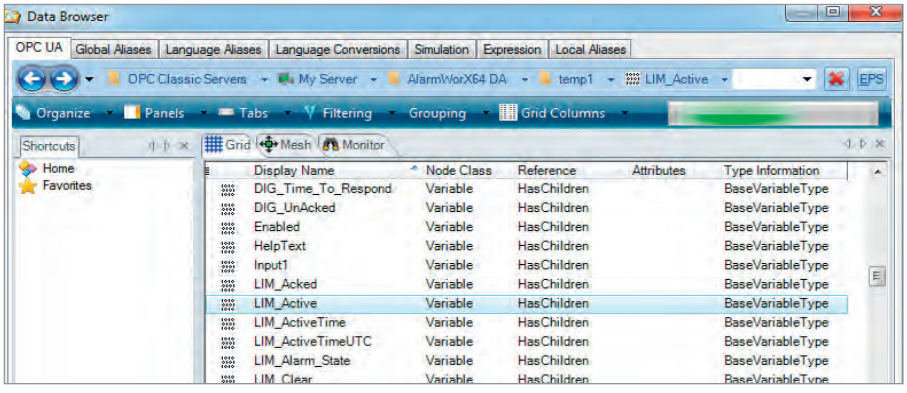



**Рис. 13. Выбор атрибутов тега через Data Browser**

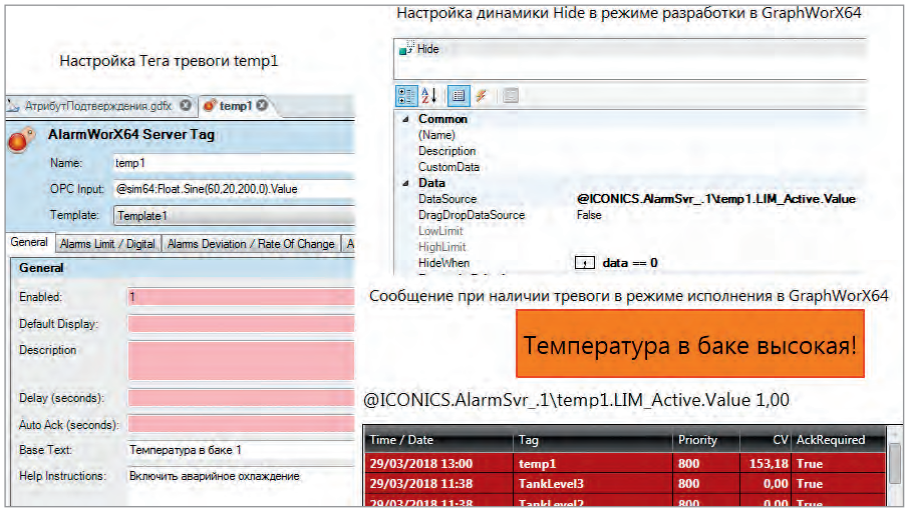



**Рис. 14. Вывод сообщения при наличии тревоги**

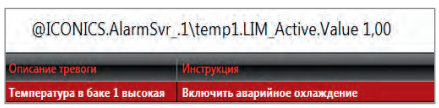



**Рис. 15. Всплывающий элемент тревог AlarmWorX64 Viewer**

Эти атрибуты можно выбрать через браузер данных (Data Browser) по следующему пути: *Home\OPC Classic Server\My Server\ AlarmWorX64 DA\ <имя тега>\<атрибут>* (рис. 13).

На рис. 14 приведён пример настройки всплывающего сообщения по атрибуту *LIM_Active* для тега тревоги *temp1*. Для создания эффекта всплывающего окна можно воспользоваться динамикой Size (изменение размера) вместо Hide. Таким же образом можно настроить всплывающую таблицу тревог, например, настроенную только на отображение столбцов *Описание тревоги* и *Инструкция* (рис. 15).

## Вопрос

**В конфигурации OPC-сервера создаётся OPC-тег с типом данных String. В TrendWorX64 Logger создаётся конфигурация с сохранением этого тега в архиве. Почему при попытке извлечь данные с помощью ReportWorX Express извлекаются нулевые значения?**

## Ответ

В приложении TrendWorX64 Logger нет возможности архивировать строковые данные. Для этой цели надо использовать Hyper Historian или Hyper Historian Express (в версии 10.9 и выше). Если «строка» представляет собой число, её в TrendWorX64 Logger надо хранить в виде числа. Другой способ – архивировать «строку» с помощью AlarmWorX64 Logger. Строковые данные сохраняются в поле *RelatedValues*, прикреплённом к специально выделенному для этих целей тегу тревоги и настроенному на определённые условия архивации.

**Автор – сотрудник фирмы ПРОСОФТ**
**Телефон: (495) 234-0636**
**E-mail: info@prosoft.ru**

## Контроллер VIPA MICRO PLC получил награду iF DESIGN AWARD


Около 2 000 гостей посетили 9 марта в Мюнхене презентацию международных наград “iF DESIGN AWARDs”. Среди победителей в этом году был MICRO PLC от Vipa Controls Yaskawa.

Ежегодно на протяжении 65 лет iF International Forum Design GmbH (Ганновер) присуждает награды достойнейшим. Признанием отмечены достижения в таких дисциплинах, как дизайн продуктов, дизайн упаковки, коммуникации и дизайн услуг, архитектурный и дизайн интерьера, а также профессиональные концепции. В 2018 году на конкурс было подано 6402 заявки из 54 стран в семи дисциплинах.

Компактный контроллер MICRO PLC получил награду за дизайн продукта. Система управления MICRO PLC Yaskawa впервые была представлена миру в 2016 году. Её отличают чрезвычайно компактные размеры корпуса и удобство в эксплуатации.

Полностью переработанная концепция отображения состояния каждого из каналов позволяет пользователю мгновенно отслеживать важную информацию о состоянии всей системы. Вместе с тем ширина процессорного модуля чуть меньше 72 миллиметров, что более чем на 50% компактнее, чем у сопоставимых контроллеров. В то же время MICRO PLC демонстрирует исключительную производительность. Технология SPEED7, характерная для всех ПЛК Vipa Controls, обеспечивает максимальную вычислительную мощность и быстрое выполнение программы.

Пропускная способность системной шины до 48 Мбит/с в сочетании с широчайшими коммуникационными возможностями даёт дополнительные преимущества пользователям. Это делает MICRO PLC одним из самых быстрых микроконтроллеров, доступных в настоящее время на рынке, и позволяет MICRO PLC справляться с задачами управления за пределами своей «весовой категории». ●

## ПРОСОФТ и FASTWEL на семинаре «Технологии QNX и КПДА в России»

25 апреля в Москве в гостиничном комплексе «Измайлово Альфа» прошло ежегодное специализированное мероприятие, организованное компаниями «СВД Встраиваемые Системы» и «СВД Софтвер» и целиком посвящённое применению защищённых ОС РВ семейств QNX и КПДА в системах ответственного назначения, а также ключевым трендам развития мировых технологий реального времени.

Традиционно высокий интерес к технологиям QNX у отечественных инженеров и разработчиков имеет под собой прочный фундамент. Сегодня, когда в мире существует множество разнообразных операционных систем, ОС QNX, в отличие от самой популярной ОС Windows, которая применяется в основном частными пользователями, задействована в управлении производствами и объектами с высочайшими требованиями к электронному оборудованию и системам автоматизации.

Кроме того, QNX управляет атомными станциями, сложными многофункциональными станками и другими важными промышленными и инфраструктурными объектами и системами.

Аудиторию мероприятия ждали доклады и мастер-классы по особенностям настройки и диагностики целевых и инструментальных систем, а также по разработке программного обеспечения для операционных семейств QNX и КПДА. В выставочной зоне были представлены новейшие программные и программно-аппаратные платформы.

Свою лепту в работу семинара внесли компании FASTWEL и ПРОСОФТ.

Алексей Уваров, ведущий инженер-программист российской компании FASTWEL – лидера в разработке электроники для ответственных применений, – представил доклад, в котором речь шла о том, как серийная и заказная электроника, в том числе созданная на базе отечественных процессоров «Байкал» и «Эльбрус», функционирует под управлением ОС РВ QNX.

Начальник технического отдела компании ПРОСОФТ Дмитрий Швецов в своём выступлении рассказал о решениях для промышленной автоматизации на базе платформ QNX, которые предлагаются в программе поставок компании.

Докладчик сделал акцент на главных преимуществах системы, в частности, на наличии в ней развитой среды разработки и интегрированного интерфейса POSIX, благодаря которому разработчик может использовать большое число стандартных инструментальных средств, включая бесплатные технологии GNU GDB и GCC, применяемые для разработки в ОС общего назначения. С этой точки зрения ОС QNX является одной из самых развитых систем реального времени.

Таким образом, благодаря высокой масштабируемости система может применяться как на небольших устройствах, встраиваемых в станок или конвейер, так и в огромных машинах или настольных компьютерах. ●

## 15-я международная выставка нефтегазового оборудования «НЕФТЬ И ГАЗ» / MIOGE

18–21 июня 2018 года в Москве в МВЦ «Крокус Экспо» состоится 15-я международная выставка нефтегазового оборудования «НЕФТЬ И ГАЗ» / MIOGE.

Международная выставка нефтегазового оборудования и технологий «НЕФТЬ И ГАЗ» / MIOGE – ведущее международное нефтегазовое бизнес-мероприятие в России, дающее возможность широкой аудитории специалистов отрасли ознакомиться с новейшими разработками, представленными лидерами отечественной и мировой нефтегазовой промышленности, а также установить прямые деловые контакты и решить задачи по развитию бизнеса.

В рамках технической программы выставки состоятся специализированные мероприятия, организованные российскими и международными отраслевыми ассоциациями и компаниями. Вход свободный. Необходимо выбрать мероприятие и зарегистрироваться на сайте выставки MIOGE.

Выставка «НЕФТЬ И ГАЗ» / MIOGE проводится с 1993 года. Выставка удостоена знака Всемирной ассоциации выставочной индустрии (UFI). Зарегистрироваться и получить бесплатный пригласительный билет можно на сайте MIOGE.

В рамках выставки проходит Российский нефтегазовый конгресс / RPGC. В нём традиционно принимают участие более 1000 представителей отечественной и международной нефтегазовой промышленности, в том числе руководители компаний-лидеров отрасли, отраслевых министерств и ведомств, нефтегазовых ассоциаций и финансово-инвестиционных компаний. ●

В этой рубрике мы представляем
новые аппаратные средства,
программное обеспечение и литературу.
Материалы рубрик «Демонстрационный зал»
и «Будни системной интеграции»
снабжены QR-кодами со ссылками
на соответствующие сайты.
QR-код можно «прочитать»
с помощью любого Smart-устройства
и утилиты сканирования кода.

Запросить дополнительную информацию можно,
заполнив карточку на сайте журнала
«Современные технологии автоматизации»:
www.cta.ru/demo

## FPU500 – реконфигурируемый вычислительный модуль на базе ПЛИС

УЗНАТЬ БОЛЬШЕ

Компания **FASTWEL** выпустила реконфигурируемый вычислительный модуль **FPU500**, который предназначен для построения высокопроизводительных бортовых систем сбора и цифровой обработки сигналов реального времени на платформе CompactPCI Serial 3U. Вычислительным ядром FPU500 является ПЛИС Virtex-6 с оперативной памятью объёмом 4 Гбайт. Интеграция FPU500 в вычислительную систему обеспечивается по шине PCI-E x8 Gen2.

Для ввода сигналов в систему предусмотрена возможность установки мезонинных модулей стандарта FMC различного функционального назначения, совместимых со спецификацией ANSI/VITA 57.1.

Типовые области применения реконфигурируемого вычислительного модуля FPU500 – это цифровая обработка сигналов (ЦОС), системы шифрации/дешифрации каналов данных, радарные комплексы, беспилотные комплексы, обработка видеопотоков, нейронные сети и т.д.

## Беспроводное устройство сбора и передачи данных WISE-4220

УЗНАТЬ БОЛЬШЕ

Компания **Advantech** запустила в производство новую серию беспроводных устройств ввода-вывода **WISE-4200**. Одним из первых доступен для заказа модуль WISE-4220-S231. Устройство поддерживает передачу данных по каналам Wi-Fi на частоте 2,4 ГГц по стандарту 802.11b/g/n, благодаря чему может легко интегрироваться в существующие сети без дополнительных затрат.

Отличительной особенностью модуля является наличие встроенных датчиков температуры и влажности. Максимальное расстояние между соседними узлами не должно превышать 110 м. Модуль конфигурируется мобильными устройствами напрямую без дополнительного программного обеспечения или приложений (стандарт HTML5). Использование функции журнала с отметкой времени RTC даёт нулевую потерю собранных данных. Вся информация может быть автоматически перенесена в облачный сервис или на компьютер.

WISE-4220-S231 – это оптимальное решение для сферы ЖКХ и систем управления климатом дома.


## AMD Ryzen V1000 в COM-модулях Advantech

УЗНАТЬ БОЛЬШЕ

Компания **Advantech** представила процессорный модуль формата COM Express Basic тип 6 – **SOM-5871**. Новинка выполнена на базе процессоров AMD серии Ryzen V1000 с низким энергопотреблением – от 12 до 54 Вт, что позволяет системе с пассивным охлаждением работать в расширенном диапазоне температур, до +60°C.

Линейка производится по технологии 14 нм и включает в себя двух- и четырёхъядерные модели с графическим ядром Vega, благодаря которому обеспечивается декодирование видео в различных форматах с разрешением UltraHD. Плата поддерживает подключение четырёх независимых дисплеев через видеовыходы VGA/LVDS/HDMI/DP.

Модуль с функциями безопасного шифрования памяти (SME) и защищённой виртуализацией на основе шифрования данных (SEV) поддерживает оперативную память DDR4 SODIMM с коррекцией ошибок (ECC). Поддержка iManager, WISE-PaaS/RMM и SUSI API позволяет осуществлять дистанционное управление и связывать системы с облачными сервисами.

## GQA 120 Вт – DC/DC-преобразователь промышленного класса

УЗНАТЬ БОЛЬШЕ

Корпорация **TDK** объявила о выходе серии DC/DC-преобразователей промышленного класса **GQA120**. Доступны модели с выходными напряжениями 5, 12, 15, 24, 28 и 48 В, допускающие подстройку до ±10% от номинала для получения требуемых нестандартных значений.

Модули способны работать в широком диапазоне питающих напряжений от 9 до 36 В DC (от 18 до 36 В DC для модели с выходным напряжением 48 В), а также выдерживают всплески до 50 В DC длительностью до 1 секунды без отключения. КПД источников достигает 91,5%, а диапазон рабочих температур составляет –40…+105°C на теплоотводящем основании. Все модели серии имеют размер корпуса и расположение выводов промышленного стандарта 1/4-Brick.

Новики ориентированы на широкий диапазон применений, в том числе в беспилотных транспортных средствах, портативной аппаратуре, высоконадёжном оборудовании связи, системах телеметрии на железнодорожном транспорте и в морской навигации.


## Высокопроизводительная рабочая станция IPC-SYS28FN

УЗНАТЬ БОЛЬШЕ

Новинка **AdvantiX**: 2U безвентиляторный компьютер **IPC-SYS28FN** для установки в 19″ стойку. Высокую производительность обеспечивает процессор Intel Core i5/i7 для чипсета QM77, встроенная видеосистема Intel HD Graphics 4000 (до 1 Гбайт, поддержка Dual Head) и возможность расширения объёма ОЗУ до 16 Гбайт (2×DDR3-1333/1600 с поддержкой ECC). Дисковая подсистема позволяет установить до 4×2,5″ HDD/SSD SATA с поддержкой «горячей» замены и RAID 0/1/10/5.

Предусмотрены слоты расширения 1×PCI-e x8 и 3×MiniPCIe, а также программируемый сторожевой таймер. На передней панели можно разместить до 10 закручивающихся разъёмов LAN M12 (Ethernet 10/100/1000, возможна поддержка PoE), а также порты USB, HDMI, RS-232/422/485 и DIO.

Предусмотрено множество вариантов электропитания для сетей постоянного и переменного тока. Диапазоны рабочих температур: –30…+70°C для AC-версии, –40…+70°C для DC-версии. Модель будет доступна для заказа с 2019 года.

## Компактная оперативная память DDR4 SODIMM от Apacer

УЗНАТЬ БОЛЬШЕ

**Apacer DDR4 SODIMM** 2400 МГц – четвёртое поколение оперативной памяти, являющееся эволюционным развитием предыдущих поколений DDR SDRAM. Отличается повышенными частотными характеристиками и пониженным напряжением питания.

Основное отличие DDR4 от предыдущего стандарта DDR3 заключается в удвоенном до 16 числе внутренних банков, что позволило увеличить скорость передачи внешней шины. Пропускная способность памяти DDR4 в перспективе может достигать 25,6 Гбайт/с (в случае увеличения максимальной эффективной частоты до 3200 МГц). Кроме того, повышена надёжность работы за счёт введения механизма контроля чётности на шинах адреса и команд.


*Основные характеристики*

- Тип модуля: SODIMM.
- Технология: DDR4.
- Частота: 2133/2400/2666 МГц.
- Ёмкость: 2/4/8/16 Гбайт.
- Напряжение: 1,2 В.
- Количество контактов: 260.
- Высота PCB: 1,18”.
- Диапазон рабочих температур 0…+85°C.

## Самый компактный неуправляемый коммутатор EKI-2525LI от Advantech

УЗНАТЬ БОЛЬШЕ

Компания **Advantech** представила новый неуправляемый 5-портовый промышленный Fast Ethernet-коммутатор **EKI-2525LI**. Со слов производителя, новинка является одним из самых компактных устройств подобного класса, представленных на рынке. Габариты составляют всего 25×80×84 мм. Высота корпуса сравнима с корпусами популярных ПЛК Siemens и Mitsubishi.

Несмотря на столь компактные размеры, функциональность полностью соответствует данному классу изделий. Это стандартный набор, позволяющий определить тип кабеля и скорость передачи данных, а также обеспечивающий визуализацию работоспособности.

Помимо этого производитель оснастил коммутатор резервированным входом по электропитанию (12–48 В DC), защитой от переполюсовки входного напряжения и перегрузки по току и дежурным реле контроля. Металлический корпус со степенью защиты IP40 предназначен для крепления на DIN-рейку. Диапазон рабочих температур –40…+75°C.

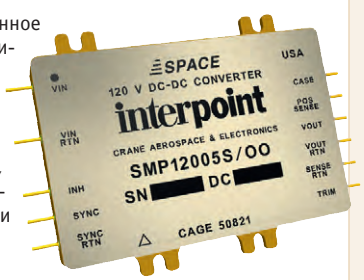
## Радиационно-стойкие 40 Вт DC/DC-преобразователи постоянного тока 100/120 В

УЗНАТЬ БОЛЬШЕ

Преобразователи напряжения **Crane Aerospace & Electronics** серии **SMP120** созданы для работы от бортовой сети космических аппаратов постоянного напряжения 100/120 В.

Выпущены две модели в герметичных стальных корпусах 76,2×58,42×12,22 мм: 40 Вт с выходным напряжением 5 В (КПД 72%) и 49 Вт – 28 В (КПД до 79%). Диапазон входного напряжения от 80 до 160 В, стойкость к импульсам входного напряжения 180 В длительностью 100 мс. Предлагаются модели в исполнениях Class H и Class K согласно требованиям MIL-PRF-38534 с уровнями радиационной стойкости L (50 крад) и R (100 крад). Стойкость по эффекту отказов SEL – 43 МэВ·см$^2$/мг.

Сервисные функции: дистанционное включение/выключение, синхронизация частоты преобразования внешним сигналом, подстройка выходного напряжения, защита от КЗ нагрузки, блокировка при пониженном входном напряжении, защита от перенапряжения на выходе, внешняя обратная связь и ограничение пускового тока.



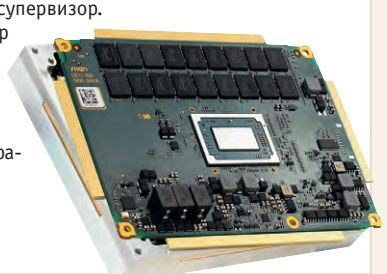

## Новый модуль Rugged COM Express от MEN

УЗНАТЬ БОЛЬШЕ

**CB71C** –сверхзащищённый модуль на базе семейства гибридных процессоров AMD V1000 для применения на железных дорогах, общественном транспорте и в промышленных приложениях.

*Основные характеристики*

- VITA 59, совместим с COM Express Basic тип 6.
- До 32 Гбайт ОЗУ DDR4 с поддержкой ECC (напаяно).
- eMMC-накопитель объёмом 16 Гбайт (напаян).
- Поддержка до 4 видеовыходов с разрешением 4K (DP, eDP, HDMI, DVI).
- Высокоскоростные интерфейсы PCI Express 3.0, SATA 3.0, Gigabit Ethernet и USB 3.0.
- Криптопроцессорный модуль (TPM), аппаратное шифрование данных.
- Функционально безопасный супервизор.
- Диапазон рабочих температур –40…+85°C, кондуктивное охлаждение.
- Электромагнитное экранирование.
- Устойчивость к ударам и вибрациям.
- Доступна версия в стандарте PICMG COM.0 COM Express.



## Обновление ноутбука-трансформера V110 Getac

УЗНАТЬ БОЛЬШЕ

Компания **Getac**, ведущий производитель защищённых мобильных компьютеров, анонсировала масштабное обновлении ноутбука-трансформера **V110**.

Благодаря обновлению процессора Kaby Lake Intel Core i5/i7 до последнего 7-го поколения и возможности подключения OPAL SSD 256 или 512 Гбайт новый V110 станет ещё более производительным, эффективным, будет обладать повышенной безопасностью и мобильностью для сотрудников коммунальных служб и других организаций с выездным обслуживанием объектов. Специалисты коммунальных служб часто работают на открытом воздухе в отдалённых районах в течение продолжительных периодов времени, независимо от погоды. Сбор данных, управление информацией, синхронизация между различными устройствами и поддержание связи с центральным офисом становятся серьёзными препятствиями, которые им приходится преодолевать.


Анонсированная дата выпуска обновления продукта – второй квартал 2018 года.

## Серия ИБП CyberPower: HSTP3T15KE(BC)-C и HSTP3T20KE(BC)-C

УЗНАТЬ БОЛЬШЕ

Компания **CyberPower** выпустила бюджетную линейку ИБП серии С — это качественная и надёжная защита ЦОД, интеллектуального оборудования и устройств с высокими требованиями к качеству электропитания от любых нарушений электроснабжения с широкими возможностями адаптации решения к требованиям конкретной задачи. Построенные на базе интегральных IGBT-модулей с высокоскоростной цифровой обработкой сигналов ИБП обладают высоким КПД при малом количестве электронных компонентов. Возможности параллельной работы и резервирования, увеличения времени автономной работы, интуитивно понятный графический дисплей и опциональная карта удалённого управления делают их наиболее эффективными в классе.

Со значительным уменьшением стоимости серии С качество и характеристики отвечают мировым требованиям. Гарантийный период 4 года.

ИБП серии С поставляется как со встроенными аккумуляторами, так и с внешними батарейными кабинетами.

## Модули ввода/вывода ADAM-E5000

УЗНАТЬ БОЛЬШЕ

Компания **Advantech** выпустила в массовое производство модули серии **ADAM-E5000**, предназначенные для контроллера ADAM-5000/ECAT. ADAM-5000/ECAT – распределённая высокоскоростная система ввода-вывода с 4 слотами для EtherCAT. EtherCAT – стандарт промышленной сети семейства Industrial Ethernet с технологиями, используемыми для распределённого управления в режиме реального времени. Протокол стандартизован в IEC 61158 и применяется к приложениям автоматизации, которым требуется более быстрая и эффективная связь.


В состав серии ADAM-E5000 входит линейка модулей, начиная от базовых моделей DI/O и заканчивая высокоскоростными AI/O для разных сценариев приложений. Модули DI/O поддерживают 16 или 32 канала, а модули AI/O могут быть на 4 и 8 каналов. Вся серия имеет высокую степень помехоустойчивости.

Минимальное время обновления данных с точной синхронизацией делает серию ADAM-E5000 подходящей для управления перемещением в режиме реального времени.

## Новое поколение одноплатных компьютеров в популярном формате

УЗНАТЬ БОЛЬШЕ

Компания **Advantech** выпустила в массовое производство плату **PCM-9366**. Новинка в формате 3,5" выполнена на базе мобильных процессоров Intel Apollo Lake. В процессорах 14 нм используются 2 или 4 ядра с микроархитектурой Goldmont и графическая подсистема Intel HD Graphics 500/505, которая обеспечивает декодирование видео в различных форматах с разрешением до 2560×1600 точек и высокую производительность 3D-графики с поддержкой DirectX11, OpenGL3.2, OpenCL1.2. Три независимых дисплея подключаются через видеовыходы VGA+LVDS+HDMI.

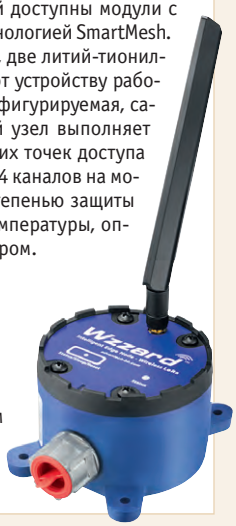
PCM-9366 имеет гибкие возможности расширения благодаря большому количеству портов ввода/вывода: 6×USB, 4×COM, 2×CAN, 8-битный GPIO, 2×LAN, и слотов расширения: 1×M.2, 1×mSATA.

Одноплатный компьютер имеет длительный срок жизни – до 2030 года, а также обеспечивает надёжность работы 24 часа в сутки, 7 дней в неделю, что делает его подходящим решением для интеллектуальных встраиваемых систем.

## Беспроводные модули ввода/вывода серии Wzzard

УЗНАТЬ БОЛЬШЕ

Компания **Advantech** расширяет производственную линию беспроводных модулей ввода/вывода серией **Wzzard**. В ней доступны модули с поддержкой беспроводных сетей LoRa и Wi-Fi с технологией SmartMesh. Технология LoRa имеет низкое энергопотребление, две литий-тионилхлоридные батареи 3,6 В типа AA 2,4 А·ч позволяют устройству работать автономно более года. SmartMesh – самоконфигурируемая, самовосстанавливающаяся сеть, в которой каждый узел выполняет функции маршрутизатора/ретранслятора для других точек доступа той же сети. Поддерживаются 32 модуля в сети, до 4 каналов на модуль и не более 8 модулей на канал. Модули со степенью защиты корпуса IP66 оснащены встроенным датчиком температуры, опционально – встроенным трёхосевым акселерометром.




Варианты исполнения:

- 2 термопары J + 1 DO;
- 2 термопары K + 1 DO;
- 2 AI + 1 DO;
- 3 AI;
- 2 DI + 2 DO.

Wzzard подойдёт для проектов с распределённым сбором данных и неблагоприятными условиями окружающей среды.

## Расширение линейки неуправляемых коммутаторов SPIDER

УЗНАТЬ БОЛЬШЕ

Компания **Hirschmann** представила новые модели в линейке неуправляемых коммутаторов **SPIDER III**.

Новинки отличаются возросшим количеством коммутационных портов, до 26 Fast Ethernet либо до 8 Gigabit Ethernet, что позволяет быстро расширить существующую Ethernet-сеть. Как и прежде, линейка SPIDER III обладает улучшенными характеристиками в области обеспечения безопасности сети для данного типа устройств. Это реализуется при помощи задания предварительной базовой конфигурации коммутатора посредством USB-накопителя.

Конструктивно коммутаторы SPIDER III выполнены в металлическом либо пластиковом корпусе для монтажа на DIN-рейку со степенью защиты IP30/40. Диапазон рабочих температур -40…+70°C, при этом опционально доступно конформное покрытие печатных плат коммутатора. Преимуществом SPIDER III является наличие отраслевых промышленных сертификатов ISA12.12 Class 1 Div. 2, ATEX Zone 2, IEC 61850-3, IEEE1613, DNVGL.

## OLED-дисплеи 2,23" с кристаллом драйвера на печатной плате

УЗНАТЬ БОЛЬШЕ

Компания **Raystar Optronics** выпустила графические OLED-дисплеи серии **REP012832A** с белым цветом свечения экрана. Изображение удобно для считывания благодаря контрастности 2000:1 и размеру 2,23". Для управления применяется микросхема драйвера SSD1305Z, она обеспечивает работу через параллельный 6800/8080-совместимый 8-разрядный интерфейс, $I^2C$ и 4-проводной SPI. REP012832A снабжены 20 металлическими контактами и отверстиями для монтажа на плату. Внешние сигналы подключаются через плоский гибкий кабель с соединителем или соединение пайкой. Диапазон рабочих температур –40…+80°C.

Дисплеи применяются в системах «Умный дом», в медтехнике, приборах с интеллектуальным управлением и др.

*Основные характеристики*

- Габаритные размеры 66,5×35×9 мм.
- Видимая область экрана 55,018×13,098 мм.


## 4/2-канальный модуль АЦП/ЦАП стандарта FMC с интерфейсом JESD204B

УЗНАТЬ БОЛЬШЕ

Мезонин **Perfectron MIC1832** выполнен в соответствии со стандартом FMC (ANSI/VITA 57.1) и предназначен для использования в составе несущих модулей AMC, VPX, PCI, PCIe, CompactPCI.

Плата имеет две микросхемы ЦАП с максимальной частотой дискретизации 2800 МГц и две микросхемы АЦП с максимальной частотой дискретизации 1250 МГц. Конфигурация позволяет реализовать 4 независимых канала цифроаналогового преобразования и 4 независимых канала аналого-цифрового преобразования. В качестве опорного тактового сигнала используется сигнал с несущей платы. Для ввода/вывода аналоговых сигналов на плате модуля установлены разъёмы SSMC (AEP 7110-1511- 000).

Диапазон рабочих температур составляет –40…+85°C.

Области применения: формирование и приём ВЧ-радиосигналов, широкополосные цифровые приёмники, цифровые приёмопередающие устройства, SDR, радиолокация, АФАР, стендовое и измерительное оборудование.

## Промышленные источники питания WAGO EPSITRON® IP67 в герметичном корпусе

УЗНАТЬ БОЛЬШЕ

Новые промышленные источники питания от компании **WAGO** серии **EPSITRON® IP67** предназначены для питания промышленного оборудования напряжением 24 В DC и не требуют размещения внутри защитных корпусов и шкафов благодаря надёжной конструкции и высокой степени защиты. Их основное преимущество в том, что напряжение преобразуется из 230 В AC в 24 В DC там, где это необходимо, что снижает себестоимость системы питания. Даже в жёстких промышленных условиях ИП работают надёжно: конструкция со степенью защиты IP67 предохраняет от влажности и пыли.


*Преимущества WAGO EPSITRON® IP67*

- Компактная конструкция.
- Энергоэффективность до 92,3%.
- Низкие потери мощности.
- Быстрое подключение без использования инструментов за счёт 7/8" резьбового разъёма.
- Активная коррекция коэффициента мощности снижает требования к качеству входного питания.
- Эффективная защита от водяных капель.

## Универсальные компактные источники питания 350 Вт AC/DC

УЗНАТЬ БОЛЬШЕ

Компания **XP Power** выпустила источники питания серии **SMP350** для монтажа в шасси, обеспечивающие мощность до 350 Вт .

В корпус встроен охлаждающий вентилятор, имеются винтовые зажимы, модули генерируют низкий уровень ЭМП. Размеры корпуса 91,44×177,8×43,1 мм, удельная мощность 499 Вт/дм$^3$ .

Серия конкурентоспособна по цене и предназначена для широкого ряда применений, включая управление производственными процессами, измерительное и связное оборудование, коммунальный и энергетический секторы.

Диапазон входного напряжения 85–264 В, предлагаются одноканальные модели с выходными напряжениями 12, 15, 18, 24, 28, 36 и 48 В. Диапазон рабочих температур –40…+70°C. Наличие входа дистанционного включения/выключения упрощает управление системой. Высокий КПД ведёт к уменьшению генерируемого тепла и увеличению ресурса, пониженная входная мощность в режиме холостого хода уменьшает потребляемую мощность в дежурном режиме.

## IIoT-шлюз IMG-6322GT от ORing

УЗНАТЬ БОЛЬШЕ

Компания **ORing** представила IIoT-шлюз **IMG-6322GT** для обеспечения взаимодействия различных промышленных устройств.

Новинка является универсальным устройством, способным обеспечить взаимодействие по различным физическим линиям. Помимо поддержки беспроводных технологий LTE и Wi-Fi (IEEE 802.11a/b/g/n), которые встречаются во многих IIoT-устройствах, шлюз IMG-6322GT оснащён последовательными интерфейсами передачи данных RS-232/422/485, а также Ethernet-портами 2×10/100/1000Base-T(X). Это позволяет не только связать между собой как современные промышленные устройства, так и оборудование, функционирующее на базе RS-линий, но и обеспечить удалённый мониторинг и управление.

Функциональность для обеспечения безопасности беспроводных соединений реализуется путём поддержки протоколов WEP, WPA/WPA2, WPAPSK, 802.1X, Radius, TKIP. Конструктивно шлюз IMG-6322GT выполнен в металлическом корпусе и предназначен для монтажа на DIN-рейку.

## Если в офисе жёсткие условия, используйте трекбол NSI R55

УЗНАТЬ БОЛЬШЕ

В случае, когда использование бытовых указательных устройств невозможно, но условия эксплуатации не требуют высоких степеней защиты, лучшим выбором становятся компромиссные решения.

Отличным примером является профессиональный механический настольный трекбол **NSI R55**. Шар из фенольной резины диаметром 57,2 мм помещён в корпус из ударопрочного ABS-пластика. Благодаря специально разработанной эргономичной конструкции он обеспечивает пользователю удобство при продолжительной работе. Модуль снабжён тремя встроенными кнопками, соответствующими функциям кнопок мыши. Ресурс трекбола составляет более 6 млн оборотов, кнопок – свыше 5 млн нажатий. Подключение устройства возможно к порту USB или PS/2 с помощью прилагаемого адаптера, без установки специальных драйверов. Модуль обладает степенью защиты IP40, устойчив к вибрациям (5g, 2–5 кГц по любой оси) и предназначен для эксплуатации при температурах 0…+55°C.


## OLED-дисплеи 1,71" с разрешением 128×32 пикселя

УЗНАТЬ БОЛЬШЕ

Компания **Raystar Optronics** выпустила графические дисплейные модули серии **REX012832G** формата 128×32. Интегральная микросхема драйвера SSD1307ZD обеспечивает работу через интерфейс I$^2$C и 4-проводной последовательный SPI. Напряжение питания логической части дисплея 3 В, коэффициент мультиплексирования строк 1/32.

В конструкции «кристалл на стекле» (COG) управляющая микросхема размещена на подложке дисплея для уменьшения габаритов. Дисплеи подходят для применения в портативных устройствах, испытательном оборудовании, медицинских переносных приборах и пр. Предлагается модель с белым цветом свечения. Диапазон рабочих температур –40…+80°C, диапазон температур хранения –40…+85°C.

*Основные характеристики*

- Габаритные размеры 50,5×15,75×2,01 мм.
- Видимая область экрана 42,22×10,54 мм.
- Размер пикселя 0,308×0,388 мм.
- Шаг пикселя 0,33×0,33 мм.

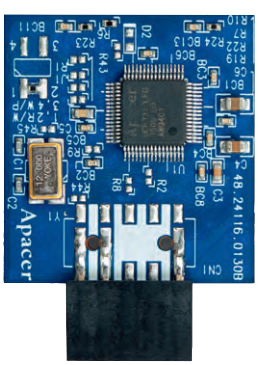

## Твердотельный накопитель UDMII Plus (Type D LP) от Apacer

УЗНАТЬ БОЛЬШЕ

Твердотельный накопитель **UDMII Plus (Type D LP)** выполнен в небольшом форм-факторе, который электрически соответствует высокоскоростному интерфейсу USB 2.0. Предназначенный специально для использования в серверах новый накопитель может похвастать улучшенной скоростью, встроенными функциями S.M.A.R.T., опциональной защитой от записи и другими усовершенствованиями.

*Основные характеристики*

- Модель – UDM 1U-M.
- Интерфейс USB 2.0.
- Разъём 10-pin (2×5).
- Флэш-память NAND – SLC.
- Ёмкость от 256 Мбайт до 8 Гбайт.
- Поддерживаемая скорость чтения до 30 Мбайт/с.
- Поддерживаемая скорость записи до 25 Мбайт/с.
- Максимальный диапазон рабочих температур –40…+85°C.
- Ударопрочность 50g.
- Вибростойкость 15g.
- Размеры 31,95×24×5 мм.



## Дифференциальный аттенюатор TP-DA25

УЗНАТЬ БОЛЬШЕ

Для увеличения входного диапазона с USB-осциллографов серии Handyscope HS6 DIFF и дифференциальных измерений компания **TiePie** разработала дифференциальный аттенюатор **TP-DA25**.

Аттенюатор TP-DA25 предназначен для измерения высоких напряжений до 1000 В CAT II (коэффициент 1:25), выполнен совместно с измерительным кабелем и располагается непосредственно перед входами Handyscope HS6 DIFF.

Устройство не требует источника питания, имеет высокий коэффициент подавления синфазного сигнала (CMRR), нечувствительно к внешним шумам. Внешние помехи эффективно подавляются специальной конструкцией дифференциального аттенюатора, а два измерительных щупа могут быть размещены на расстоянии более двух метров друг от друга, что было бы невозможно при использовании стандартных осциллографов, так как у них максимальная длина провода между измерительным зондом и землёй из-за высокой чувствительности к помехам ограничена примерно 20 см.

## Новый модуль ET975 в форм-факторе COM Express от iBASE

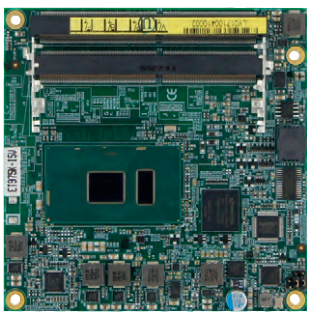
УЗНАТЬ БОЛЬШЕ

Компания **iBASE**, мировой лидер в производстве промышленных материнских плат и встраиваемых систем, представляет свой новый модуль ET975 в форм-факторе COM Express на основе процессора 7-го поколения Intel Core i7/i5/i3 (Kaby Lake-U) с низким энергопотреблением, который изготавливается с использованием техпроцесса 14 нм.Семейство процессоров Kaby Lake-U характеризуется долговечностью, производительностью и низким энергопотреблением.

Модуль ET975 подходит для применения в автоматизации производства, аппаратах самообслуживания, киосках и для управления различными цифровыми вывесками.

*Основные характеристики*

- Напаянные процессоры Intel Core i7/i5/i3 7-го поколения и выше.
- 2×DDR4 SODIMM, максимум 32 Гбайт.
- Поддержка двух портов DDI или DDI +VGA.
- 1×Intel PCI-E GbE LAN.
- 8×USB 2.0, 4×USB 3.0, 2×COM, 2×SATAIII.
- 4×PCI-E (x1), 1×PCI-E (x4).



## Модульные AC/DC-преобразователи в кондуктивном исполнении

УЗНАТЬ БОЛЬШЕ

Компания **TDK-Lambda** выпустила серию модульных AC/DC-преобразователей **CM4**. Они выполняются в конвективном или кондуктивном исполнении с теплоотводом на шасси оборудования.

Благодаря наличию промышленных и медицинских сертификатов безопасности серия подходит для широкого спектра применений. Размеры CM4 101,6×41×177,8 мм, при этом обеспечивается до 600 Вт длительно отдаваемой мощности. Диапазон напряжений питания 85–264 В AC с линейным падением мощности до 425 Вт при пониженных напряжениях сети 120–85 В AC. В источник можно установить до 4 одноканальных выходных модулей, а комбинации из их последовательного или параллельного соединения дают выходные напряжения от 1,5 до 232 В и токи до 90 А.

При кондуктивном охлаждении температура основания может достигать +105°C. Диапазон рабочих температур –40…+70°C со снижением мощности на 2,5%/°C от +50°C. КПД достигает 90%, а потребление в режиме холостого хода не превышает 1 Вт.

## Механизм MPLS-TP теперь и в промышленных сетях

УЗНАТЬ БОЛЬШЕ

Компания **Hirschmann** представила абсолютно новый продукт **DRAGON PTN**, предназначенный для установки гарантированной пропускной способности и времени доставки служебной информации в промышленных Ethernet-сетях. В качестве инструмента задания гарантированной скорости передачи данных в DRAGON PTN используется надёжная технология Multiprotocol Label Switching – Transport Profile (MPLS-TP) на основе специализированных служебных пакетов. Неотъемлемой частью DRAGON PTN является специализированное ПО HiProvision. Их совместное использование позволит обеспечить доступность и распределение полосы пропускания, а также возможность спрогнозировать поведение передачи потока данных по мере его прохождения по сети крупного промышленного объекта.

DRAGON PTN представляет собой полностью законченное устройство, выпускаемое в модульном исполнении с возможностью конфигурирования и резервирования отдельных его компонентов.

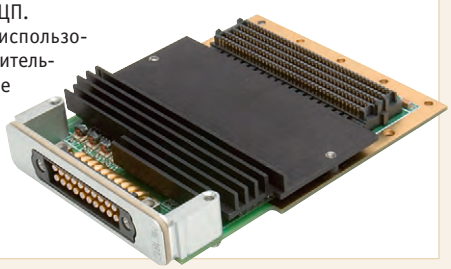
## 16-канальный мезонинный модуль АЦП стандарта FMC

УЗНАТЬ БОЛЬШЕ

Мезонин **Perfectron MIC1812** выполнен в соответствии со стандартом FMC (ANSI/VITA 57.1). Плата имеет шестнадцать 14-битовых аналого-цифровых преобразователей (далее АЦП) с частотой дискретизации до 125 МГц. В качестве опорного тактового сигнала может быть использован сигнал как с внешнего источника, так и внутренний с несущей платы. Возможность выдачи тактового сигнала на внешний разъём позволяет поддержать каскадное включение нескольких плат для синхронного аналого-цифрового преобразования.

На плате мезонина смонтирован разъём Nicomatic 341D000F51-0020-140002, позволяющий использовать коаксиальные кабели для ввода требуемого количества аналоговых сигналов. Каждый аналоговый канал имеет входной усилитель, позволяющий получить оптимальную амплитуду сигнала на входе АЦП.

Мезонин может быть использован совместно с вычислительными модулями на базе ПЛИС форматов CompactPCI Serial: FPU500, FPU502, или VPX – FPU1500.



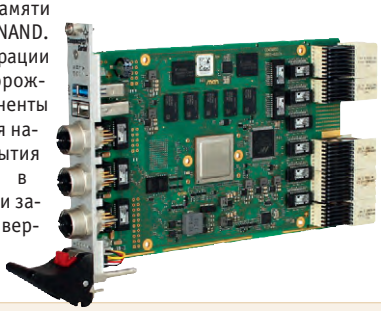
## Одноплатный компьютер MEN G40A

УЗНАТЬ БОЛЬШЕ

Компания **MEN** представляет процессорную плату **G40A** формата 4HP/3U CPCI Serial на базе процессора NXP ARM Cortex A72 LS1046A. Она поддерживает последовательные интерфейсы PCIe 3.0, USB 3.0 и SATA 3.0, оборудована встроенным Ethernet-коммутатором и Ethernet-портами на лицевой панели. Также обеспечена совместимость с интерфейсами UART, $I^2C$, SPI и т.д.

Мониторинг осуществляется с помощью встроенного контроллера управления платой и сторожевого таймера. Поддерживается технология Wake-on-LAN. Плата G40A комплектуется оперативной памятью DDR4 с поддержкой ECC. Конфигурация может быть дополнена энергонезависимым ОЗУ SRAM, картой памяти MicroSD и накопителем eMMC NAND.

Для защиты от ударов и вибрации в соответствии с железнодорожными стандартами все компоненты на плате пропаяны. Благодаря наличию конформного покрытия G40A можно использовать в условиях высокой влажности и запылённости. Также доступна версия для установки в безвентиляторные системы.



## Весенние новинки встраиваемых систем AdvantiX: встречаем ER-3100/4100

УЗНАТЬ БОЛЬШЕ

Обновляется модельный ряд **AdvantiX ER**. На смену компьютерам ER-3000 и ER-4000 приходят новые модели – **ER-3100** и **ER-4100**.

Новинки построены на основе единой платформы от iBase – партнёра AdvantiX. Две модели имеют идентичные корпуса, наборы интерфейсов и систему кондуктивного теплоотвода. Отличия ER-3100 от ER-4100 в диапазоне рабочих температур и вычислительной мощности. В ER-3100 установлен процессор Celeron или Pentium, диапазон рабочих температур +5…+50°C. В ER-4100 процессор Atom x5 или x7, диапазон рабочих температур –40…+70°C.

Набор портов в моделях идентичен: 4×USB 3.0, 2×Gigabit Ethernet, 3×COM (разъём DB9), 1×COM (RJ-45), HDMI и Display-порты. За обработку графической информации отвечает Intel HD Graphics 500/505. В малом форм-факторе помещается система, оснащённая необходимым набором интерфейсов, а информация в ней хранится на современных носителях M.2 от компании Innodisk.

## Источники питания TDK-Lambda RWS-B с 7-летней гарантией стали мощнее

УЗНАТЬ БОЛЬШЕ

Корпорация **TDK** расширила серию **RWS** линейками **RWS1000B** и **RWS1500B**. Новинки оснащены винтовыми клеммами с защитными панелями вместо шинопроводов, что позволяет значительно облегчить монтаж кабелей нагрузки. Опционально источники могут быть заказаны в исполнении с двусторонним защитным покрытием печатной платы, обратным потоком воздуха, функцией удалённого включения/отключения, а также выходами активного токораспределения (однопроводная схема) для параллельного включения блоков, сигнала состояния выходного напряжения "DC good" и сигнала отказа вентилятора.

Высокомощные источники серии RWS-B позволяют работать в широком диапазоне напряжений питания от 85 до 265 В AC и могут использоваться при температурах окружающего воздуха от –20 до +60°C. Они разработаны для общепромышленного и телекоммуникационного оборудования, систем и приборов измерения и сбора данных, питания светодиодных табло и экранов.

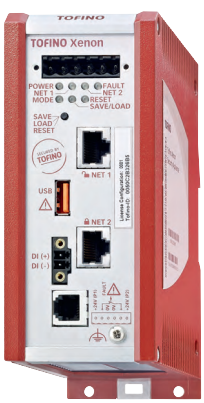
## GOOSE-протокол теперь под защитой Tofino Xenon

УЗНАТЬ БОЛЬШЕ

Компания **Hirschmann** представила очередное программное обновление для промышленного брандмауэра **Tofino Xenon**. Новая версия 3.2 отличается расширенной поддержкой как IT, так и промышленных протоколов, доступных для аналитики.

В дополнение к имеющимся возможностям контроля промышленных протоколов Modbus TCP, Ethernet/IP, OPC Classic, IEC 104 и DNP3 появилась поддержка анализа протокола Generic Object-Oriented System Events (GOOSE). Данный протокол описан внутри стандарта МЭК 61850 и, как правило, широко используется на предприятиях энергетического сектора (типовое применение протокола – передача сообщений между терминалами релейной защиты и автоматики).

Модуль, обеспечивающий защиту GOOSE-протокола, имеет наименование Tofino Xenon GOOSE Enforcer LSM и предназначен для осуществления глубокой инспекции пакетов данных (Deep Packet Inspection – DPI) GOOSE-сообщений, которые присутствуют в промышленной Ethernet-сети.




## Управляемый коммутатор ORING RES-P9242GCL для применения на энергоподстанциях

УЗНАТЬ БОЛЬШЕ

Компания **ORing** представила управляемый коммутатор **RES-P9242GCL**, соответствующий стандартам IEC 61850-3 и IEEE 1613 и предназначенный для применения на объектах энергетики.

Он оснащён 24 портами стандарта 10/100Base-T(X) и 2 гигабитными комбопортами. Поддерживается большое количество протоколов резервирования, как проприетарных: O-Ring, O-Chain, так и стандартизованных: MRP, MSTP (RSTP/STP). Программная реализация поддержки стандарта IEEE 1588v2 обеспечивает высокую точность синхронизации времени, что важно для объектов энергетики. Дополнительным бонусом может служить наличие ПО Open-Vision, которое позволяет осуществить комплексную групповую конфигурацию устройств ORing.

Конструктивно коммутатор RES-P9242GCL выполнен в металлическом корпусе, предназначенном для монтажа в 19" стойку. Диапазон рабочих температур –40…+85°C. Время наработки на отказ (MTBF) составляет 297 924 ч.

## Переход от аналоговых к IP-камерам с видеосервером GeoVision

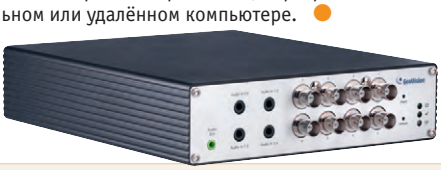
УЗНАТЬ БОЛЬШЕ

Часто перед заказчиками встаёт вопрос о постепенном переходе от устаревшего аналогового оборудования к современным IP-камерам высокого разрешения. Если на объекте до сих пор используются HD или аналоговые камеры и требуется быстро и экономично развернуть решение для обеспечения безопасности на основе IP-камер, то видеосервер **GV-VS2820** является хорошим решением.

*Возможности видеосервера **GeoVision***

- Преобразование аналоговых видеосигналов (TVI или AHD) в цифровые.
- Поддержка внешнего USB-накопителя объёмом до 6 Тбайт и возможность удалённого просмотра.
- Установка в ограниченное пространство благодаря компактному дизайну.
- Поддержка GPS.
- Поддержка камер сторонних производителей.

Теперь клиенты могут управлять и просматривать видео с любых камер в режиме реального времени при помощи программного обеспечения VMS на локальном или удалённом компьютере.



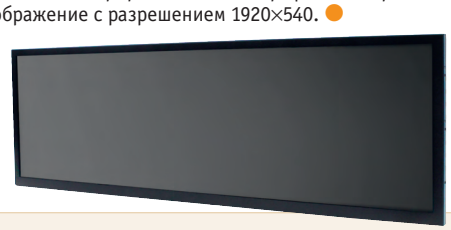
## Новый 37" панельный компьютер iBASE

УЗНАТЬ БОЛЬШЕ

Компания **iBASE**, ведущий мировой производитель встраиваемых систем и цифровых рекламных вывесок, объявляет о выпуске 37-дюймового защищённого панельного компьютера **ARD-037-N** «всё в одном» с ЖК-дисплеем, имеющим разрешение 1920×540.

Этот компактный безвентиляторный панельный компьютер оснащён процессором Intel Pentium QC N4200 с тактовой частотой до 2,5 ГГц. Новый защищённый компьютер ARD-037-N предназначен для использования в системе пассажирских информационных систем (PIS) на автобусных или железнодорожных станциях. Также он подойдёт для демонстрации рекламы, расписаний поездок, прогнозов погоды, информации о пробках и о прибытии и отправлении общественного транспорта.

Компьютер ARD-037-N оснащён 2 Гбайт оперативной памяти DDR3L-1866 с возможностью расширения до 8 Гбайт. Также в нём имеются накопитель mSATA ёмкостью 64 Гбайт и интегрированная в SoC графика, которая позволяет выводить изображение с разрешением 1920×540.



GeoVision inc

# Профессиональные системы видеонаблюдения

от GeoVision

## Хранение данных

Резервное копирование

- Автосохранение данных на внешние системы

Система хранения

- Система хранения данных из 24 HDD
- Расширение до 192 HDD для крупных систем

## Экономичное решение

H.265 HEVC
Решения H.265

- Уменьшение потока, экономия на хранении данных

Сервер записи

- Принимает до 128 каналов IP-камер, распространяет до 300 каналов

1080P
Видео-сервер HD

- Использование СХД в рабочей системе
- Перевод в единую систему хранения данных

Открытая платформа

- Работа с оборудованием сторонних производителей

Городские здания

Общественная безопасность

Наш журнал продолжает рубрику «Будни системной интеграции». Её появление не случайно и связано с растущим числом интересных системных решений в области АСУ ТП, с одной стороны, а с другой – с участившимися запросами в адрес редакции от различных предприятий с просьбами порекомендовать исполнителей системных проектов.

Цель рубрики – предоставить возможность организациям и специалистам рассказать о внедрённых системах управления, обменяться опытом системной интеграции средств автоматизации производства, контроля и управления. Публикация в этой рубрике является прекрасным шансом прорекламировать свою фирму и её возможности перед многотысячной аудиторией читателей нашего журнала и с минимальными затратами привлечь новых заказчиков.

Рубрика призвана расширить для специалистов кругозор в области готовых решений, что, несомненно, создаст условия для прекращения «изобретательства велосипедов» и для выхода на более высокие уровни системной интеграции.

## «Икслайт» за Полярным кругом: система подсветки мемориального комплекса в Мурманске

Компания **«Икслайт»** разработала и реализовала концепцию художественного освещения мемориального комплекса, посвящённого стойкости и мужеству жителей города-героя в годы Великой Отечественной войны. Задача проекта заключалась в том, чтобы мемориал, расположенный на берегу Семёновского озера, выделить в ландшафте и сделать его визуально привлекательным в вечернее и ночное время.

Важным условием при выборе оборудования была необходимость безупречной работы светильников в условиях сурового мурманского климата, они должны обладать высокими защитными свойствами: герметичностью, устойчивостью к перепадам температуры и воздействию влаги, прочностью. Заказчик ориентировался на компании с богатым опытом в разработке освещения для объектов культуры и в поставке оборудования для них.

В центральной части комплекса, который занимает площадь более 5 тысяч м$^2$, располагается смотровая площадка круглой формы. В центре площадки установлен монумент из трёх колонн, подсвеченных вмонтированными в плитку грунтовыми светильниками **XLD-ALGA** со специальной эллиптической оптикой и возможностью регулировки направления светового пучка (направление можно фиксировать в углах 20, 30 и 40°). Возле монумента установлена кирпичная стена, на которой размещены награды Мурманска и стенды с архивными фотоматериалами. В тёмное время суток они подсвечены прожекторами **XLD-FL12** с поворотными механизмами, позволяющими настраивать световую экспозицию.

Проект был успешно реализован, все требования заказчика удовлетворены, а обновлённый мемориал ещё раз подтвердил и упрочил высокий статус среди горожан и гостей города.

УЗНАТЬ БОЛЬШЕ

## Коммутаторы ORing на автомобильном заводе Tesla

На протяжении последних лет электрокары производства Tesla являются примером развития технологий как в IT, так и в автомобильной сфере. Компания реализовала ряд значимых проектов. Это стало возможным благодаря одной из самых технологичных производственных линий в мире. Завод, словно огромный механизм, обладает линиями, способными выполнять все производственные работы самостоятельно, начиная от обработки кузовного материала до сборки уже готового автомобиля.

Одна из самых сложных систем завода – это система контроля качества автомобильных деталей, подаваемых на конвейер. Она включает большое количество датчиков, ПЛК, HMI, предназначенных для контроля, управления и сбора данных о деталях и частях производимого автомобиля.

Реализация подобной системы не могла обойтись без надёжной высокоскоростной сети передачи данных. Для этих целей компания Tesla реализовала на своём предприятии промышленную сеть, базирующуюся на технологиях Industrial Ethernet. При этом из-за ограниченного пространства в шкафах возникла задача применения Ethernet-оборудования с минимальными габаритами.

В итоге для решения задачи сбора информации и передачи служебных данных контроля компания Tesla применила промышленные неуправляемые коммутаторы **ORing IES-150B**. Данные коммутаторы отличаются очень компактными габаритными размерами 26,1×70×95 мм. При этом устройство имеет металлический корпус со степенью защиты IP30, диапазон рабочих температур составляет –40…+70°C. Отличительной особенностью также является высокое значение времени показателя наработки на отказ (MTBF) > 2,5 млн часов.


УЗНАТЬ БОЛЬШЕ

## Компания VIVOTEK установила систему подсчёта посетителей в Национальной библиотеке Латвии

Национальная библиотека, расположенная в столице Латвии Риге, привлекает разнообразных посетителей, от жителей, нуждающихся в традиционных библиотечных услугах, до любителей культуры, посещающих бесчисленные выставки, которые проходят в этом учреждении. Национальная библиотека Латвии, которая проводит постоянные, временные и виртуальные выставки и обладает исчерпывающим объёмом средств печати и цифровых ресурсов, является важным национальным культурным учреждением, получившим признание ЮНЕСКО, а также центром исследований и образования.

Одновременное посещение библиотеки огромным количеством людей ставит сложные задачи перед сотрудниками охраны. Камеры **VIVOTEK FD8166A-S** и счётчик **SC8131** обеспечивают современную технологию подсчёта людей, которая лежит в основе получения всеобъемлющего отчёта о количестве посетителей библиотеки.

Интеллектуальный и централизованный контроль над камерами через программное обеспечение **VAST** гарантирует, что проблемы, связанные с управлением объектами, ушли в прошлое.

Сотрудники Национальной библиотеки Латвии должны обладать навыками работы с большим количеством людей и учитывать непредсказуемый характер посещений, зависящий от времени суток и популярности выставок. Камера VIVOTEK FD8166A-S и счётчик SC8131 централизованно управляются программным обеспечением VAST VIVOTEK, что в сочетании с простотой в эксплуатации и высокоэффективной технологией подсчёта позволяет сотрудникам библиотеки точно определить, где находятся посетители в данный момент.

УЗНАТЬ БОЛЬШЕ

## Прогрессивная система мониторинга и управления сетью горячего водоснабжения

Системы горячего водоснабжения являются одними из самых энергозатратных в современном мире. На нагрев воды тратится бóльшая часть энергоресурсов. Системы контроля обычно представляют собой локальные узлы, которые управляются непосредственно персоналом.

Как правило, в котельных персонал несёт ответственность за проверку всех составных частей оборудования вручную, что может повлечь за собой значительные затраты, как по времени, так и по человеческим ресурсам. Сложившаяся ситуация была достаточно острой в ряде североамериканских штатов, особенно в государственных учреждениях, таких так больницы, школы и детские сады.

Для изменения этого положения дел органы местного самоуправления запустили программу создания сети контроля в реальном времени объектов горячего водоснабжения и теплоэнергетики. Для реализации намеченного сценария необходимо было обеспечить связь локальных объектов с центральным пунктом сбора информации, фактически подключить каждый бойлер к Интернету для передачи контрольной информации в пункты управления. В итоге данная сеть была реализована силами ряда североамериканских компаний-интеграторов. В качестве связного устройства выступили роутеры **Advantech** с поддержкой сотовых сетей 3G/4G, которые не только обеспечили связь между разными объектами, но и позволили создать инструментарий для визуализации состояния удалённых объектов.


## Getac F110 поступил на пожарную службу

Пожарные работают в экстремальных условиях, от них ждут помощи в самых разных чрезвычайных ситуациях, включая пожары в жилых зданиях, коммерческих помещениях и на транспорте. Вызовы поступают в любую погоду, днём и ночью, в будни и в праздники, в любое время года. Поэтому для пожарных критически важны надёжные высококачественные автомобили, ИТ-устройства и предметы экипировки.

Компания Rosenbauer – один из ведущих поставщиков пожарных автомобилей и средств пожаротушения в мире. В основе продукции Rosenbauer лежат самые современные и передовые технологии. Специалисты Rosenbauer совместно с компанией **Getac** и её партнёром Mettenmeier разработали комплексное решение на основе полностью защищённого планшета **Getac F110** и программного обеспечения EMEREC для управления информацией в мобильных средах. Это решение было успешно внедрено в пожарной части австрийского города Амштеттена.

Полностью защищённый планшет Getac F110 оказался оптимальной аппаратной платформой для Rosenbauer. Это устройство разработано на основе инновационных технологий и выполнено в прочном корпусе, способном выдержать любое экстремальное воздействие.

В отличие от других планшетов на рынке F110 сочетает в себе чрезвычайную лёгкость и портативность, устойчивость к вибрациям, влаге, дождю, холоду и жаре. Также планшет может работать без подзарядки до 12 часов, что сделало его прекрасным решением для экстремальных применений в чрезвычайных ситуациях.

УЗНАТЬ БОЛЬШЕ

## Hirschmann в городском транспорте Мюнхена

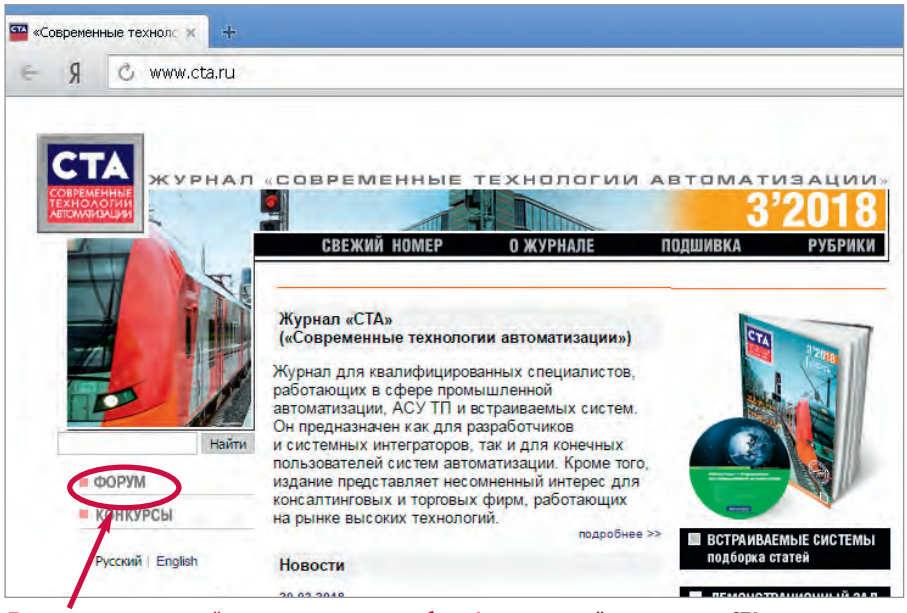
Городская система общественного транспорта в Мюнхене является одной и самых прогрессивных и развитых. Более 1170 станций и автобусных остановок составляют сеть маршрутов города протяжённостью более 600 километров. При этом контроль управления движением городского общественного транспорта осуществляется из центрального пункта управления.

Для улучшения качества обслуживания, а также реализации перспективы применения новых технологий, таких как современные информационные системы, видеонаблюдение, контроль движения и т.д., в компании MVG, являющейся второй по величине муниципальной транспортной компанией города, было принято решение внедрить на общественном транспорте технологию Industrial Ethernet.


Первыми по очереди прошли модернизацию поезда метро. В каждом поезде была организована резервированная Ethernet-подсеть, к которой были подключены различные системы состава, начиная от информационных и заканчивая контрольным оборудованием. В качестве сетевого оборудования были применены коммутаторы серии **Octopus** от **Hirschmann**, которые были установлены непосредственно в вагонах метро. Также модернизации подверглась и сетевая инфраструктура более чем 100 станций метро, сеть была реализована на основе технологии Industrial Ethernet с применением коммутаторов Hirschmann серии **MS30**. Проведённая модернизация и переход на технологию Industrial Ethernet позволили не только улучшить качество услуг, но и объединить в одну сеть городскую систему общественного транспорта.

УЗНАТЬ БОЛЬШЕ

## «СТА» в Internet: www.cta.ru




**Приглашаем читателей принять участие в работе форума на сайте журнала «СТА»: www.cta.ru**

## Мобильное приложение «Журнал «СТА»

Бесплатное приложение «Журнал «СТА» доступно пользователям Android в Google Play в разделе «Приложения/ Бизнес» и пользователям iOS в App Store в разделе «Бизнес».
С помощью этого приложения можно читать с экрана номера нашего журнала сразу после выхода их в свет.

УЗНАТЬ БОЛЬШЕ
в Google Play на Android

УЗНАТЬ БОЛЬШЕ
в App Store на iOS

**Редакция журнала «СТА» приглашает к сотрудничеству авторов и научных редакторов.**

**Телефон**: (495) 234-0635, **E-mail**: info@cta.ru

**Уважаемые читатели,** присылайте в редакцию вопросы, ответы на которые вы хотели бы увидеть на страницах журнала. Мы также будем благодарны, если вы сообщите нам о том, какие темы, по вашему мнению, должны найти своё отражение в журнале.

## Уважаемые рекламодатели,

журнал «СТА» имеет тираж 10 000 экз., распространяется по подписке, в розницу, через региональных распространителей, а также по прямой рассылке ведущим компаниям стран СНГ, что позволит вашей информации попасть в руки людей, принимающих решения о применении тех или иных аппаратных и программных средств.

УЗНАТЬ БОЛЬШЕ

## Журнал «СТА» доступен в печатной и электронной версиях

**Для квалифицированных специалистов,** работающих в сфере промышленной автоматизации, АСУ ТП и встраиваемых систем, на сайте журнала www.cta.ru может быть оформлена **бесплатная подписка** на его **печатную** или **электронную** версию. Бесплатная подписка действует до конца года.

При выборе бесплатной подписки на **ЭЛЕКТРОННУЮ** версию журнала вы будете подписаны на получение доступа к электронной версии журнала. Ссылка на журнал в электронном виде будет приходить на e-mail адрес, указанный в анкете.

При покупке **ЭЛЕКТРОННОЙ** версии журнала номер будет доступен в электронном виде **для чтения с экрана, загрузки или печати.**

Специалистам, выбравшим бесплатную подписку на **ПЕЧАТНУЮ** версию журнала, номера будут отправляться на указанный в форме адрес доставки.

**Для гарантированного и регулярного получения ПЕЧАТНОЙ** версии журнала необходимо оформить на неё **платную подписку** через подписное агентство «Роспечать» по каталогу «Роспечать».
Подписные индексы:
на полугодие – 72419, на год – 81872.

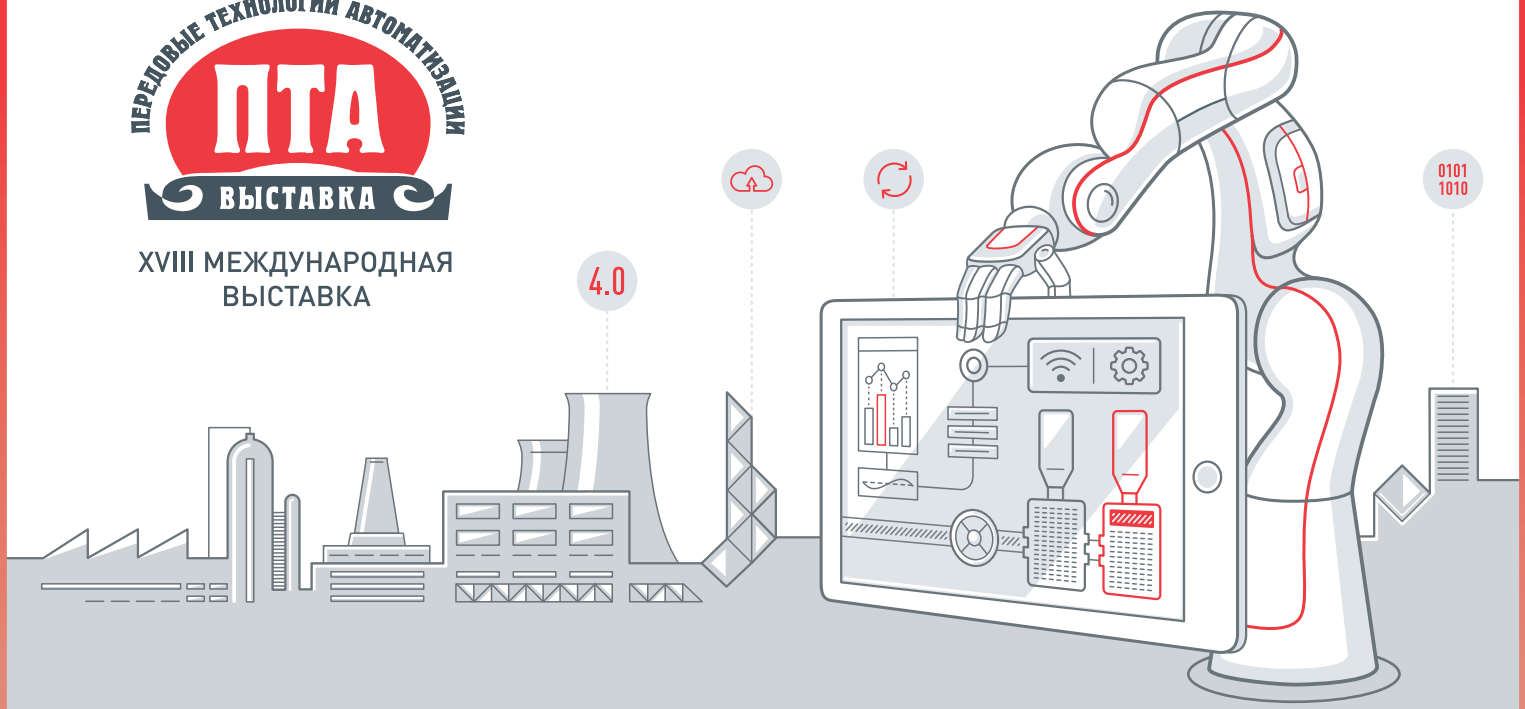
## РЕКЛАМА В НОМЕРЕ

ПЕРЕДОВЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ

ПТА

ВЫСТАВКА

XVIII МЕЖДУНАРОДНАЯ ВЫСТАВКА




# ПЕРЕДОВЫЕ ТЕХНОЛОГИИ АВТОМАТИЗАЦИИ

# ПТА-2018

**17-19 ОКТЯБРЯ 2018**

ЦВК «ЭКСПОЦЕНТР», МОСКВА

- Автоматизация промышленного предприятия
- Автоматизация технологических процессов
- Бортовые и встраиваемые системы
- Системная интеграция и консалтинг
- Системы пневмо- и гидроавтоматики
- Измерительные технологии
- Робототехника и мехатроника
- Облака, IoT, Big Data в промышленности

## В ДЕЛОВОЙ ПРОГРАММЕ

- Кибербезопасность на промышленном предприятии
- Промышленный интернет вещей (IIoT)
- Встраиваемые системы
- Промышленная автоматизация на пути к Industry 4.0

Совместно: ChipEXPO – 2018

При поддержке: Экспоцентр

Организатор: Экспоэлектроника

+7 (495) 234-22-10
event@pta-expo.ru
www.pta-expo.ru

# СТА 3/2018 TABLE OF CONTENTS

УЗНАТЬ БОЛЬШЕ

# ПРОМЫШЛЕННЫЕ СЕРВЕРЫ ПОСЛЕДОВАТЕЛЬНЫХ ИНТЕРФЕЙСОВ

## С РЕЗЕРВИРОВАННЫМ ПОДКЛЮЧЕНИЕМ К ETHERNET


**Скачайте диск с Техпортала ProSoft:**

**tp.prosoft.ru/CTA-3-2018**

**–40...+70°C**

## Серии EKI-1500, EKI-1200

ADVANTECH
*Enabling an Intelligent Planet*

- **Два порта Ethernet 10/100Base-TX с функцией резервирования**
- **Преобразование Modbus RTU/ASCII в Modbus TCP (серия EKI-1200)**
- **Режимы: виртуальный COM-порт, сервер/клиент TCP и UDP, Serial Tunnel**
- **Множественный доступ к COM-портам**
- **Автоматическое восстановление соединения**
- **Скорость передачи до 926,1 кбит/с**
- **Защита портов от электростатического разряда до 15 кВ постоянного тока**

**EKI-1521**
1 порт RS-232/422/485

**EKI-1222**
Шлюз Modbus RTU/ASCII в Modbus TCP

**EKI-1524**
4 порта RS-232/422/485

**EKI-1526**
16 портов RS-232/422/485

PROSOFT®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

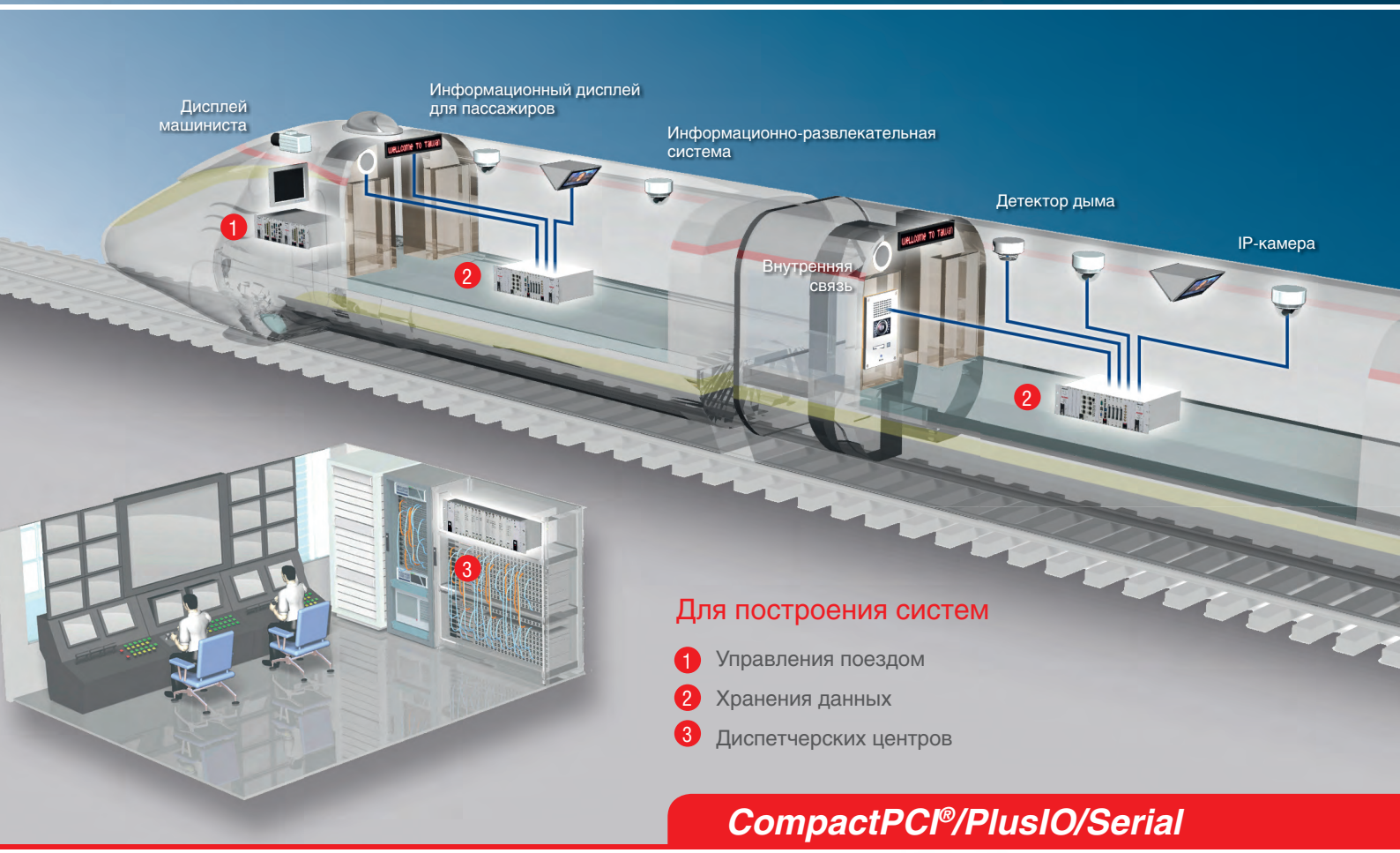
WWW.PROSOFT.RU

УЗНАТЬ БОЛЬШЕ

ADLINK TECHNOLOGY INC.

# Надежные CompactPCI

## компьютерные платформы для железнодорожных применений




### Для построения систем

1. Управления поездом
2. Хранения данных
3. Диспетчерских центров

## CompactPCI®/PlusIO/Serial

**cPCI-A3515**

Процессорная плата 3U CompactPCI Serial
с процессором Intel Core i7 4/5-го поколения и ECC

**cPCI-3510 (BL)**

Процессорная плата 3U CompactPCI PlusIO
с процессором Intel Core i7 4/5-го поколения и ECC

**cPCI-3620**

Процессорная плата 3U CompactPCI
с процессором Intel Atom E3800 SoC и ECC

**cPS-H325/WDC**

3U CompactPCI 8HP модуль питания PICMG 2.11
с диапазоном рабочих температур –40…+85°C