КОЛОНКА РЕДАКТОРА

Архитектурные вопросы распределенных СКУД

Протяженные периметры и территориально распределенные СКУД – особенность крупных предприятий со сложной, географически разнесенной структурой, включающей в себя центральный офис, филиалы в одном или различных городах, подразделения, отделы. При построении СКУД на подобных предприятиях:

- необходимо в режиме реального времени управлять и получать информацию от множества устройств одного или разных производителей;
- важно обеспечивать высокую скорость, надежность функционирования и удобство использования системы.

Для предприятий с протяженным периметром или территориально распределенной структурой существует множество вариантов организации СКУД. Среди этого множества можно выделить некоторые общие для всех задачи.

Программная часть СКУД

1. Представление организационной структуры предприятия: поддержка зон доступа подразделений и головного офиса и др.
2. Поддержка системы отчетности в разрезе зон доступа и временных ограничений.
3. Синхронизация баз данных между центральным сервером и промежуточными серверами, контроллерами.

Аппаратная часть СКУД

Как правило, имеет распределенную архитектуру, включающую в себя множество контроллеров (серверов), с центральным сервером, каждый из которых отвечает за свою часть проходных и зон доступа в пределах одного здания или группы зданий. На каждом из таких контроллеров (серверов), кроме центрального, хранится БД сотрудников, имеющих доступ к соответствующим данному контроллеру (серверу), зонам. На центральном сервере хранится общая БД всех сотрудников. С некоторой периодичностью происходит синхронизация данных между центральным сервером и контроллерами (серверами).

Наиболее популярным в локальных сетях контроллеров является интерфейс RS-485, менее известный – CAN. Обычно данные между контроллерами (серверами) передаются по выделенной сети Ethernet, не загружая общую локальную сеть предприятия.

Шамиль Оцоков
Редактор рубрики "Управление идентификацией", руководитель разработки программного обеспечения компании "Сонда Эксперт", д.т.н.

Варианты построения сети для системы доступа

Выбор каналов коммуникации в соответствии с задачами и требованиями заказчика

Системы контроля и управления доступом имеют широкую сферу применения – не только в области обеспечения безопасности, но и везде, где требуется контроль перемещения или просто учета различных объектов (предметов, товаров, транспорта, людей). СКУД может также быть компонентом интегрированной системы безопасности (ИСБ) со сложной структурой сети. Поэтому выбор структуры построения сети и каналов коммуникации играет немаловажную роль при создании (проектировании) систем доступа на различных объектах

Александр Крахмалев
Заместитель генерального директора ГК "СИГМА", к.т.н.

СКУД являются автоматизированными информационными системами и строятся на основе иерархической сетевой структуры, в которую на верхнем уровне управления входят компьютерные сети, а ниже локальные сети специальных устройств – контроллеров, которые, в свою очередь, могут иметь свою сетевую структуру сбора информации со считывателей.

К СКУД применимо определение ГОСТ 34.003 "Автоматизированные системы. Термины и определения": "Автоматизированная система; АС: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций". То есть СКУД – человеко-машинная система, поэтому для ее эффективности нужно учитывать не только технические факторы и характеристики, но и все аспекты взаимодействия с человеком: пользователями, персоналом по эксплуатации, обслуживанию.

Вопросы, решаемые на этапе проектирования

Несмотря на общие принципы построения, использование СКУД в различных областях применения предполагает решение разных задач. Из этого следует, что требования к СКУД могут существенно различаться. Для создания эффективного и качественного решения необходимо прежде всего четко и правильно сформулировать задачи, которые она должна решать, и определить соответствующие этим задачам требования, в том числе к структуре построения сети и выбору каналов коммуникации.

Эти вопросы решаются в процессе проектирования СКУД на этапе разработки ТЗ, так как именно на этапе проектирования закладываются все необходимые качественные характеристики.

Каждый объект, на котором создается СКУД, является уникальным, и каждая проектируемая система представляет собой продукцию единичного производства, создаваемую заново для каждого конкретного объекта. Важнейший вопрос при проектировании – выбор технических и программных средств, из которых будет создаваться система и которые представляют продукцию серийного производства, специально предназначенную для построения СКУД.

Хочу обратить внимание специалистов, что когда мы обсуждаем параметры и технические характеристики системы, в частности СКУД, то необходимо уточнение, что именно в каждом случае подразумевается под этим понятием:

- СКУД – комплекс технических средств – продукт серийного производства.
- СКУД – проектируемая система как продукт единичного производства для каждого конкретного объекта.

Комплекс технических средств, специально предназначенных для построения СКУД, как правило, предлагается одним производителем (разработчиком) и может включать в себя достаточно полный набор оборудования для построения СКУД на каком-либо объекте с учетом специфики решаемых задач. Преимущества такого решения – внутренняя совместимость оборудования и программных продуктов.

СКУД – проектируемая система в любом случае представляет собой сложное техническое решение, и при его создании приходится использовать различное оборудование – как по функциональному назначению, так и оборудование разных производителей. При этом всегда встает задача совместимости, которая во многом связана с выбором структуры построения сети и каналов коммуникации. Причем она включает в себя две составляющие:

1) задача обеспечения взаимодействия оборудования компонентов СКУД в составе единой системы;

2) совместимость оборудования разных производителей.

Компоненты СКУД и их совместимость

Современный рынок СКУД сложился таким образом, что обычно основные компоненты СКУД (идентификаторы, считыватели, контроллеры, ПО АРМ верхнего уровня, исполнительные устройства, и различные дополнительные аксессуары) разрабатываются и производятся разными предприятиями, специализирующимися на каком-либо конкретном типе изделий. И это правильно, так как специализация позволяет добиться максимальных качественных характеристик и оптимальных технико-экономических показателей.

Однако при этом проблема совместимости оборудования разных производителей выходит на первое место при проектировании СКУД. Ее оптимальным решением может быть использование стандартов на всех уровнях взаимодействия компонентов.

Как было сказано выше, СКУД – автоматизированная информационная система, построенная на иерархической сетевой структуре. Рассматривая наиболее общую структуру СКУД, можно выделить в ней основные компоненты:

- считыватели, расположенные на контролируемой территории (зоне), осуществляющие считывание идентификационных признаков с объектов контроля;
- контроллеры, обеспечивающие работу считывателей, управление исполнительными устройствами, обмен информационных потоков в СКУД;
- исполнительные устройства (замки, турникеты, шлюзы и т.д.);
- компьютеры АРМ ПО верхнего уровня управления СКУД.

Верхний уровень сетевой иерархии СКУД – локальная вычислительная сеть (ЛВС) компьютеров АРМ ПО управления СКУД. На этом уровне применяется стандартное компьютерное и сетевое оборудование, используются соответствующие каналы и протоколы передачи информации. Вопросы взаимодействия здесь решены в достаточной мере на основе многочисленных ИТ-стандартов. Необходимо только учитывать, что СКУД как система безопасности должна быть надежно защищена как от несанкционированного вмешательства, так и от сбоев, неисправностей, проблем с электропитанием и т.д.

Наиболее развитая сетевая структура, специфическая для современных СКУД, – это локальная сеть контроллеров. Массовую распространенность получили контроллеры, обеспечивающие работу 2–4 точек доступа. Для больших объектов количество точек доступа может исчисляться десятками, сотнями и более, соответственно, сеть контроллеров представляет собой наиболее сложный и развитый уровень.

Интерфейсы передачи данных в СКУД

В локальных сетях контроллеров самым распространенным является стандартный интерфейс RS-485, разработанный в 1983 г. Он служит для создания связи между устройствами и не является протоколом, а только определяет базовые правила и физический канал для обмена данными, позволяя передавать последовательные сообщения, причем их содержимое полностью определяется разработчиком. О характеристиках, особенностях, недостатках, структурах этого интерфейса написано множество статей, имеется большое количество информационных материалов и документации, и думаю, что нет необходимости обсуждать эту тему.

При проектировании СКУД на первое место выходит проблема совместимости оборудования разных производителей

Значительно реже в СКУД применяется не менее известный интерфейс CAN (Control Area Network – локальная сеть контроллеров). Это последовательный протокол связи с эффективной поддержкой распределения контроля в реальном времени и высоким уровнем помехоустойчивости. Основное назначение – организация передачи информации в сложных условиях, таких как среды с высоким уровнем различного рода помех. Локальная сеть CAN была разработана в 1980-х гг. и первоначально была предназначена для автомобильной промышленности. В настоящее время CAN используется во многих прикладных областях, таких как автоматизация промышленного производства, медицинское оборудование, транспорт и т.д. В отличие от RS-485 CAN определяет не только физическую среду связи, но и протокол передачи данных (сообщений).

Здесь также хочу напомнить об интерфейсах в системах автоматизации управления инженерным оборудованием зданий и сооружений, которые часто называют системами интеллектуальных зданий.

Интерфейсы систем интеллектуальных зданий

Это направление широко распространено за рубежом и активно применяется в России. Интерфейсы систем интеллектуальных зданий довольно стандартизированы – некоторые приняты в качестве международных и национальных стандартов, а также стандартов ассоциаций компаний – производителей соответствующего оборудования. Как правило, в них имеются спецификации для реализации подсистем безопасности, в том числе и СКУД.

Наиболее распространенные интерфейсы систем интеллектуальных зданий:

LonWorks

Промышленный стандарт организации управляющих сетей, широко используется для построения распределенных систем автоматизации зданий и промышленных предприятий, транспортных сетей. Несомненными преимуществами LonWorks являются независимость от протокола физического уровня, свобода в выборе сетевых топологий, алгоритм разрешения коллизий. LonWorks – признанный международный стандарт для построения систем автоматизации зданий, позволяющий связать в единое целое системы жизнеобеспечения, безопасности, электроснабжения, построенные на оборудовании различных производителей.

Протокол BACnet

BACnet (Building Automation and Control Networks – сети автоматизации и управления зданий) был принят в 1995 г. BACnet представляет собой специализированный протокол передачи данных для автоматизации зданий и управляющих сетей.

KNX/EIB

Открытый протокол для управления инженерным оборудованием зданий и сооружений. Стандарт KNX принят в качестве международного (ISO/IEC 14543-3), европейского (CENELEC EN 50090 и CEN EN 13321-1) и получил распространение во многих странах. Стандартизация устройств KNX позволяет использовать совместимые продукты различных производителей в составе единой системы, в том числе компоненты систем безопасности.

Более подробно ознакомиться с этими стандартами систем "интеллектуального" здания можно также в многочисленных материалах интернет-публикаций.

RS-485, CAN, а также стандарты систем интеллектуального здания разработаны давно, однако довольно широко применяются в настоящее время. Это доказывает их надежность, а наличие стандартизации обеспечивает их широкое применение. Очевидно, что они будут весьма востребованы и в ближайшей перспективе

Знаковые шаги на пути стандартизации IP-СКУД

Особую роль в современном развитии СКУД играет внедрение IP-технологий и дальнейшее развитие на основе IP и интеграции систем без-

Широкое внедрение ИТ-технологий в СКУД позволяет судить о перспективности этого направления. Стандартизация обеспечивает появление инновационных решений в СКУД

опасности – в особенности СКУД и систем видеонаблюдения. Это подтверждается активным внедрением IP-решений как за рубежом, так и в России. Тенденция понятна, так как сами IP-технологии развиваются стремительными темпами. Не менее активно совершенствуется и стандартизация в этой области, что отразилось на деятельности международного комитета по стандартизации в области систем безопасности МЭК ТК 79 Alarm and Electronic Security Systems ("Электронные системы тревожной сигнализации"). В комитете ТК 79 с 2007 г. активно ведется работа над стандартизацией СКУД при участии российских специалистов. В 2010 г. в ТК 79 был принят новый подход в стандартизации, который связан как раз с внедрением IP-технологий в СКУД и СОТ и проявился в активном влиянии международных промышленных ассоциаций ONVIF (Open Network Video Interoperability Forum) и PSIA (Physical Security Interoperability Alliance). Эти ассоциации, начинавшие работу с создания своих корпоративных стандартов в области IP-видеонаблюдения, в последние годы предлагают также свои стандарты и в области СКУД. Приведу для информации перечень международных стандартов на СКУД.

Базовые стандарты

- IEC 60839-11-1 Ed.1: Alarm and Electronic Security Systems – Part 11-1: Electronic Access Control Systems – System and Components Requirements ("Электронные системы контроля доступа. Требования к системам и компонентам").
- IEC 60839-11-2 Ed. 1.0 Alarm and Electronic Security Systems – Part 11-2: Electronic Access Control Systems – Application guidelines ("Электронные системы контроля доступа. Руководство по применению").

Стандарты, касающиеся применения IP-технологий в СКУД

- IEC 60839-11-31: SOAP Base Protocol (ONVIF Core Specs) (МЭК 60839-11-31 SOAP Базовый протокол (на базе спецификаций ONVIF)).
- IEC 60839-11-32: SOAP EACS Commands – IP (МЭК 60839-11-32 SOAP EACS команды – IP).
- IEC 60839-11-41: REST Base Protocol (PSIA Core Specs) (МЭК 60839-11-41 REST Базовый протокол (на базе спецификаций PSIA)).
- IEC 60839-11-42: REST EACS Commands (МЭК 60839-11-42 REST EACS команды).
- IEC 60839-11-33: Electronic Access Control Systems – Access Control Configuration for IP Interoperability Based on Web Services ("Электронные системы контроля доступа. Конфигурация управления доступом для IP. Функциональная совместимость на основе Web-служб").
- IEC 60839-11-5: Alarm and Electronic Security Systems – Part 11-5: Electronic Access Control Systems – Open Supervised Device Protocol (OSDP) ("Электронные системы контроля доступа. Открытый протокол контроля устройств").
- PNW: Open Source Protocol for Using a Mobile Device as an Access Control Credential. (Предложение новой темы: протокол с открытым исходным кодом для использования мобильного устройства в качестве устройства идентификации для контроля доступа).

Некоторые из данных стандартов находятся еще на стадии проектов или предложений.

Выводы

1. Наиболее развитая сетевая структура, специфическая для современных СКУД, – это локальная сеть контроллеров СКУД.
2. Применяемые здесь интерфейсы RS-485, CAN, а также интерфейсы систем интеллектуальных зданий разработаны более 10 лет назад, однако широко распространены и в настоящее время, что доказывает их надежность и функциональность. Очевидно, что в ближайшей перспективе они будут востребованы.
3. Современные контроллеры СКУД разрабатываются на новых электронных компонентах и в большинстве случаев имеют встроенный IP-интерфейс, что дает возможность подключать их непосредственно к сетям Ethernet/Internet. Это широкое внедрение ИТ-технологий в область СКУД и систем безопасности в целом позволяет судить о безусловной перспективности этого направления, тем более что стандартизация в ИТ-отрасли активно развивается. Соответственно, это обеспечивает появление инновационных решений в области СКУД. ■

Ваше мнение и вопросы по статье направляйте на ss@groteck.ru