



Развитие технологии Industrial Ethernet на примере новинок коммуникационного оборудования

Михаил Дормаков

В статье на примерах новинок компаний Hirschmann и EtherWAN рассматриваются основные направления развития технологии Industrial Ethernet. Приведённые примеры наглядно иллюстрируют функциональные возможности и особенности применения современных сетевых устройств.

ВВЕДЕНИЕ

Ни у кого не осталось сомнений, что стандартом де-факто в промышленных коммуникациях становится Ethernet. И хотя на многих предприятиях переход на новый стандарт либо ещё не начался, либо не завершился в силу объективных причин (нехватка финансирования, долгий жизненный цикл оборудования для передачи данных в частности и всего промышленного оборудования в целом), случится это неизбежно.

История технологии Ethernet насчитывает уже более 40 лет, из них более 30 лет ведутся работы по её адаптации к промышленной среде. Первопроходцем в этом деле является немецкая компания Hirschmann, имеющая более чем 30-летний опыт разработок промышленного телекоммуникационного оборудования. Именитому европейскому разработчику и производителю буквально наступают на пятки азиатские компании. Уровень их разработок в последние годы значительно вырос, и хотя говорить о прямой конкуренции между западными и азиатскими производителями пока рано, следует признать, что у последних есть очень интересные технические решения по доступным ценам.

За 30 лет промышленный Ethernet прошёл большой путь развития, скорость передачи данных увеличилась на 3 порядка (с 10 Мбит/с до 10 Гбит/с), появились новые типы устройств, топологии сетей, методы и подходы к проектированию сети, её администрированию и обслуживанию. Но если до недавнего

времени развитие промышленного Ethernet можно было охарактеризовать как экстенсивное (увеличение полосы пропускания, появление новых сред передачи данных, включая беспроводные технологии, применение новых типов разъемов), то сейчас развитие стандарта (или скорее целого направления в телекоммуникациях) можно охарактеризовать как интенсивное. Отметим основные направления развития промышленных коммуникаций:

- расширение сфер применения и появление новых отраслевых стандартов;
- развитие и стандартизация технологий сетевого резервирования;
- активное развитие сегмента PoE-устройств и увеличение их мощности;
- увеличение производителями доли устройств с поддержкой стандарта Gigabit Ethernet при снижении их стоимости;
- новые решения в области безопасности как ответ на возникающие угрозы;
- расширение функций устройств путём совершенствования программного обеспечения.

Коммутаторы для подстанций: акцент на надёжности, масштабируемости и снижении затрат

Телекоммуникационное оборудование стандарта Ethernet находит всё больше новых сфер применения. Каждая из задач может обладать рядом уникальных свойств и создавать особые условия

внешней и внутренней среды для работы оборудования, и чаще всего эти условия вовсе не тепличные. В этом случае к оборудованию предъявляются особые требования, что ведёт к необходимости проведения соответствующих доработок, испытаний и сертификации изделий.

Одной из актуальных задач, решаемых в настоящее время в области промышленной автоматизации, является создание автоматизированной цифровой электрической подстанции. Работы в данном направлении ведутся достаточно давно, разработан международный стандарт IEC 61850 (в России МЭК 61850). Он определяет коммуникационные процессы на подстанции, абстрактные модели оборудования и выполняемые им функции, общие требования к оборудованию, описывает методики его испытаний и приёмки. Коммуникационное оборудование, предназначенное для эксплуатации на объектах электроэнергетики, давно и успешно применяется. В настоящее время в России существуют полностью цифровые подстанции, находящиеся в опытной эксплуатации.

Коротко обозначим требования, предъявляемые к сетевому оборудованию для подстанций.

- Стойкость к ЭМИ и статическому электричеству.
- Широкий температурный диапазон и способность работать в суровых климатических условиях.
- Резервированное питание.
- Стойкость к механическим воздействиям.



Рис. 1. Промышленный коммутатор серии GRS, сертифицированный по МЭК 61850-3

- Поддержка стандартизированных протоколов сетевого резервирования.
- Поддержка современных протоколов удалённого управления.
- Поддержка функций сетевой безопасности и протоколов высокоточной синхронизации времени.

Под брендом Hirschmann давно выпускается оборудование, отвечающее этим требованиям и поддерживающее стандарт МЭК 61850-3. Недавно линейка коммутаторов для подстанций пополнилась ещё одной серией, получившей наименование Greyhound (или серия GRS, рис. 1). Производитель позиционирует данные устройства как бюджетное решение, призванное составить достойную конкуренцию прекрасно зарекомендовавшей себя серии MACH1000.

Функционал коммутатора основан на новой операционной системе HiOS (собственная разработка Hirschmann). Устройство имеет защищённое исполнение, пассивное охлаждение, монтируется в 19" стойку. Имеется поддержка профиля промышленного протокола МЭК 61850.

Серия представлена двумя базовыми версиями – на 16 портов 10/100Base-TX и на 8 портов 10/100Base-TX и 8 портов типа SFP. Каждая из базовых версий может иметь 4 гигабитных комбинированных uplink-порта.

Современная автоматизированная подстанция должна обладать гибкостью и масштабируемостью. Эти два качества легко достижимы с коммутаторами GRS благодаря наличию в них конфигурируемого интерфейсного модуля «горячей» замены. В модуле может быть до 8 портов Fast Ethernet, имеющих различные виды разъёмов и сред передачи данных (медной и оптической различных типов).

Поддерживается управление устройством через Web-интерфейс, Telnet, HTTP/S, TFTP, SNMP, реализован протокол канального уровня LLDP. Имеются широкие возможности диагностики работы устройства и сети (сигнальное реле, сообщения syslog, RMON, SNMP-trap).

Возможности сетевого резервирования обеспечены поддержкой стандартизированных протоколов MRP и RSTP, а также агрегированием каналов LACP.

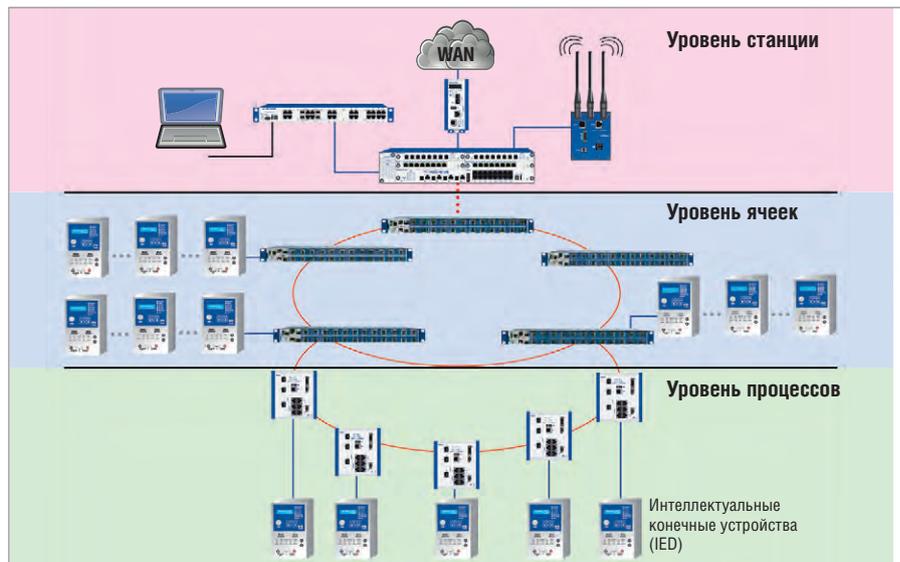


Рис. 2. Система автоматизации подстанции по стандарту МЭК 61850 с трёхуровневой коммуникационной сетью

Сетевая безопасность обеспечивается благодаря применению развитых механизмов авторизации пользователей (протокол IEEE 802.1x, RADIUS), списков доступа (ACL), ограничению доступа по MAC- и IP-адресам, использованию локальных учётных записей, разноразрядных политик доступа, паролей.

Также следует отметить поддержку протокола синхронизации времени SNTP.

Согласно стандарту МЭК 61850 система автоматизации подстанции состоит из трёх уровней: уровня станции, контрольного уровня и исполнительного уровня (рис. 2). Коммуникационная сеть между этими тремя уровнями делится на сеть уровня станции и сеть нижнего уровня (сеть процессов). Для первой характерны более низкие требования ко времени восстановления после сбоя, к задержкам передачи данных, к потерям пакетов и синхронизации времени. Вторая требует гарантированной доставки сообщений, минимального (в идеале нулевого) времени восстановления и высокоточной синхронизации порядка десятков наносекунд.

Исходя из этого, а также с учётом технических характеристик можно сделать вывод, что коммутаторы серии GRS можно применять в сети уровня станции. В то же время для сети уровня процессов подойдут коммутаторы серии RSP, поддерживающие протоколы нулевого времени восстановления после сбоя PRP и HSR, а также протокол высокоточной синхронизации времени PTPv2.

Более подробно ознакомиться с подходом к проектированию цифровой подстанции можно в цикле статей «Этапы создания эффективной системы автоматизации подстанции» [1].

НОВЫЕ ВОЗМОЖНОСТИ PoE-КОММУТАТОРОВ ДЛЯ БЕЗОПАСНОГО ГОРОДА

С развитием современных технологий появилось куда больше возможностей по обеспечению безопасности на улицах больших и малых населённых пунктов нашей необъятной Родины. Прежде всего за это стоит благодарить повсеместное распространение всемирной паутины, совершенствование сетевых проводных и беспроводных технологий и систем видеонаблюдения. Активно развиваются такие программы, как «Безопасный город» (с поддержкой властей или же на общественных началах). В торговых центрах и других общественных местах устанавливаются камеры высокого разрешения, фиксирующие события и помогающие в расследовании происшествий или в предупреждении правонарушений. Установка камер предполагает строительство сетевой инфраструктуры и прокладку цепей питания. Задача упрощается в случае использования технологии передачи питания по сигнальному кабелю PoE. В настоящее время существует два стандартизированных варианта этой технологии: IEEE 802.3af с мощностью подключаемого устройства до 15,4 Вт и IEEE 802.3at с мощностью до 30 Вт. Компания EtherWAN одной из первых вывела на рынок коммутатор с допустимой мощностью нагрузки до 60 Вт на канал – это серия EX78602 (рис. 3). Коммутаторы имеют 4 канала с мощностью 30 Вт на канал и два – 60 Вт на канал, при этом 6 PoE-портов позволяют передавать данные со скоростью до 100 Мбит/с. Имеются два uplink-порта Gigabit Ethernet, конфигурируемых при заказе (медные, оп-



Рис. 3. Промышленные PoE-коммутаторы серии EX78602

тические либо SFP). Функции коммутатора полностью соответствуют II уровню модели OSI, поддерживаются стандартизированные технологии резервирования семейства xSTP, а также фирменная α -Ring со временем восстановления <15 мс. Из других особенностей коммутатора следует отметить диапазон рабочих температур от -40 до +75°C и напряжение питания 52...57 В постоянного тока.

Хотя технология, позволяющая подать потребителю мощность до 60 Вт, пока не стандартизирована, она уже успешно применяется. Протестирована возможность совместной работы коммутатора серии EX78602 с уличными камерами нескольких известных производителей.

Следует также отметить, что применение в системах безопасности и видеонаблюдения промышленных коммутаторов вместо офисных даёт ряд преимуществ. Так, это избавляет от необходимости встраивать в шкаф с коммутаторами дополнительную систему подогрева/охлаждения в случае установки на улице (а при ориентации на использование технологии PoE это ещё более актуально). Также значительно снижаются затраты на сервисное обслуживание. Надёжность промышленного сетевого оборудования высока, и в долгосрочной перспективе его относительно высокая стоимость с лихвой окупается.

При проектировании сети видеонаблюдения нужно хорошо продумать её топологию. При использовании кольцевого резервирования нужно учесть, что хотя в этом случае топология имеет вид кольца, по факту она является линейной, что накладывает ограничения на объём передаваемых данных и количество коммутаторов в коль-



Рис. 4. Промышленный управляемый 8-портовый коммутатор Gigabit Ethernet серии EX70900

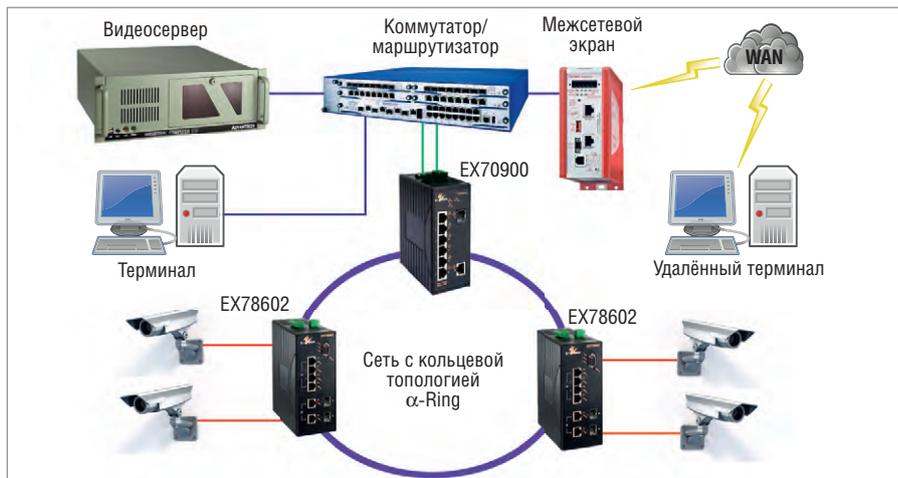


Рис. 5. Пример сети системы видеонаблюдения на базе коммутаторов серии EX70900 и EX78602

це. При использовании большого количества коммутаторов и камер высокого разрешения полосы пропускания магистральных портов может не хватать. В этом случае возможны заметные задержки передачи данных или даже их потеря, поэтому следует внимательно подойти к расчёту объёмов передаваемых данных.

Возможным выходом из положения может стать применение интеллектуальной системы безопасности. Суть её состоит в применении интеллектуальных камер видеонаблюдения, анализирующих обстановку в кадре и имеющих встроенную систему принятия решений о наличии событий, требующих внимания оператора и принятия решения человеком. Такими событиями могут быть появление определённого человека (анализируется лицо), массового скопления людей, изменение интенсивности перемещения объектов, обнаружение пламени и многие другие ситуации. Камера не передаёт в сеть непрерывный видеопоток, а включается в случае необходимости только в момент обнаружения заранее определённого события. В остальное время трафик ограничивается передачей коротких сообщений вида «всё спокойно».

GIGABIT ETHERNET В МАССЫ

Как правило, для подключения IP-видеокамер достаточно, чтобы коммутатор имел порты Fast Ethernet. При объединении в сеть нескольких коммутаторов следует использовать магистральные порты Gigabit Ethernet и при необходимости – агрегирование каналов. Для обеспечения достаточной пропускной способности при передаче больших объёмов данных с множества камер (или других источников интенсивного трафика) сеть более высокого уровня должна строиться на основе коммутаторов, все порты которых гигабитные. Примером

такого устройства является новинка компании EtherWAN – управляемый коммутатор серии EX70900 (рис. 4). Коммутаторы этой серии предназначены для применения в сетях IP-видеонаблюдения, системах машинного зрения и других промышленных сетях с высокими требованиями к пропускной способности и надёжности. Устройство выполнено в компактном корпусе с пассивным охлаждением и монтируется на DIN-рейку, имеет 8 портов Gigabit Ethernet (6 типа RJ-45 и 2 на выбор: RJ-45, оптические или SFP). Поддерживаются все основные функции управляемого коммутатора II уровня OSI: VLAN, GVRP, QoS, ограничение полосы пропускания, IGMP-Snooping, зеркалирование портов (в том числе n:1), DHCP. Доступны следующие технологии сетевого резервирования: STP, RSTP, MSTP, кольцевое резервирование α -Ring, агрегирование каналов. Коммутатор управляется и настраивается через Web-интерфейс, SNMP, консоль, имеется возможность обновить прошивку и текущие настройки через TFTP-сервер. Диапазон рабочих температур от -40 до +75°C. Пример топологии сети, построенной на основе коммутаторов серий EX78602 и EX70900, представлен на рис. 5.

В промышленных сетях особо важных объектов, требующих применения технологий резервирования, высокой синхронизации времени, контроля полосы пропускания и применения средств сетевой безопасности, должны использоваться управляемые коммутаторы. Однако существует много гораздо менее требовательных задач, решение которых можно возложить на неуправляемые устройства.

Большинство жилых зданий не имеет специально приспособленного помеще-

оборудования, поэтому его размещение часто носит стихийный характер. Коммутаторы устанавливаются на чердаках, в подвалах, плохо отапливаемых помещениях. Вместе с тем компьютерное и сетевое оборудование для домашнего использования давно оснащается портами Gigabit Ethernet, поэтому вполне логично использовать для предоставления услуг широкополосного доступа к сети Интернет гигабитные каналы передачи данных. Для этих целей вполне подходит такой коммутатор, как EX39924 компании EtherWAN. Устройство относится к категории бюджетных, оно неуправляемое, оснащено 24 портами Gigabit Ethernet, имеет пассивное охлаждение и диапазон рабочих температур от -10 до +60°C. В коммутаторе применяется неблокируемая архитектура, что позволяет длительное время эксплуатировать его при полной загрузке каналов (например, если большинство жителей дома вдруг решат посмотреть по выделенному каналу футбольную трансляцию). Расширенный диапазон рабочих температур позволяет установить устройство в нежилом помещении. Коммутатор не требует настройки и удаленного администрирования. Выпускается версия с 16 комбинированными портами RJ-45/SFP, поэтому при необходимости сеть легко масштабируется на любые расстояния с применением оптических кабелей и сменных оптических модулей. Преимущество SFP-портов также в том, что они повышают ремонтпригодность и сокращают время простоя сетей: вышедший из строя модуль легко заменить новым.

Также данный коммутатор можно применять при автоматизации технологических процессов, нетребовательных ко

времени восстановления сети после сбоя и не предъявляющих требований к безопасности сети и эффективному управлению потоками данных.

ЕЩЁ РАЗ О КИБЕРБЕЗОПАСНОСТИ

Проблема защиты промышленных объектов от киберугроз давно вызывает беспокойство специалистов различных отраслей и руководства на самом высоком уровне. Хотя в России пока нет стандартов, чётко определяющих стратегии и подходы к обеспечению информационной безопасности в промышленности, интеграторам, разработчикам, сотрудникам предприятий и всем тем, кто так или иначе связан с промышленным производством, необходимо со всей серьёзностью отнестись к обеспечению эффективной защиты информационной инфраструктуры АСУ ТП.

С целью обобщения имеющихся методик и опыта в области повышения безопасности промышленных объектов на западе был разработан и принят стандарт IEC 62443 (ранее имевший обозначение ISA-99). Он описывает общий подход к обеспечению сетевой безопасности промышленных объектов. При этом следует иметь в виду, что каждая отрасль, каждое промышленное предприятие требует индивидуального подхода к формированию стратегии защиты. В частности, в США корпорацией NERC (North American Reliability Corporation) был разработан стандарт NERC CIP (Critical Infrastructure Protection), применяемый для проектирования систем безопасности объектов энергетики.

В статье «Промышленные сети в условиях возросших киберугроз» [2] по-

дробно описаны методы повышения безопасности промышленных сетей и систем управления. Один из основных шагов на пути к безопасной промышленной сети — её сегментация, создание безопасных зон и определение защищённых путей передачи данных между ними. При этом необходимо строго регламентировать, какие данные должны передаваться и кто имеет к ним доступ. Также нужно выделить тот факт, что для обеспечения защиты промышленного сектора следует применять технологии и решения, специально разработанные именно для него.

Необходимый элемент для сегментации сети — межсетевые экраны. Устройства должны иметь промышленное исполнение и функции для применения на промышленном предприятии. По своему назначению промышленные межсетевые экраны можно разделить на два вида: устройства, применяемые на границе сети, и устройства для защиты производственных ячеек. Первые предназначены для отделения промышленного сегмента от офисной или корпоративной сети. Вторые позволяют сегментировать промышленную сеть и наделить специальными функциями, призванными обезопасить промышленные протоколы (например Modbus или OPC). Применяемая в них технология глубокого анализа пакетов DPI (Deep Packet Inspection) позволяет обезопасить техпроцессы от вредоносного ПО, передаваемого в пакетах, разрешённых классическим брандмауэром.

Примером устройства для установки на границе сети может служить серия межсетевых экранов Eagle20/30 компании Hirschmann (рис. 6). Недавно она



Упрочнённые решения для нефтегазовых, морских приложений и наблюдения



rBOX510-6COM (ATEX/C1D2) -40...+70°C

Упрочнённая безвентиляторная встраиваемая система для монтажа на DIN-рейку с процессором Intel® Atom™ E3827 1,75 ГГц и с сертификатом взрывозащиты

- 4 изолированных порта RS-232/422/485 и 2 RS-232/422/485
- 1 изолированный порт цифрового ввода-вывода (8 входов/8 выходов)
- Поддержка одного накопителя 2,5" SATA SSD/HDD (или mSATA) и одного CompactFlash™
- Поддержка пакета ПО удаленного управления AXView 2.0



fBOX330-870-FL

Безвентиляторная встраиваемая система с процессором 3-го поколения Intel® Core™ и Intel® QM77 для морских ПК



eBOX671-885-FL

Интеллектуальная безвентиляторная встраиваемая система с процессором Intel® Core™ i7/i5/i3 и Celeron®, Intel® Q87, с поддержкой 4 PoE, 6 USB 3.0, HDMI/DVI/DisplayPort и 2 PCIe Mini Card

Axiomtek Co., Ltd.

Tel: +886-2-2917-4550 Fax: +886-2-2917-3200
E-mail: adam.lan@axiomtek.com.tw

www.axiomtek.com



Рис. 6.
Многофункциональный межсетевой экран Hirschmann Eagle30

обзавелась новой усовершенствованной программной начинкой – операционной системой HiSecOS версии 2.0, определяющей функции устройства. Среди основных характеристик устройств нужно отметить трансляцию адресов NAT, широкие возможности фильтрации трафика и анализа его содержимого в соответствии с установленными правилами, управление доступом на основе ACL (на II и III уровне), технологии резервирования на III уровне VRRP, протокол OSPFv2, возможность организации VPN, ограничение доступа к сети по паролю и на основе распределения ролей. Устройство может управляться удалённо по протоколу SNMP, RADIUS, SSH2/SFTP, через Web-интерфейс, локально через консоль. Брандмауэры Eagle 20/30 имеют 4 порта 100Base-TX, до двух портов Gigabit Ethernet (используются SFP-модули), а также могут оснащаться двумя портами с технологией передачи данных по телефонным проводам SHDSL. Наличие технологии SHDSL позволяет применять роутеры Eagle 20/30 в качестве оборудования «последней мили» при подключении к Интернет-провайдеру либо для соединения удалённых сегментов промышленной сети. Имея в сумме 8 различных портов, Eagle 20/30 является, по сути, уникальным устройством среди аналогичных промышленных межсетевых экранов/маршрутизаторов.

Для защиты производственных ячеек можно использовать программно-аппаратный комплекс Tofino Xenon известного бренда Tofino Security, принадлежащего концерну Velden (рис. 7). Комплекс состоит из аппаратной платформы и специализированного программного обеспечения. Аппаратная платформа конфигурируемая, может иметь различные ти-



Рис. 7.
Программно-аппаратный комплекс для защиты промышленного IT-контура Tofino Xenon

пы портов (RJ-45 или оптические), различные диапазоны рабочих температур и отраслевые сертификаты. Программное обеспечение состоит из программы-конфигуратора для комплексной настройки безопасности сети и программных модулей. Программные модули определяют функции межсетевого экрана Tofino Xenon. Каждое устройство имеет индивидуальный набор модулей, в зависимости от требований, предъявляемых к нему. Базовым является модуль межсетевого экрана Firewall LSM (LSM – Loadable Security Module, загружаемый модуль безопасности). Дополнительно можно установить модули глубокого анализа пакетов промышленных протоколов Modbus TCP, Ethernet IP, OPC. Комплекс обладает поддержкой более 125 ИТ-протоколов и промышленных коммуникационных протоколов.

ЗАКЛЮЧЕНИЕ

Приведённые примеры чётко иллюстрируют основные тенденции в области развития Industrial Ethernet. Появление новых стандартов, таких как МЭК 61850 в области энергетики, отражает необходимость приведения нормативной базы в соответствие с новыми реалиями и техническими решениями, а также проникновение технологий Ethernet в эту область. Новые стандарты резервирования (IEC 62439), позволяющие обеспечить нулевое время восстановления после сбоя и гарантированную доставку информации, применяются для построения сетей промышленных предприятий и, в частности, внедряются на объектах энергетики. Появление новых

коммутаторов с поддержкой технологии PoE и рост бюджета мощности позволяют расширить сферы их применения и функциональность систем управления и безопасности. Увеличение скоростей передачи данных расширяет области применения коммутационной техники, повышает качество обслуживания объектов и пользователей и даёт возможность масштабировать сети без потерь и задержек данных. Также гигабитные сети стали очевидно доступнее. Появление новых технических решений и устройств для защиты сетевой инфраструктуры АСУ ТП, улучшение методик и подходов к сетевой безопасности, их стандартизация и сертификация позволяют создать системы, устойчивые к негативным внешним и внутренним воздействиям. Постоянное совершенствование программной и технической составляющей сетевых устройств, выпуск новых версий ПО, его регулярное обновление и установка патчей способствуют повышению безопасности и расширяют функциональные возможности устройств связи. ●

ЛИТЕРАТУРА

1. И. Лопухов. Этапы создания эффективной системы автоматизации подстанции: [ч. 1–5] // Современные технологии автоматизации. – 2013. – № 1; № 2; № 3.
2. И. Лопухов. Промышленные сети в условиях возросших киберугроз // Современные технологии автоматизации. – 2014. – № 4.

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

НОВОСТИ НОВОСТИ НОВОСТИ НОВОСТИ

«ТЕХНОПРОМ–2015»

В Новосибирске завершила работу выставка III Международного форума технологического развития «ТЕХНОПРОМ–2015», которую посетили более 7500 гостей.

В 2015 году более 150 компаний из России, Франции, Японии, США, Словении и других стран представили новейшее оборудование, инновационные технологии, решения и продукты, способные стать основой технологического прорыва российской экономики. Выставочная экспозиция дополняет деловую программу форума, демонстрируя технологический и инновационный потенциал российских предприятий, работающих в высокотехнологичных отраслях экономики. Отличительной чертой является авторитетнейший состав участников форума: здесь присутствуют люди, интерес которых к той или иной разработке, представленной экспонентами, может дать серьёзный толчок к развитию предприятия и отрасли в целом.

Основные разделы выставки: аэрокосмические, энергоэффективные и SMART-технологии, наука, технологии в условиях Арктики, машиностроение, оптические, био- и нанотехнологии, ГЛОНАСС, инновационная инфраструктура и институты развития. Была организована специализированная площадка TECHNO View, где прошло более 10 технологических презентаций и мастер-классов.

Ознакомившись с экспозицией выставки «ТЕХНОПРОМ–2015», заместитель Председателя Правительства Российской Федерации Д.О. Рогозин отметил, что такие выставки объединяют фундаментальную науку и промышленность. «Проекты, представленные на выставке, должны находить практическое применение. Главный вопрос сегодня – как перебросить связующий мост между фундаментальной наукой и внедрением новых технологий в производство. Для этого надо создать переход от разработки до реализации», – сказал он. ●



HIRSCHMANN

A BELDEN BRAND



Radio

Clear Space®
WLAN

LTE
GSM

UMTS

WLAN проходит без помех

Clear Space® — запатентованная технология получения чистого сигнала в шумных средах



Серия Hirschmann OpenBAT

Беспроводное оборудование стандарта IEEE 802.11n (Wi-Fi)

- 1 или 2 радиомодуля IEEE 802.11a/b/g/h/n
- Скорость передачи до 450 Мбит/с
- Технологии MIMO 3x3, MESH, WDS
- -40...+75°C, конформное покрытие
- Внутреннее и внешнее исполнение IP40/IP67

Вся необходимая инфраструктура:

BAT-C – простой и компактный клиент сети

Антенны, кабели, грозозащита

BAT-Controller – аппаратный централизованный контроллер точек доступа

BAT-Planner – ПО для расчета зон покрытия и скоростей передачи на плане объекта



ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР ПРОДУКЦИИ HIRSCHMANN

PROSOFT®

МОСКВА
С.-ПЕТЕРБУРГ
АЛМА-АТА
ВОЛГОГРАД
ЕКАТЕРИНБУРГ
КАЗАНЬ
КНБВ
КРАСНОДАР
Н. НОВГОРОД
НОВОСИБИРСК
ОМСК
САМАРА
УФА
ЧЕЛЯБИНСК

Тел.: (495) 234-0636 • Факс: (495) 234-0640 • info@prosoft.ru • www.prosoft.ru
 Тел.: (812) 448-0444 • Факс: (812) 448-0339 • info@spb.prosoft.ru • www.prosoft.ru
 Тел.: (727) 329-5121; 320-1959 • sales@kz.prosoft.ru • www.prosoft-kz.com
 Тел.: (8442) 260-048 • volgograd@prosoft.ru • www.prosoft.ru
 Тел.: (343) 376-2820; 356-5111 • Факс: (343) 310-0106 • info@prosoftsystems.ru • www.prosoftsystems.ru
 Тел.: (843) 203-6020 • Факс: (843) 203-6020 • info@kzn.prosoft.ru • www.prosoft.ru
 Тел.: +38 (044) 206-2343; 206-2478 • info@prosoft-ua.com • www.prosoft-ua.com
 Тел.: (861) 224-9513 • Факс: (861) 224-9513 • krasnodar@prosoft.ru • www.prosoft.ru
 Тел.: (831) 215-4084 • Факс: (831) 215-4084 • n.novgorod@prosoft.ru • www.prosoft.ru
 Тел.: (383) 202-0960; 335-7001/7002 • Факс: (383) 230-2729 • info@nsk.prosoft.ru • www.prosoft.ru
 Тел.: (3812) 286-521 • Факс: (3812) 315-294 • omsk@prosoft.ru • www.prosoft.ru
 Тел.: (846) 277-9166 • Факс: (846) 277-9165 • info@samara.prosoft.ru • www.prosoft.ru
 Тел.: (347) 292-5216/5217 • Факс: (347) 292-5218 • info@ufa.prosoft.ru • www.prosoft.ru
 Тел.: (351) 239-9360 • chelyabinsk@prosoft.ru • www.prosoft.ru