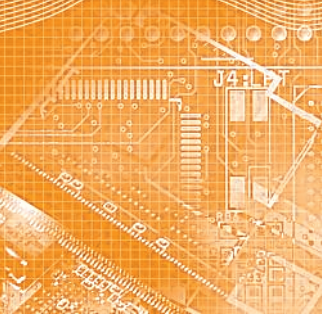


Как защитить АСУ ТП: экспертиза Innostage

Айрат Мухаметшин

Критическая информационная инфраструктура сегодня – одна из основных целей для киберпреступников. Рассказываем об уязвимостях и отличительных особенностях АСУ ТП – и о том, как защитить их от атак.

В ушедшем году ФСБ России зафиксировала более 5 тысяч кибератак на критическую инфраструктуру России. Среди целей атак следует выделить промышленный сектор – на него, по данным Positive Technologies, было совершено 223 атаки, причем 97% из них – целевые, направленные на критическую информационную инфраструктуру.

Если раньше критическая инфраструктура интересовала в основном коммерчески мотивированных хакеров и группировки, атаки которых были направлены на извлечение прибыли, то сегодня одна из основных целей атак – нанесение максимального материального ущерба. Чаще всего цели достигаются путем воздействия на АСУ ТП и, соответственно, на автоматизируемый технологический процесс, что приводит к сбоям и останову на производстве.

Данные обстоятельства стали причиной повышенного внимания к защите автоматизированных систем управления технологическими процессами (АСУ ТП). Ранее им не уделялось достаточно внимания. Считалось, что АСУ ТП, находящиеся вне корпоративной сети, и так достаточно безопасны, ведь «АСУ ТП напрямую к Интернету не подключена».

Но, несмотря на отсутствие «прямого подключения к Интернету», АСУ ТП становится объектом успешных атак – технологический сегмент ЛВС предприятий перестал быть физически отделённым, будучи связанным с корпоративным сегментом через системы класса MES (Manufacturing execution system).

Соответственно, даже некогда отдельные системы стали частью общей информационной инфраструктуры предприятия. А с некоторых пор к MES-системам добавились СУУТП (APC – advanced process control) – системы улучшения управляемостью технологическими процессами, которым в силу выполняемого ими функционала необходима сетевая связность с АСУ ТП.

То есть необходимость автоматизации управления производством как таковым стала причиной появления «объединяющей прослойки» между корпоративным и технологическим сегментами предприятия, объединяя ранее разрозненные локальные системы в единую информационную инфраструктуру.

Помимо этого, АСУ ТП уже не представляет из себя «чёрный ящик» с точки зрения используемых технологий информатизации. С одной стороны, в основе построения верхнего уровня систем автоматизации лежат всё те же «гражданские» широко распространённые протоколы передачи данных (например, стек протоколов TCP/IP).

С другой, современные редакции протоколов прикладного уровня (например, Modbus или OPC) используют в качестве транспорта протокол TCP. Также широкое распространение получили и проприетарные протоколы (например, S7 от Siemens), но и они не лишены уязвимостей, которые эксплуатируют злоумышленники для совершения атак на инфраструктуру.

Поэтому серверы управления, серверы баз данных АСУ ТП с точки зрения технологий реализации компьютерных атак не представляют для злоумышленника «особенный» объект. Чего не скажешь про потенциальный ущерб, наносимый данной атакой.

Поэтому ещё одна причина повышенного внимания к обеспечению ИБ АСУ ТП – развитие управляющих функций. Распределённые системы управления выполняют значительную часть операций по управлению промышленными объектами и технологическими процессами на них.

Особенности АСУ ТП как объекта защиты

Несмотря на унификацию используемых технологий информатизации и передачи данных, системы промышленной автоматизации как объекты защиты обладают рядом отличительных особенностей, которые влияют на применяемые методы обеспечения кибербезопасности и отличают их от систем корпоративного сегмента.

Среди них:

- длительный жизненный цикл (наличие нескольких поколений СВТ и ПО в составе одного объекта автоматизации);
- наличие специального ПО и оборудования, работающих в определённой конфигурации и чувствительных к внесению изменений;
- чувствительность к задержкам передачи текущих значений параметров производственного процесса, управляющей информации;
- использование специализированных проприетарных протоколов передачи данных с доказанными уязвимостями.

Данные особенности способствуют реализации широкого спектра угроз информационной безопасности, что особенно опасно ввиду критичности объектов автоматизации с точки зрения промышленной безопасности и последствий для окружающей среды.

Основными векторами реализации угроз ИБ являются:

- заражение вредоносным кодом,
- атаки из внешних компьютерных сетей,
- несанкционированный доступ к компонентам систем управления и обрабатываемой информации,
- приведение управляющих систем в состояние «отказ в обслуживании»,
- модификация данных, файлов, уставок, параметров управляющих команд.

Кроме того, длительный жизненный цикл, являясь с точки зрения автоматизации производства, благом, в то же время является полной противоположностью с точки зрения ИБ – ряд используемых ОС уже снят с поддержки производителя, то есть прекращён выпуск обновлений безопасности, что позволяет находить новые бреши в «обороне».

В нашей практике встречались случаи, когда переставала существовать фирма – производитель и интегратор ПТК АСУ ТП, при этом сама АСУ ТП продолжала функционировать. Справедливости ради, устаревшие системы автоматизации встречаются всё реже и реже.

Особенности построения систем защиты АСУ ТП

Ключевая особенность организации защиты АСУ ТП – это обеспечение состояния защищённости при необходимости соблюдения требований высокой доступности сервисов автоматизации.

Многие компоненты систем чувствительны к внесению изменений в конфигурацию – как вмешательство в работу комплекса автоматизации, так и изменение состава его компонентов с дальнейшим изменением логики информационных взаимодействий несёт в себе риски нарушения (сбоев) хода технологического процесса. Это как и необходимость перезагрузки серверов и АРМ, так и изменение конфигурации ЛВС и настроек сетеобразующего оборудования. И если в случае необходимости перезагрузки серверов и АРМ риски можно нивелировать поочерёдной установкой и настройкой средств защиты на резервированных АРМ и серверах с последующей проверкой корректности функционирования, то риски вмешательства в функционирование ЛВС, когда технологический объект управления находится «на режиме», нивелировать полностью не удаётся.

Поэтому оптимальным вариантом проведения работ является внедрение средств защиты во время технологического останова, но если такой возможности нет – то план производства работ прорабатывается особенно тщательно, с привлечением в том числе технологов и специалистов из числа оперативного персонала для наиболее точного прогнозирования последствий тех или иных действий по установке и настройке средств защиты.

Для защиты систем автоматизации применяют как средства, используемые в корпоративном сегменте, так и специализированные средства, разработанные для применения в промышленной автоматизации. Отличием в функционале может служить, например, способность межсетевого экрана работать с промышленными (в том числе проприетарными) протоколами передачи данных. Одним из способов вредоносного воздействия на систему автоматизации может служить эксплуатация уязвимостей в промышленных протоколах передачи данных.

Немаловажен фактор ресурсоёмкости средства защиты ввиду частого наличия требования высокой доступности сервисов автоматизации. Поэтому, например, настройка средств антивирусной защиты «по умолчанию» чаще всего приводит к недопустимой нагрузке на аппаратные ресурсы чувствительных компонентов комплекса автоматизации.

Выходом из ситуации может быть «тонкая» настройка антивируса для снижения ресурсоёмкости либо использование промышленного антивируса, изначально «заточенного» для работы в промышленных сетях.

Целесообразность применения того или иного функционала средства защиты определяется: применяемыми в объекте защиты технологиями информатизации, критичностью защищаемого ресурса (актива), «местоположением» защищаемого ресурса в архитектуре системы автоматизации.

Из дополнительных факторов следует выделить физическую среду функционирования защищаемого комплекса автоматизации – требования по климатике (например, отапливаемые серверные помещения либо неотапливаемый блок-бокс контрольного пункта телемеханики), условия размещения в монтажном конструктиве (шкаф стоечного исполнения, крепление на DIN-рейку и т.д.), агрессивность среды (требования пыле- и влагозащищённости используемых программно-аппаратных средств) – возможность активного охлаждения или обязательное пассивное охлаждение.

Если говорить о корпоративном сегменте, то физическая среда функционирования «стандартная» – капитальное серверное помещение с регулируемой климатикой.

С чего начинать построение системы защиты?

Первый этап должен быть самым простым и доступным, поэтому первоочередные мероприятия заключаются в настройке уже имеющихся средств защиты информации встроенного в АСУ ТП функционала безопасности: механизмов контроля и управления доступом, регистрации и учёта, резервного копирования настроек и данных, так и средства обеспечения сетевой безопасности (при их наличии).

Если средства обеспечения сетевой безопасности (межсетевые экраны) расположены между корпоративным и технологическим сегментами, то в качестве первоочередных мер необходимо пересмотреть правила межсетевых взаимодействий в сторону усиления (по принципу «всё, что не разрешено, – то запрещено») и сегментации ЛВС (выделение сегментов для АСУ ТП, сервисов управления производством).

Реализация данных мероприятий не требует длительных согласований и существенных капитальных вложений, но при этом существенно повышают защищённость комплексов автоматизации от самых распространённых угроз.

Следующий этап (он может быть как вторым, так и «нулевым») – определение целевого состояния безопасности, – то есть состояние и конфигурация системы с настроенными механизмами безопасности (здесь речь идёт уже не только про встроенные, но и наложенные средства), позволяющие системе стабильно функционировать в условиях кибератак – то есть когда приняты меры к нейтрализации выявленных актуальных угроз ИБ и нивелированию сопутствующих рисков.

Определение целевого состояния безопасности служит основой для выработки плана (дорожной карты) реализации мероприятий по обеспечению ИБ. В плане может быть отражена очерёдность реализации (внедрения) мер и необходимые затраты.

Защита АСУ ТП – часть общей ИБ-стратегии предприятия

Дорожная карта мероприятий по обеспечению ИБ АСУ ТП должна ставить целью не только реализацию набора мер как таковых, но и выстраивание данных мер (не только технических, но и организационных) в связную и функционально согласующуюся систему защиты.

Меры не должны быть реализованы «сами по себе», а быть оптимальными (не избыточными), взаимоувязанными и неконфликтующими, а также не снижать управляемость технологическими процессами.

Для этого необходима точная и детальная настройка средств защиты. Во-первых, важно учесть нюансы функционирования АСУ ТП как критичного программно-технического комплекса; во-вторых – чтобы «специальный» функционал (например, разбор и анализ тегов, разбор проприетарных промышленных протоколов и т.д.) активно использовался; в-третьих – чтобы система защиты АСУ ТП являлась частью единой системы кибербезопасности, необходимо полноценное «встраивание» средств обеспечения ИБ АСУ ТП в соответствующую инфраструктуру. А встраивание специализированных средств защиты должно быть рассмотрено не только с точки зрения управления системой ИБ, но и получения от данных средств событий безопасности для последующего анализа и выработки мер по ИБ на основе результатов анализа и корреляции данных событий. ●

Автор – сотрудник компании Innostage

НОВОСТИ реклама

MISCOM6208 – новая серия управляемых Ethernet-коммутаторов от MAIWE

Компания MAIWE из г. Ухань (Китай) представила обновление популярной серии 8-портовых управляемых коммутаторов на DIN-рейку. Серия MISCOM6208 является дальнейшим развитием серии MIEN6208 и представляет собой типовое решение для построения промышленных Ethernet-сетей, которое можно встретить в большом количестве проектов. Серия управляемых коммутаторов MISCOM6208 построена на новой аппаратной платформе и подходит для решения самых различных задач. Из отличительных особенностей можно отметить поддержку нескольких протоколов резервирования STP/RSTP, ERPS, MW-ring (< 20 мс), а также возможность удалённого взаимодействия с коммутатором по протоколам SNMP V1/V2/V3, SSH, HTTPS. Серия MISCOM6208 отличается наличием большого числа конфигураций коммутатора, которая позволяет выбрать тип портов, исходя из требуемых задач. Диапазон рабочих температур для MISCOM6208 –40...+85°C, степень защиты IP 40. Новая серия также доступна с различными вариантами напряжений питания либо резервированный модуль питания с входным 9...60 В (DC) либо 85...264 В (AC)/110~370 В (DC). На продукцию серии MISCOM6208 MAIWE предоставляется официальная гарантия 5 лет. ●

Все на борт! Панели Weintek серии cMT X в судостроении

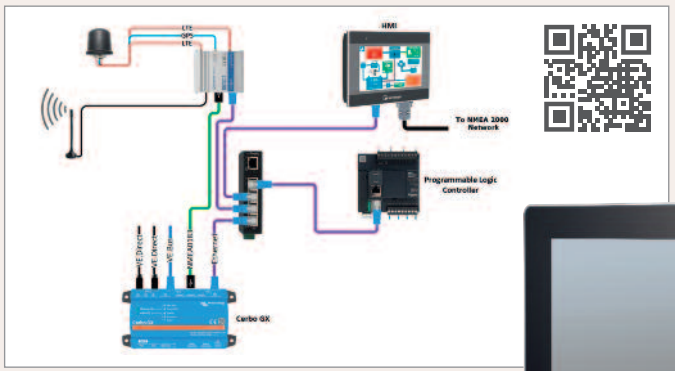


Схема бортовой системы Ortomate

cMT3092X – панель из «продвинутой» линейки серии cMT X

Строить экологически чистые лодки, которые значительно уменьшают «углеродный след» и обеспечивают более тихое, чистое и естественное плавание для своих владельцев – это основная цель компании Ortomarine, производителя электрических и гибридных судов. Основатель и владелец компании Роб Хаудл поделился своим опытом и рассказал, почему основным устройством ЧМИ для своих лодок он выбрал именно Weintek.

Роб имеет более чем 30-летний опыт работы в области промышленной автоматизации, и это в сочетании с желанием привнести новые и инновационные идеи в создание современных и экологичных судов позволило ему реализовать свои давние мечты. Долгое время работая в нефтегазовой промышленности, где традиционные подходы к выбору и применению оборудования в проектах в какой-то степени ограничивают разработчиков и производителей, Роб отметил для себя, насколько важно использовать то оборудование, которое не только отвечает современным техническим и программным требованиям, но и постоянно развивается и улучшается, поддерживая вновь появляющиеся веяния, будь то новые протоколы, интерфейсы и другие технологические тренды. Основываясь на своём многолетнем опыте и на том, что он абсолютно свободен в выборе оборудования для своих разработок, в качестве ЧМИ без колебаний Роб сделал выбор в пользу Weintek. При разработке своих судов компания Ortomarine использует как современные и интеллектуальные, но малоизвестные устройства – Nest и Hive, так и оборудование от всемирно признанного производителя солнечных батарей и инверторов – Victron. К тому же в морской отрасли достаточно распространено использование стандарта CAN. Учитывая применение разнородных устройств, в том числе и IoT, а следовательно, и соответствующих протоколов и интерфейсов, таких как Node Red, MQTT и т.д., Weintek панели новой флагманской серии cMT X позволили реализовать столь непростую задачу. «Стандартная» и «продвинутая» линейки панелей серии cMT X поддерживают CAN в качестве встроенного протокола, поэтому с лёгкостью могут получать данные и отображать параметры общей мощности, мощности солнечной батареи, использования энергии, состояния зарядки аккумулятора и т.д. А за счёт подключения ПЛК посредством Ethernet дополнительно отображают всю остальную бортовую систему. Ещё одним преимуществом применения ЧМИ Weintek является поддержка NMEA 2000. Это ещё один глобальный стандарт связи морского оборудования, применяемый в том числе в автомобилях и прочих промышленных приложениях для мониторинга таких параметров, как, например, частота вращения двигателя или температура выхлопных газов и т.д.

Бесплатное и удобное программное обеспечение с мощным инструментарием – EasyBuilder Pro и EasyAccess дополняет перечень факторов для использования панелей оператора Weintek.

Широкий спектр панелей – широкий выбор применения. Ведь модели серии cMT X – это не только высокопроизводительные панели с богатым коммуникационным функционалом, но и степень защиты IP66 (по передней панели), алюминиевый или пластиковый корпус, рабочая температура до –20°C и, конечно же, наличие сертификата российского морского регистра. За счёт чего вышеописанный опыт применения панелей оператора Weintek не менее актуален и для наших отечественных производителей в морской отрасли судостроения. ●

IES6300TSN – коммутатор с поддержкой TSN-технологий от 3onedata

Компания 3onedata представила новый промышленный гигабитный коммутатор IES6300TSN с возможностью работы в промышленных сетях TSN (Time-Sensitive Networking). TSN – это новый уровень технологий и стандартов, которые позволят обеспечить Ethernet-сетям минимальный и прогнозируемый уровень задержки передачи пакета данных. В основе TSN лежит группа стандартов IEEE. Новая серия устройств поддерживает такие стандарты, как планирование процесса пересылки трафика в режиме реального времени (IEEE802.1Qbv), формирование профиля передачи трафика IEEE802.1Qav и протокол точной синхронизации времени (IEEE802.1AS). При этом, кроме поддержки TSN-стандартов, имеется дополнительная поддержка таких протоколов, как PTP(1588 v2), STP/RSTP/MSTP, ERPS, 802.1Q VLAN, QoS, IGMP static/multicast, SNMPv1/v2c/v3, LLDP, Port Mirroring, RMON, DHCP и многое другое.

Коммутатор оснащён 8-гигабитными портами типа RJ45 и 2 гигабитными SFP-портами. Новинка выполнена в металлическом корпусе, предназначена для монтажа на DIN-рейку. Диапазон рабочих температур составляет –40…+75°C. Напряжение питания 9…60 В (DC). ●

Ультракомпактный встраиваемый компьютер от IEI

Компания IEI представляет встраиваемый компьютер TANGO-3010 на базе четырёхъядерного процессора Intel® Celeron J6412 семейства Elkhart Lake. Компактная, но достаточно производительная модель обеспечивает стабильный функционал в различных условиях ограниченного пространства. Новинка весом 1,35 килограмма имеет габариты 139×137×39 мм.

Устройство оснащено широким набором портов ввода/вывода, включающим 3× 2.5 Gigabit Ethernet, 2× USB 3.2, 2× USB 2.0, 1× RS-232/422/485 и 1× RS-232.

Функции беспроводной связи реализованы за счёт предустановленного модуля M.2 2230 с поддержкой Wi-Fi 6E и Bluetooth 5.2 последнего поколения без необходимости вывода внешней антенны.

Модель поддерживает подключение двух независимых дисплеев через видеовыходы HDMI, а высокая производительность системы обеспечивает декодирование видео в различных форматах с разрешением до 4K (4096×2130 точек).

TANGO-3010 поставляется с напаянным модулем оперативной памяти DDR4 8/16 Гбайт, а для хранения данных реализованы: слот M.2 2280 (с интерфейсом подключения PCIe Gen 4 [x4]) и полноразмерный отсек для накопителей размера 2,5". Оба накопителя выведены на одну сторону поверх процессорной платы и имеют лёгкий доступ под нижней крышкой компьютера.

Устройство работает под управлением операционных систем Microsoft® Windows® 10/11 и Linux.

Новый встраиваемый компьютер от IEI – это одна из самых функциональных моделей из линейки компактных встраиваемых компьютеров на базе x86 архитектуры, она гарантирует стабильный высокий функционал в различных условиях ограниченного пространства.

Компактная мобильная клавиатура с тачпадом SL-80-TP от iKey

Компания iKey представляет компактную, лёгкую и полностью герметичную мобильную клавиатуру SL-80-TP. Данное изделие имеет высокую степень устойчивости к грязи, пыли, воде в соответствии с IP65. Модель SL-80-TP оснащена полностью прорезиненным наборным полем и прочным корпусом из ABS-пластика, она может быть погружена в воду на короткое время и легко очищается от загрязнений с помощью дезинфицирующих средств.

Клавиатура имеет встроенную сенсорную панель (тачпад) и благодаря компактному дизайну идеально подходит для применений, в которых мобильность или сохранение свободного пространства имеют большое значение. Кроме того, красная светодиодная подсветка клавиатуры идеально подходит для использования её в ночное время или в местах с недостаточной освещённостью. Диапазон рабочих температур составляет от –20 до +60°C (температура хранения от –40°C), а размер корпуса всего 255×188,2×19,8 мм.

Данное устройство отлично подойдёт для применения в передвижных патрульных системах обеспечения безопасности, для мобильных информационных устройств, для складского оборудования, в пищевом производстве, в медицине и в других сферах, где необходимы надёжность и удобство управления. Уже сейчас модель доступна с кириллической или любой другой раскладкой, а также сертифицирована на соответствие ТР ТС 037/2016.

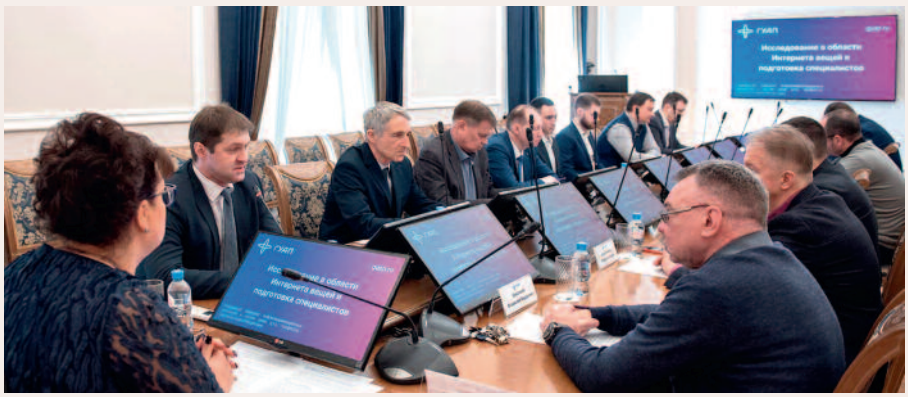
Открытие Центра компетенций по беспроводным технологиям

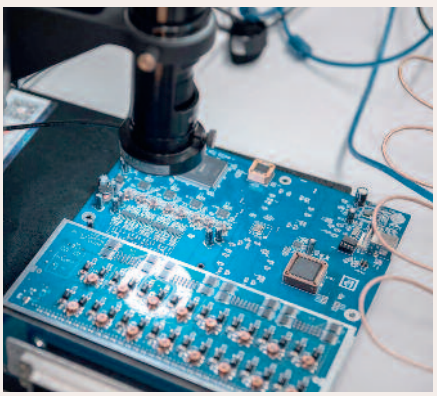
В Санкт-Петербургском государственном университете аэрокосмического приборостроения в рамках программы «Приоритет 2030» состоялось открытие Центра компетенций по беспроводным технологиям. Также был проведен круглый стол с представителями компаний – партнёров университета. Взаимодействие науки, образования и структур бизнеса, а также применение потенциала вузов для развития наукоёмких производств обсудили в ходе круглого стола.

ГУАП на встрече представляли ректор Юлия Антохина, проректор по образовательным технологиям и инновациям Владислав Шишлаков, директор Центра координации научных исследований Алексей Рабин, заведующий кафедрой инфокоммуникационных технологий и систем связи, научный руководитель нового центра Андрей Тюрликов, директор Института аэрокосмических приборов и систем Николай Майоров, директор Института радиотехники и инфокоммуникационных технологий Александр Бестугин, заведующий кафедрой радиотехнических систем Николай Поваренкин, директор Инженерной школы Сергей Солёный, директор Центра аэрокосмических исследований и разработок Валентин Оленев, научные сотрудники центра Валентин Михайлов и Никита Степанов.

Участие в диалоге приняли руководитель программы развития цифровых НИОКР ПАО «Газпром нефть» Игорь Шишлянников, директор по развитию AuroraEvernet Олег Гусев, руководитель программ разработки системных решений ПАО «Газпром нефть» Марк Бусарев, инженер по применению НТЦ «Радиотехнические устройства и системы» Виктор Вервальд.

– Новый Центр беспроводных технологий востребован с точки зрения подготовки квалифицированных кадров, реализации предметных задач, объединения научно-педагогических работников, молодых учёных. Мы рады продемонстрировать наши возможности, наработки, основательную базу.





Представим партнёрам программно-аппаратный стенд, который демонстрирует совместную работу датчиков для использования беспроводных технологий для индустриальных объектов нефтегазового сектора. Считаю, это отличный старт по расширению области работы, – открывая встречу, сказала ректор ГУАП Юлия Антохина.

Встреча дала возможность каждому представителю компаний-партнёров высказаться о тех задачах, которые есть сейчас, будь то подготовка кадров или необходимые разработки. В диалоге попытались выяснить: чем в данном случае может помочь университет, какие задачи можно решать на базе ГУАП.

Игорь Шишлянников, руководитель программы развития цифровых научно-исследовательских и опытно-конструкторских работ ПАО «Газпром нефть», рассказал о том, что компания с 2018 года реализует Стратегию цифровой трансформации. Стенд «ОКР Мультисервисная гетерогенная беспроводная IIoT-сеть» – один из артефактов реализации стратегии. Стенд решает на месторождениях важные задачи. В силу отдалённости регионов, где располагаются месторождения, сложностей с работой персонала и высокой стоимостью обустройства предприятий, лучше, чтобы работу квалифицированных специалистов выполняла техника. В этом случае беспроводные технологии автономно решают задачи.

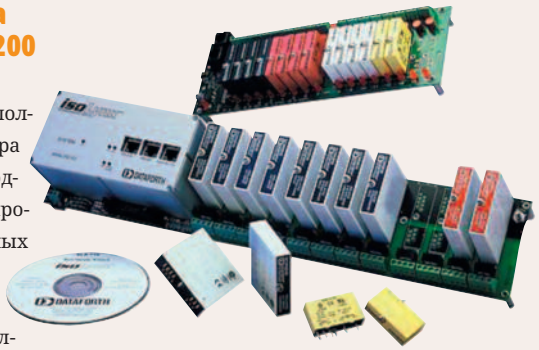
Руководитель программы развития цифровых НИОКР обратился к ГУАП с тем, что предприятию нужны специалисты в области информационной безопасности. В рамках направления по автоматизации важны специалисты по поиску датчиков нового поколения, сбору и анализу данных с уже имеющихся датчиков, работе с интеллектуальными системами управления. Игорь Шишлянников рассказал, что нефтяная компания взаимодействует со студентами ГУАП с третьего курса. Большое количество работы над стендом выполнили студенты Санкт-Петербургского государственного университета аэрокосмического приборостроения. Шишлянников пояснил, что предприятие готовит обширную программу стажировок, поэтому у студентов ГУАП будет возможность решать практические задачи.

По словам научного руководителя Центра компетенций по беспроводным технологиям, заведующего кафедрой инфокоммуникационных технологий и систем связи Андрея Тюрликова, основной задачей нового Центра станет использование исследований ГУАП при организации передачи данных в системах Интернета вещей. Одной из задач Центра также является обеспечение проектно-ориентированного обучения по направлению подготовки «Инфокоммуникационные технологии и системы связи».

Во время открытия Центра были продемонстрированы результаты проекта, выполненного по заказу ПАО «Газпром нефть». У компании на месторождениях находятся установки с большим количеством датчиков с использованием традиционных проводных систем. В ГУАП разработали программно-аппаратный стенд, демонстрирующий совместную работу датчиков с использованием технологий LoRa, NB-IoT, RFID, LTE, Wi-Fi 6 и отечественные системы радиочастотной идентификации на основе технологии поверхностных акустических волн. Стенд можно адаптировать к условиям конкретного объекта и ускорить внедрение беспроводных технологий на объекты нефтегазового сектора. Кроме того, была продемонстрирована работа методик испытаний оборудования LoRaWAN, предоставленных партнёром AuroraEvernet. Компания обозначила проблему возникновения сильных побочных излучений в определённых условиях использования. В ГУАП разработан программно-аппаратный комплекс для проведения испытаний радио-тракта, методика измерения потребления тракта питания, антенн и протокола беспроводной передачи данных LoRaWAN. Комплекс можно использовать для развития компетенций стандартизации устройств и ускорить внедрение российских протоколов беспроводных технологий Интернета вещей.

Оборудование нового Центра компетенций по беспроводным технологиям позволит не только проводить научные исследования и опытно-конструкторские разработки, но и проводить тестирование выпускаемых в РФ устройств и программного обеспечения систем Интернета вещей.

Интеллектуальная система сбора данных isoLynx® SLX200 от компании Dataforth



isoLynx® SLX200 – это модульная и полностью изолированная система сбора данных, обеспечивающая превосходную надёжность и точность для широкого спектра высокопроизводительных промышленных приложений, в том числе применяющиеся в тяжёлых условиях эксплуатации. Система полностью сертифицирована организацией Modbus-IDA и совместима со стандартом OPC, что позволяет легко интегрировать её в существующие сети Modbus, а благодаря возможности взаимодействия с более чем 650 различными модулями аналогового ввода/вывода серии SCM5B система isoLynx SLX200 предлагает максимальную гибкость для таких приложений автоматизации производства, как управление процессами, проведение испытаний и измерений, управление машинами и оборудованием, а также сбора и передачи данных.

Надёжность системы, помимо защиты, обеспечиваемой резервированием за счёт наличия в соответствующих моделях двух независимых Ethernet-портов, определяется показателем MTBF (среднее время наработки на отказ), превышающим 500 000 часов, а также возможностью работы в диапазоне температур от –40 до +85°C.

Гибкая модульная конструкция SLX200 сочетает в себе 6- или 12-канальную базовую систему ввода/вывода и дополнительные 8- или 16-канальные объединительные платы расширения, которые можно монтировать либо на панель, либо на DIN-рейку. В свою очередь, одна базовая система может обслуживать до 60 каналов аналогового ввода/вывода (серия модулей SCM5B) и 128 каналов дискретного ввода/вывода (серия модулей SCMD). Контроллер системы содержит мощный высокоскоростной RISC-процессор, аналого-цифровые и цифро-аналоговые подсистемы, интерфейс связи, соответствующую память и светодиоды состояния. Аналого-цифровая система построена на основе 16-битного преобразователя и может преобразовывать максимум 60-канальную конфигурацию за 17 мс. Цифро-аналоговый преобразователь также является 16-разрядным устройством и может записывать максимум 60-канальную конфигурацию за 33 мс.

Доступность более чем 650 стандартных и специализированных модулей ввода/вывода позволяет системе SLX200 взаимодействовать с широким спектром используемых сигналов, включая милливольты, вольты, миллиамперы, амперы, линеаризованные и нелинеаризованные термопары, термодатчики, потенциометр, тензодатчик, выход переменного тока к истинному среднеквадратичному значению, частота и т.д. ●

BioSmart Quasar 7 – новый терминал для бимодальной биометрической идентификации

Компания BioSmart на прошедшей выставке MIPS представила новую модель бимодального биометрического терминала Quasar 7. Терминал BioSmart Quasar 7 был спроектирован и создан на основе запросов рынка. Он сочетает в одном устройстве лучшие технические решения.

- Идентификация по лицу
- Идентификация по RFID-картам
- Идентификация по рисунку вен ладони (опционально может быть встроен сканер рисунка вен ладони)
- Распознавание лиц в медицинской маске и контроль средств индивидуальной защиты на сотруднике

BioSmart Quasar 7 защищён от фальсификации на аппаратном и программном уровне: это оптический комплекс из трёх камер (RGB, IR, 3D) и система liveness detection. Помимо собственного встроенного алгоритма, имеется возможность идентификации сотрудников при помощи различных сторонних сервисов (3DiVi, NtechLab, РТЛабс и CVS). Также благодаря адаптивной подсветке терминал может распознавать человека при плохой освещённости.

Корпус BioSmart Quasar 7 возможно изготовить в соответствии с цветовой гаммой бренда или интерьера помещения по вашему запросу.

Полные технические характеристики представлены ниже.

- Биометрический идентификатор: лицо и рисунок вен ладони (опционально)
- Наличие встроенного считывателя RFID-меток
- Наличие датчика вскрытия задней крышки
- Наличие защиты от попыток фальсификации биометрических данных лица (антиспуфинг)
- Максимальное количество пользователей при работе в режиме идентификации (1:N): 10 000
- Максимальное количество пользователей при работе в режиме верификации (1:1): 100 000
- Максимальное количество биометрических шаблонов лица: 100 000
- Максимальное количество событий, хранимых на терминале: 100 000
- Вероятность ошибочного предоставления доступа по биометрическим данным, FAR*: 10^{-6} – 10^{-8}
- Модуль камер: 3D-камера с RGB-сенсором 5 Мп, Ir-сенсором 1 Мп и с инфракрасным проектором
- Процессор: Rockchip RK3399
- GPU: Mali-T864 GPU
- Память: 4 Гбайт RAM, 16 Гбайт Flash
- Интерфейс взаимодействия с управляющим компьютером: Ethernet (100BASE-TX / 10BASE-Te IEEE 802.3), Wi-Fi (IEEE 802.11)
- Интерфейсы связи со сторонними устройствами: USB 2.0, Wiegand, RS-485
- Поддерживаемые форматы Wiegand: 26/32/34/37/40/42/48/50/56/58/64
- Количество интерфейсов Wiegand: 1 (двунаправленный Wiegand-интерфейс)
- Количество дискретных входов/выходов: 2/3
- Максимальное напряжение, подаваемое на дискретный вход: 12 В
- Тип дискретных выходов: открытый коллектор
- Максимальное коммутируемое напряжение на дискретном выходе: 14 В
- Максимальный коммутируемый ток через дискретный выход: 50 мА ●