

УМНОЕ СЕРДЦЕ ОХРАННОГО КОМПЛЕКСА

СЕТЕВОЙ КОМПЛЕКС ВИДЕОМОНИТОРИНГА, КАК ИНТЕГРАЦИОННОЕ ЯДРО ОХРАННОЙ СИСТЕМЫ ОБЪЕКТА

А. Данг
представитель компании SYAC (Россия)

Уходят в небытие времена, когда один производитель делал все: от пожарных датчиков и жестких дисков до видеокамер и комплексных систем видеомониторинга – конкуренция заставила производителей сегментировать рынок и сконцентрироваться на определенных сегментах. В то же время задача монтажных компаний становится все более сложной и комплексной, а необходимость в согласовании оборудования различных производителей становится определяющей. Элементы охранных систем становятся все более изощренными, "заточенными" под конкретные задачи, и пользователь хочет иметь все эти многочисленные компоненты в едином комплексе, а производители все более концентрируются лишь на определенных рынках.

XXI век – это время комплексных подходов, и конечный заказчик сегодня хочет увидеть полное решение, функционирующее в едином комплексе. Клиент нацелен на обеспечение своей личной безопасности или безопасности стационарного и мобильного объекта и для этого прибегает к самым разнообразным средствам. Вопрос объединения всех этих средств в единый комплекс и есть вопрос интеграции.

Перед специалистами компании SYAC, как компании-производителя, а также перед нашими партнерами, осуществляющие продажи оборудования по всему миру, в том числе и в России, всегда ставились самые разнообразные и амбициозные задачи, однако даже самые сложные проекты сводились чаще всего к следующим подзадачам:

- Клиент решал усовершенствовать свой охранный комплекс, и для этих целей производил приобретение самых современных устройств на рынке, однако он не хотел избавляться от многочисленной охранной инфраструктуры, которая уже успешно функционировала на объекте.
- Клиента интересовало сведение всей охранной инфраструктуры (камер, охранных датчиков, системы контроля доступа, мониторов, джойстиков) в единый комплекс с минимальными затратами.
- Заказчику необходимо было решить конкретную задачу (например, построение охранного комплекса в банке), что накладывало существенное ограничение на использование интерфейса стандартного программного обеспечения, и существовала потребность в единой работе всей охранной системы в комплексе.

С подобными проблемами сталкивался любой инсталлятор, имеющий существенный опыт на рынке. Это имеет некоторое сходство с задачей приобретения новой современной мебели в дом, где уже расположено множество разнообразных предметов интерьера, и необходимо проявить истинный профессионализм, чтобы удовлетворить желания заказчика. Всем этим задачам и служит методика интеграции охранных комплексов.

Процесс организации систем безопасности может идти несколькими базовыми путями: аппаратная интеграция и программная интеграция. Данные два подхода решают принципиально различные задачи и служат различным целям. Аппаратная интеграция: работа с различными внешними датчиками, устройствами, камерами. Программная интеграция: работа в едином интерфейсе, программное взаимодействие между различными программными продуктами.

Самые современные охранные комплексы должны обладать широким спектром интеграционных возможностей, чтобы обеспечить выполнение задачи. Если задаться целью и сделать краткий анализ тенденций на рынке охранных систем, то станет очевидным, что большинство производителей используют в качестве базы охранного комплекса именно его видеосегмент, как наиболее ресурсоемкий и технологичный. Успешные производители концентрируют усилия на создании платформы для конечного пользователя, которую можно использовать для решения самых различных охранных задач. Иначе говоря, для охранного комплекса система видеонаблюдения играет роль "сердца" или, точнее говоря, "мозга" системы, где производится сведение всех элементов и их анализ. Рассмотрим последовательно различные методики интеграции внешних устройств, которые выделили в качестве определяющих инженеры компании SYAC при разработке своего комплекса DigiEye. Логика интеграции одинакова и для иных производителей класса "премиум".

Поддержка протоколов камер

Степень интеграции системы, а также опыт производителя можно оценить, узнав, сколько протоколов различных PTZ устройств и купольных камер поддерживает система. Чем больше марок различных камер поддерживает устройство, тем меньше проблем возникнет у конечного заказчика, когда он столкнется с задачей интеграции. Идеальная система должна позволять работать с PTZ/Купольными контроллерами и камерами большинства мировых производителей. Например, в систему DigiEye в настоящее время интегрированы более 30 протоколов. Эту цифру можно взять за некоторый целевой показатель. Системы, поддерживающие меньшее число камер могут вызывать некоторый дискомфорт конечного пользователя в ограниченности его выбора. Для работы с различными протоколами и контроллерами используется 485 интерфейс. Это делает охранный комплекс идеальным решением для усовершенствования текущих проектов или создания новых решений интегрированных с продукцией сторонних производителей.

Управление заранее установленными позициями камеры, а также управление купольной камерой должно быть возможно не только посредством программного интерфейса, но и при помощи различных внешних устройств: джойстика или специализированной клавиатуры. Сегодня все больше производителей предлагают собственные удобные для использования устройства, поэтому вопрос по интеграции здесь стоит уже не столь остро.

Цифровые входы/выходы

Это один из ключевых элементов интеграции. Фактически все устройства класса "премиум" отвечают этим требованиям. Некоторые производители позволяют использовать внешнюю панель для подключения к тревожным входам/выходам. Цифровые входы/выходы можно использовать для связи с сенсорами, сигналами тревог, пожарными сигнализациями и иными устройствами.

Таким образом, тревожные входы могут выполнять функцию датчиков, которые по заранее заданному алгоритму могут изменять состояние системы и побуждать систему:

- Начать запись видеозображения.
- Осуществить последовательное переключение камер.



- Переместить PTZ/Купольную камеру в ту или иную предустановленную позицию.
- Обратиться на центральный пост охраны (передать изображения и состояния всех тревожных сигналов).

Допустим, был нарушен контур охраны (открыта дверь, с установленным на ней датчиком) или было разбито окно, и система, зафиксировав нарушение, будучи полностью интегрированным решением, мгновенно фиксирует видеoinформацию события и передает ее или оператору на центральный пост, или, например, пользователю на его мобильный телефон. Аналогично может выглядеть более привычная глазу "тревожная кнопка", активация которой также может вызывать по соответствующему алгоритму активацию тревожной фазы системы, то есть начало видеозаписи, передачи тревожного сигнала в центр и/или активации сигнализации.

Тревожный выход наоборот может являться результатом перехода системы в то или иное состояние, а также может вызывать активацию сигнализации, сирены, появление дыма и т.д. Тип устройства не имеет никакого значения – главное, чтобы он мог быть запрограммирован в формате двух состояний: активен/не активен.

Аудиоканал

Использование тревожного аудиоканала в последнее время стало жизненной необходимостью. Передача сигнала от оператора системы другому оператору выставляет требование к дуплексному каналу аудиосвязи. Наличие множества аудиоканалов не всегда является оправданным, так как в случае стационарной работы системы вряд ли имеет смысл фиксировать множественные источники звука, однако ряд задач требуют удаленной работы камер и скрытых микрофонов. В этом случае наиболее интересным является решение использовать удаленные охранные минисервера с интегрированным аудиоканалом в каждом из них.

Software Development Kit (SDK)

Помимо аппаратной интеграции существуют разработки, позволяющие объединять оборудование систем безопасности разных производителей единой программной средой. Это и является программной интеграцией. Существенно усложняет работу оператора и то количество различных раздельно работающих приложений, которое присутствует в центре мониторинга в случае использования ПО различных многочисленных сторонних производителей. При этом все без исключения заявляют о "дружественном интерфейсе", что далеко не всегда соответствует действительности. Вывод из этого таков, что необходим инструмент по интеграции ПО на программного уровне.

Одним из программных интеграционных средств является так называемый Development Kit, то есть инструмент разработчика. Любой производитель, который разработал сложное программное обеспечение, чаще всего сталкивается с задачей индивидуальной настройки системы. Инструментарий Разработчика системы (Software Development Kit, SDK) – это набор утилит и программ, позволяющих осуществить эффективную интеграцию функциональных возможностей системы DigiEye в охранные/информационные системы других производителей. Каждый производитель имеет свой набор инструментов. Компания SYAC разработало DigiEye SDK, другие производители – иные программные

средства разработчика. Отсутствие свободной продажи комплекта разработчика SDK является "красным светом" для монтажных организаций и интеграционных компаний, так как существенно ограничивает пространство для работы. Фактически

Посредством SDK пользователь в идеале должен иметь возможность получить доступ ко всем возможностям и данным системы:

- Поточная передача видео изображения и аудио.
- Загрузка и проигрывание записанных событий.
- PTZ/Контроль купольных камер (приближение, удаление, поворот, резкость, OSD и Aux).
- Мониторинг конфигурации и текущего статуса системы в реальном времени.
- Удаленное выполнение команд на охранном комплексе: установка второго монитора, перемена статуса цифровых выходов, включение/выключение записи камеры.
- Асинхронное оповещение о событиях.

Фактически пакет SDK позволяет пользователям и интеграторам использовать всю мощь технологий компании производителя, дополняя ее своими собственными разработками. Подобными модулями могут быть работа со специализированными приложениями по охране города, по идентификации автомобильных номеров, а также возможна полная модификация интерфейса. Программный пакет "SDK" должен позволять быстро и эффективно создавать собственное решение, используя заготовки, полное и подробное описание и готовые программы-образцы. Заготовки программного кода в рамках SDK могут быть отредактированы под собственные частные нужды за короткий срок, что и делает SDK идеальным интеграционным инструментом.

Сетевая интеграция

Важнейшим обстоятельством является также способность всей интегрированной системы работать в сетевом окружении. Действительно многочисленные разработчики сетевых цифровых решений давно "научили" свои системы работать в стандартном сетевом окружении, но важнейшим требованием современности является и взаимодействие по сети с внешними устройствами. SYAC идеологически с самого начала строил свои решения на этой основе, и наши специалисты, а также результаты маркетинговых исследований показывают, что клиенты зачастую имеют желание контролировать любые датчики, системы контроля доступа, шлагбаумы, двери и т.д. удаленно. Например, заказчик может иметь желание посредством карманного компьютера или смартфона полностью контролировать всю систему и контролировать доступ на свой объект будучи в сотне километров от него. Подобные решения уже возможны и становятся стандартом индустрии. Наши специалисты убеждены и призывают производителей становиться на этот путь истинной интеграции оборудования по сети.

Принцип работы прост. Создается неограниченная виртуальная сетевая матрица, где элементами выступает самое различное оборудование: любые камеры, клавиатура, мультиплексор, веб-сервер, ПК, датчики движения, терминалы системы контроля доступа, которые могут быть неограниченно удалены друг от друга, но при этом пользователь посредством ПК может управлять всеми устройствами. Для этого достаточно, лишь чтобы Ваш компьютер/смартфон был подключен к сети (LAN/WAN) посредством любых каналов связи, при этом вся передаваемая информация



не должна создавать большого трафика и должна гарантировать неприкосновенность видеоданных.

На последней выставке IFSEC2004 в Великобритании специалисты также отметили, что произошло окончательное смещение акцента от экстенсивного развития технологий в сторону интеллектуального использования имеющихся решений, и IP-технология окончательно становится стандартом индустрии в системах видеонаблюдения, а с недавних пор стала проникать и в иные охранные решения (контроль доступа, сенсоры и т.д.).

Пример проекта по интеграции: оператор связи

Теперь рассмотрим более подробно конкретный проект, который нам предоставили инженеры нашей компании. Он очень похож на те проекты, с которыми монтажные организации в России сталкиваются почти каждый день. Крупнейший итальянский провайдер услуг доступа в сеть Интернет выразил интерес в мониторинге всей своей инфраструктуры на территории Италии, разделенной на отдельные сектора и объекты в IP сети с существенным ограничением на пропускную способность в 64 Kbs. Для реализации проекта требовалась полная интеграция всех удаленных систем с уже существующими противопожарными системами, приборами контроля доступа и иным оборудованием. Более того, необходимо было, чтобы Центральная станция могла обрабатывать более 10 тревожных сигналов с более чем 10 различных объектов одновременно с организацией живого аудиоканала посредством IP.

Усилиями инженеров компании было разработано решение "под ключ", состоящей из централизованной системы охраны и мониторинга, работающей со всеми удаленными объектами одновременно, позволяющей управлять и взаимодействовать с их



аудио/видео данных. SYAC для реализации проекта использовал систему централизации DCC в центральном офисе и 142 системы DigiEye - на каждом из удаленных объектов. Каждая удаленная система управляла от 6 до 8 камер (в зависимости от размера объекта), а также включала в себя дуплексный аудиоканал и многозональную детекцию движения.

В центральном офисе охраны посредством системы DCC-premium был организован доступ к любым удаленным охранам серверам, осуществлялся полный контроль доступа различных пользователей к системе, определились их права и возможности изменять настройки системы. Из центральной станции теперь может быть осуществлен контроль над входами и выходами посредством системы тревожных входов/выходов, и могут быть активированы тревожные сигналы, соединенные с датчиками температурного режима, а также возможна удаленная проверка об ошибках в системах.

Центральная станция работает 24 часа в сутки и управляется подготовленными сотрудниками охраны под контролем специалиста, имеющего опыт работы в управлении системами охраны в банковских структурах. В результате использования технологий и уникальной интеграции всего оборудования в единую цифровую многофункциональную систему, резко увеличилась эффективность работы с удаленными объектами. Активируя некоторый тревожный вход из Центральной системы, оператор удаленно управляет полностью системой контроля доступа, а также в случае необходимости может воспользоваться аудиосвязью с удаленным объектом. На центральном объекте использовались более одной рабочей станции для одновременного получения тревожных сигналов и работой со всеми удаленными системами. Может быть осуществлено последовательное патрулирование всех объектов, удаленное воспроизведение ранее записанной видеоинформации, телеконфигурирование удаленных систем и составление полного протокола событий. Полная интеграция по всем направлениям: от программной до аппаратной - позволила создать одно из лучших решений, отвечающее всем требованиям клиента.

Выводы

Интеграция на действительно современном уровне происходит на нескольких уровнях, где центральным элементом должен выступать именно комплекс видеонаблюдения, как наиболее ресурсоемкий и операционнозначный. Сетевая интеграция, а также комплекс программной интеграции позволяет в современных условиях существенно облегчить работу монтажной организации и дает возможность строить фактически решения "под ключ", объединяя многочисленные охранные системы в единый комплекс. Интеграция - это единственный путь, который позволяет удовлетворить все запросы клиента с минимальными усилиями для компаний-инсталляторов и интеграторов.

Контроль доступа, охранные функции, видеонаблюдение

Интегрированная система безопасности ParsecNET-Ewclid

TOTALTECH

Http://www.totaltech.ru
E-mail: tt@totaltech.ru
(095) 688-1536, 631-0036, 631-6467