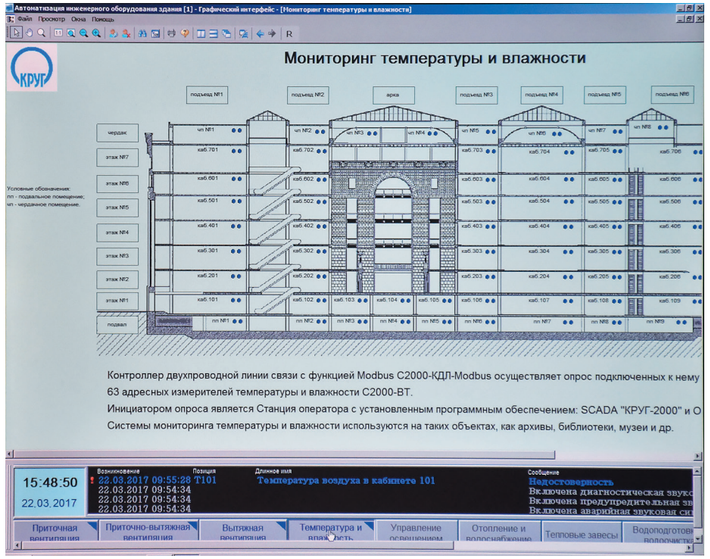
КОНВЕРГЕНТНЫЕ РЕШЕНИЯ НА СОВРЕМЕННЫХ ОБЪЕКТАХ

Текст: **ВЛАДИМИР МАКСИМЕНКО**



Мониторинг температуры и влажности

Конвергенция систем безопасности и систем автоматизации зданий – активно развивающаяся сегодня тема, о чем убедительно свидетельствуют материалы ведущих международных мероприятий в этой области [1, 2]. В России долгое время это направление развивалось большей частью обособленно, хотя ведущие отечественные специалисты постоянно отмечали необходимость комплексного подхода к проектированию современных объектов и неразрывную связь вопросов безопасности и автоматизации зданий [3]. Назревшая ситуация была связана прежде всего с ограничениями, накладываемыми нормативными документами в области безопасности, и низким уровнем развития технических решений. Между тем на современных сложных объектах, особенно в высотном строительстве, повышаются требования не только к вышеперечисленным областям, но и к качеству окружающей среды, приводя к необходимости использования большего объема инженерного оборудования как в системах безопасности, так и в управлении инженерным оборудованием зданий. При этом оказывается, что используемое оборудование зачастую дублирует друг друга, выполняя равноценные функции. Подобные негативные явления приводят не только к увеличению финансовой составляющей проекта, но и к снижению надежности, т.к. вероятность выхода из строя на большем количестве оборудования выше, чем на меньшем. Попытки выхода из этой ситуации нашли свое яркое отражение в материалах первого Intersec Форума в 2016 году. Здесь впервые проектирование и создание всех аспектов безопасности на объекте, управление инженерным оборудованием, а также их развитие и функционирование на всем жизненном цикле рассматривались как единая стратегическая задача, направленная на оптимизацию и обеспечение высоких качественных показателей в течение всего времени эксплуатации. Предлагалось рассмотреть любой объект как проект, опирающийся на 20 основных технологий и использующий одну сеть, один язык и пять сценариев, детально проработанных и охватывающих отработку большинства жизненных ситуаций. Эти сценарии, условно названные «Пожар», «Доступ», «Встреча», «Шторм» и «Взлом», решают вопросы управления большинством штатных и нештатных ситуаций в здании и демонстрировались под девизом «Цифровой. Индивидуальный. Сетевой». Решения, принимаемые на этапе планирования, просчитываются так, чтобы обеспечить их актуальность и отсутствие существенных изменений на всем жизненном цикле объекта. Таким образом достигается оптимизация предварительных инвестиций, производительности, устойчивости, сохраняется целостность стратегии, использующей междисциплинарный подход и ориентацию проекта на будущее.

Бурное развитие систем автоматизации зданий в последнее время и переход к широкому использованию открытых технологий, таких как KNX, LonWorks, BacNet и ModBus, а также IP-технологий, привели к появлению технических решений, позволяющих на новом уровне реализовать задачу сближения (конвергенции) систем безопасности и систем автоматизации зданий. В рамках упомянутого Intersec Форума и его продолжения в последующие годы основной акцент делался на широком использовании IP-технологий. Этот протокол также служит платформой, которая позволяет оборудование систем безопасности легко интегрировать в системы управления зданием. Предполагается глубокая межсистемная и профессиональная конвергенция, обеспечивающая высокую устойчивость и экономическую эффективность проекта. Появляется возможность получить полный, многофункциональный обзор в одном приложении, сформированный на базе различных технологий, функционирующих в цифровой сети. Контроль доступа может передавать данные, применяемые в регулировании освещения, которое, в свою очередь, должно включаться по расписанию или с применением световых сцен. Данные о температуре в помещении, поступающие от пожарной сигнализации, в ряде случаев могут быть использованы для комнатной автоматизации, например, для управления климатом или жалюзи. А оборудование противопожарной сигнализации может быть связано с контролем отопления, кондиционирования и вентиляции.

Вместе с тем особенно остро встала проблема кибербезопасности. Ведущие специалисты европейских компаний большое внимание уделили цифровизации. На Форуме 2018 года основное внимание уделялось вопросам неразрывной связи обеспечения защиты информации, используемой в сети современного здания, и применения для этого соответствующих стандартов. Это ярко отразилось в девизе мероприятия «Оцифровка в основе безопасности данных!». Реализация глобальной задачи перехода к цифровому формату обмена данными столкнулась с необходимостью обеспечения безопасности цифрового управления. По словам представителя ZVEI, «Именно собранные и обработанные данные создают цифровые технологии для здания на основе защиты информации». Президент Федерального ведомства по информационной безопасности Германии (BSI) сказал о новом понимании безопасности данных и информации, а также необходимости дальнейшей разработки новых стандартов, требуемых для эффективной работы как компаний, так и общества в целом: «Мы должны по умолчанию реализовать реальное и рациональное управление рисками для кибербезопасности. Это является предпосылкой для оцифровки и должно быть вопросом для руководства».

Отрадно отметить, что конвергентные решения представлены и на отечественном рынке.

Одной из проблем внедрения подобных новейших технологий является то, что системы безопасности используют закрытые протоколы обмена данными, в то время как системы автоматизации зданий, как правило, строятся на открытых протоколах (технологиях). Решение этой проблемы вылилось в разработку и выпуск устройств, которые условно можно отнести к трем направлениям:

– создание преобразователей протоколов позволяет обеспечить доступ к данным системами безопасности. Речь идет о данных, получаемых системами безопасности. Информация содержит в себе состояние температурного режима, присутствие людей в помещении, открытие и закрытие дверей и окон, которые можно использовать для целей управления инженерным оборудованием [4];
– устройства, работающие в закрытом и открытом протоколе;
– линейки приборов, поддерживающие закрытые и открытые протоколы.

Выполненные в рамках этих требований контроллеры НВП «Болид» М3000-Т и С2000-Т позволяют работать с такими SCADA-системами, как «Круг-2000», «Мастер-СКАДА 4Д» компании ИнСат и рядом других, что было успешно продемонстрировано на выставках МИПС-2017 и HighTechBuilding-2018.

Новое развитие темы конвергентных решений получено на базе оборудования М3000-Т с «Мастер-СКАДА 4Д» компании ИнСат на борту (в оперативной памяти прибора), М2000-4ДА и С2000-КДЛ ModBus, в которой открытый протокол ModBus RTU стал уже основным средством коммуникации. Эта линейка позволяет, в частности, использовать информацию о состоянии элементов систем безопасности для управления инженерным оборудованием объекта.

Одним из первых проектов, реализованных на базе контроллера М3000-Т, был проект управления освещением в автоматизированном складском комплексе с использованием протокола DALI. В этом решении информация от датчиков движения охранной сигнализации использовалась для управления освещением в определенных зонах склада, т.е. появление и движение людей в соответствующих зонах склада вызывали срабатывание датчиков охранной сигнализации, что использовалось для включения освещения в этих зонах.

На выставке HighTechBuilding-2018 совместно с компанией iRidium mobile была представлена интеграция с ОПС на базе оборудования НВП «Болид», традиционно применяющегося в системах безопасности. Данные конвертируются с помощью преобразователя С2000-ПП в открытый протокол ModBus, а ПО iRidium обеспечивает удобный интерфейс, гибко настраиваемый под пожелания заказчика и позволяющий развернуть его на любых мобильных средствах – планшетах, смартфонах и т.п. Теперь пользователь может производить постановку и снятие с охраны прямо со своего мобильного устройства, а в случае инцидента получать подробные уведомления на телефон с указанием источника сработки.

Примеры интерфейсов этого проекта приведены на рис. 1 и рис. 2.

В заключение интересно привести пример одного из недавних конвергентных решений, реализованных на описанных выше принципах:

Гостиничный комплекс "Park Inn Izhevsk" – десятиэтажный комплекс общей площадью 11,7 тыс. кв. м, рассчитан на 161 номер,

который является лучшим в системе отелей Park Inn по признанию The Rezidor Hotel Group. На объекте представлена интегрированная система безопасности, основой которой является АРМ «Орион Про» (НВП «Болид»). В единой взаимосвязи работают системы охранно-пожарной сигнализации, пожаротушения, речевого оповещения людей о пожаре IV типа, видеонаблюдения, дымоудаления, вентиляции, автоматизации пожарных и дренажных насосов, лифтов. В проекте использовано 618 единиц оборудования и программного обеспечения. ■

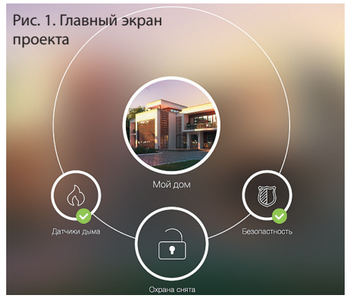


Рис. 1. Главный экран проекта

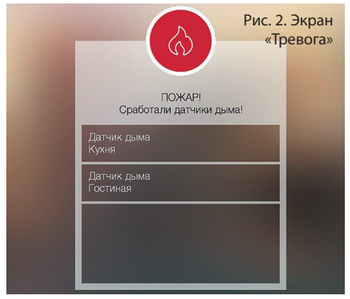


Рис. 2. Экран «Тревога»

СПИСОК ЛИТЕРАТУРЫ:

1. «Алгоритм безопасности», № 4, 2016. Конвергенция систем безопасности и систем автоматизации зданий.
2. «Алгоритм безопасности», № 2, 2018. СИСТЕМЫ БЕЗОПАСНОСТИ И ЦИФРОВОЕ УПРАВЛЕНИЕ.
3. Сборник трудов Международной научно-практической конференции «Охрана, безопасность, связь – 2015», Воронеж. – 2015. – Часть 1. Комплексная концепция функционирования инженерных систем, систем безопасности и управления как основа обеспечения устойчивости объекта.
4. F+S: технологии безопасности и противопожарной защиты, № 3, 2012. Новый способ интеграции ИСО «Орион» с внешними системами.
5. Алгоритм безопасности, № 6, 2012. Контроллер С2000-Т на службе «Умного дома».