Интегрированные системы в до- и посткомпьютерную эру

На мой взгляд, индустрия систем безопасности находится на пороге очередной тихой революции. Недавно уже были всяческие цифровые революции, связанные, по общему мнению, с компьютерами. Теперь, по-моему, на пороге очередная цифровая революция, связанная, наоборот, с отказом от компьютеров (по крайней мере, частичным). Для пояснения своей точки зрения в этой статье я приведу не столько текущие факты, сколько историческую ретроспективу, чтобы попытаться оценить, чем обусловлены существующие сегодня методы интеграции и чего можно ожидать в ближайшем будущем.

А.М. Омельянчук
Начальник КБ компании "Сигма-ИС"

Что такое интегрированные системы безопасности? Такие системы устанавливались начиная с 1970-х гг., и всегда под этим понимали немного разное. Неизменным оставалось лишь одно: несколько подсистем различного назначения - как правило, охранно-пожарная сигнализация, СКУД, видеонаблюдение - должны работать как единая система. Типичными признаками интегрированной системы являются единое рабочее место оператора и возможность автоматических действий в одной подсистеме в ответ на события в другой.

Прошлый век

Традиционное решение конца прошлого столетия - релейно-мебельная интеграция. Единое рабочее место обеспечивается за счет аккуратного монтажа нескольких пультов в единый стол. Взаимосвязь между подсистемами осуществлялась за счет до сих пор единственного стандартного интерфейса - "сухого контакта". Выход тревоги от охранной сигнализации заводится на вход запуска записи видеосистемы, выход тревоги пожарной сигнализации - на вход разблокировки аварийных выходов системы СКУД и т.д. Сколько-нибудь сложная система предоставляет оператору десятки экранов и клавиатур управления, а связи между подсистемами осуществляются 100-парным кабелем. Новый уровень интеграции возник после начала активного применения компьютеров. В принципе две системы, имеющие компьютеры, можно объединить более информативным каналом, нежели несколько "сухих контактов". К сожалению, как уже упоминалось, это единственный в отрасли стандарт. Потому подключение каждой новой системы подразумевает тесное общение с ее разработчиками и как минимум дописывание нового программного кода. Тем не менее возможности систем с компьютерной интеграцией значительно шире и, как правило, подразумевают управление с одного компьютера всеми подсистемами, а также возможность настроить тысячи виртуальных связей, не прокладывая, как это потребовалось бы ранее, тысячи проводов.

Надо сказать, что сейчас уже существует довольно много программных комплексов, ориентированных на относительно быстрое подключение новых подсистем. Вы приносите описание интерфейса удаленного управления новой подсистемы, и уже через пару недель, а то и раньше основные параметры подсистемы доступны в этой программной системе. Дело в том, что основные понятия во многих подсистемах схожи, а потому разработчики таких программ придумывают некий промежуточный уровень (свой внутренний стандарт представления данных), более или менее пригодный для всех известных им подсистем. И затем для каждой новой подсистемы делают только "драйвер" -конвертер/преобразователь из внутреннего формата данных подсистемы в формат данных интегрирующего ПО. Конечно, никакие "изюминки", никакие гениальные новые функции вновь подключаемых подсистем, как правило, не доступны. Или, по крайней мере, требуют значительно больше времени, чем две недели, чтобы из универсального компьютерного АРМ можно было воспользоваться этими новыми функциями.

Как измерить интеграцию

По мере развития возможностей интеграции появились и новые критерии "глубины интеграции". Например, SIA (Ассоциация индустрии безопасности США) предложила использовать как основной признак качественной интеграции такое понятие, как "общая база данных". Как всегда бывает с достаточно сложными понятиями, это определение не слишком удачно. Понятно, что, по сути, имеется в виду возможность конфигурирования всех подсистем с одного рабочего места в единообразном пользовательском интерфейсе. Однако остаются открытыми вопросы: зачем центральной программе хранить все данные у себя в базе и обязательно ли база данных должна предусматривать одну из типовых СУБД (SQL, Oracle и т.д.) или обычные файлы - это тоже базы данных? В нормативных документах некоторых наших ведомств в начале нынешнего столетия было популярно требование к аппаратуре всех подсистем "иметь возможность удаленного управления". Это требование гарантировало как минимум возможность мебельной интеграции. А с учетом того, что эти пульты часто являются компьютерными программами, их даже можно запустить на одном компьютере. Кроме того, при наличии удаленного управления заведомо есть некоторый более или менее описанный интерфейс для подключения этого удаленного пульта, а значит, зная такие интерфейсы для всех подсистем, можно посадить несколько программистов, и они сделают "интегрирующую программу". В качестве аналога критерия "глубины интеграции" порой фигурировало довольно абсурдное требование, чтобы удаленное управление осуществлялось в объеме не менее локального. Абсурдное, например, потому, что типичное локальное действие -"включить порт удаленного управления" - в принципе невозможно осуществить удаленно. К счастью, строгость законов Российской империи, как известно, изрядно смягчается необязательностью их исполнения. На моей памяти никто из технических специалистов этих ведомств ни разу не заикался о проверке этого требования в полном объеме - приемлемым считалось, если удаленно можно было использовать основные функции.

Системы без компьютеров

Одновременно все эти годы шел процесс повышения интеллектуальности контроллеров подсистем. То, что раньше называлось ППК (прибор приемно-контрольный), или рекордер, сейчас уже трудно назвать такими простыми терминами. Современный видеорекордер - далеко не просто магнитофон, от которого происходит его название. Да и называть современные контроллеры охранно-пожарных систем словом ППК, как назывались их предки, состоявшие исключительно из лампочек и тумблеров, - у меня язык не поворачивается. Самый простой микропроцессор в отдельно взятом пожарном извещателе или даже Smart-карте в вашем кармане сегодня может сравниться по

вычислительной мощности с персональными компьютерами 1980-х гг. и значительно превышает возможности "больших" компьютеров, использовавшихся в "почтовых ящиках" в 1970-е гг. А что уж говорить про центральные процессорные блоки больших охранных систем - они полностью сравнимы по мощности со вполне современными компьютерами: гигабайты памяти, гигагерцы тактовой частоты... Разумеется, по мере повышения интеллектуальности контроллеров множились надежды на то, что интегрированные системы охраны будут выглядеть как компьютерные сети - действительно, вроде бы если у всех контроллеров есть Ethernet-разъем, то их можно легко объединить в одну сеть. К сожалению, жизнь показала, что соединить-то их можно (в том смысле, что они не сгорят при таком соединении), но и взаимодействовать они добровольно не начнут. Будучи на одинаковых разъемах, "разговаривают" они на разных языках. Отсутствие стандартизации мешает. Много раз пытались создать какие-то стандарты, но они устаревали быстрее, чем даже были написаны первые черновые варианты. Прогресс приводит к ежедневному появлению многих новых понятий, которых вчера еще не было, и протокол, вроде бы всех устраивавший ранее, сегодня уже никому не интересен. Все так же, как и в компьютерных системах. Чтобы подключить новое оборудование, нужно написать новый "драйвер", а то и добавить отдельный аппаратный "конвертер протоколов".

Впрочем, в одном повышение интеллекта контроллеров сыграло свою роль. Все большие системы сейчас сами по себе хоть немного, да интегрированные: как минимум охранная и пожарная сигнализация, контроль доступа и иногда пожаротушение, реализованные в одном контроллере, - получаются интегрированными.

Интеграция с видео

Самые большие сложности для аппаратных контроллеров всегда представляла интеграция видео. Видеосигнал содержит намного больше информации (буквально в математическом смысле слова) - мегабайты в секунду. Неудивительно, что и в прошлом, во времена релейной интеграции, часто видеопроцессор (свит-чер или мультиплексор) являлся центром интеграции.

Компьютерное интегрирующее ПО исторически развивалось с другой стороны. Наиболее развитыми компьютерными АРМ обладали системы контроля доступа - ведь там неизбежно необходимо много работы осуществлять по ведению базы данных карт доступа и полномочий их владельцев. Поэтому системы контроля доступа имели в своем составе компьютерные АРМ уже тогда, когда видеосигнал был уделом видеомагнитофонов.

Второй источник компьютерных интегрированных систем - компьютерные видеосистемы: в каком-то смысле дешевые, с цифровой обработкой видеосигнала с помощью компьютера. Такие системы иногда считаются дешевле, потому что компьютер предоставляет стандартные средства для хранения массивов видеоданных, а также монитор для отображения видеоизображения. Поэтому кажется, что это дешевле, чем использовать специальные видеомониторы и видеонакопители. Правда, сопоставимые по качеству (в старых советских терминах -с одинаковой "приемкой") компьютеры и специальные устройства стоят примерно одинаково.

Самое главное, компьютерная система имеет богатые средства управления, а также интерфейс, привычный многим пользователям компьютеров. Разработка новых систем на базе готовых, наработанных для офисных приложений библиотек с помощью развитых средств программирования намного легче, чем для встроенных микропроцессоров. Поэтому первые цифровые системы обработки видео нередко строились на основе

компьютеров с добавлением более или менее специализированных средств ввода видеосигнала. Естественное расширение компьютерных систем видеонаблюдения - подключение охранных систем, которые - с точки зрения программирования - обычно крайне просты. Результат уже называется интегрированной системой. СКУД в таких системах нередко подключается только вместе с отдельным ПО управления СКУД, поскольку работа со СКУД далеко не так проста. Считающаяся же "интегрирующей" система управления видеозаписью лишь получает от системы контроля доступа отдельные сигналы - например, о проходе в заданную дверь -для активации видеозаписи.

Наиболее "продвинутыми" (в смысле интеграции) оказались те системы, авторы которых разрабатывали как СКУД, так и видео. Они наиболее интегрированные в том смысле, что объединяют в себе видео, СКУД и "охранку", однако в большинстве случаев они поддерживают только один тип видеоаппаратуры, только один тип аппаратуры СКУД и в лучшем случае несколько вариантов "охранки". Именно эти системы сейчас наиболее эффективны, если необходимо подключить какое-то новое оборудование. Да, с немалым трудом и, как правило, только при активной поддержке авторов нового оборудования, но постепенно список "подключаемых подсистем" у таких программ растет и растет.

Интеграция с видео без компьютеров

Самое интересное, что абсолютно те же самые процессы параллельно шли и среди аппаратных (некомпьютерных) средств. В классических охранных системах еще в 1990-х гг. появились дополнительные модули для регистрации видео -хотя бы отдельных кадров с последующей пересылкой по телефонному или иному каналу на пост наблюдения. Как всегда, видеоверификация призвана снизить количество ложных тревог и ложных выездов на объект тревожной группы. С другой стороны, в каком-то смысле интегрированными стали домофоны и видеодомофоны, многие из которых сейчас поддерживают минимальную СКУД и иногда даже охранно-пожарную сигнализацию. Наиболее активно в этом направлении развивались домофоны для многоквартирных домов. Со стороны "от видео" также развивались некомпьютерные автономные видеосерверы. Первым делом они были оснащены дисками (или флэш-накопителями) для видеозаписи. Через некоторое время для целей оптимизации использования дискового пространства к ним были добавлены средства видеоанализа и входы (как всегда, под "сухие контакты") для охранной сигнализации. Все это позволяет более эффективно использовать диск, писать с высоким качеством в подозрительных ситуациях и с более низким - при отсутствии сигналов тревоги. Решительный шаг был сделан, когда некоторые такие видеорекордеры обзавелись собственным небольшим экраном для просмотра видеозаписи. Так они стали полным эквивалентным заменителем компьютерной видеосистемы. Надо сказать, что схемотехника и в большой мере программное обеспечение у данных систем порой трудно отличить от "компьютерных". Конечно, оптимизированные для круглосуточной работы одноплатные системы конструктивно более надежны, чем модульные компьютеры широкого назначения. Однако внутри, как правило, стоит процессор либо x86 (реже PowerPC), либо ARM (как в современных КПК), а операционная система - либо Linux, либо Windows-Embedded. Конечно, для обработки видео обычно присутствует специальный DSP-процессор, и, в отличие от чисто компьютерных систем, в таких случаях этот процессор нередко может эффективно выполнять свою работу даже при полном отключении процессора управления, а вся эта привычная комбинация из Windows и Pentium-подобного процессора занимается лишь красивым пользовательским интерфейсом (опять же потому, что его намного легче создавать с использованием огромного количества наработанного для Linux/Windows инструментария). Конечно, если экран не превышает 5-10 дюймов, на нем неуместно использовать многооконный

интерфейс, но оно и к лучшему - все эти масштабируемые передвигаемые окна порой полезны в офисных приложениях, но страшное зло в системах безопасности.

Почти сразу такие оснащенные дисплеями видеорекордеры научились показывать картинку не только с собственного диска, но и по сети, записанную своими менее продвинутыми собратьями. Ну и, конечно, вскоре появились системы, для которых их создатели, как и для "компьютерных" интегрированных систем, написали драйверы для подключения одной или нескольких, в первую очередь охранных, систем. Или перенесли на такие контроллеры программы управления СКУД и т.д.

Немного о перспективах

Впрочем, не следует переоценивать скорость развития технологий. Когда я говорю "такие системы" во множественном числе, это означает, что я лично знаком с двумя такими системами. Возможно, в мире существуют и другие, но их количество, несомненно, на несколько порядков меньше, чем количество интегрирующих программ для компьютеров и других "интегрированных" решений.

Напомню, что и "обычные" компьютерные системы могут быть реализованы с использованием не настольных, а индустриальных моноблочных одноплатных компьютеров, обладающих также повышенной надежностью (и непропорционально повышенной ценой). Граница между ними и контроллерами, выросшими из микропроцессорных решений, тонка. Основным критерием я бы назвал применение схемотехнических решений, обеспечивающих продолжение видеозаписи и видеоанализа при зависании операционной системы процессора управления. Впрочем, и этот критерий не идеален. И на обычном компьютере можно реализовать решения, освобождающие плату видеосопроцессора от зависимости от операционной системы (но это иногда может, например, потребовать установки отдельного жесткого диска, предназначенного исключительно для видеозаписи). Однако даже если видеозапись будет идти, все прочие, собственно "интегрирующие" функции в лучшем случае не будут мешать работать отдельным подсистемам, а в худшем - при зависании Windows прекратит работу охранная или пожарная сигнализация. В этом отношении embedded (встраиваемые) версии Linux и Windows значительно надежнее. Кроме того, во встраиваемых версиях операционных систем можно легко выкинуть все ненужные компоненты и тем самым еще значительно повысить скорость и надежность работы устройства.

Подводя итоги сказанного, вновь с грустью упомяну о медленно развивающемся процессе стандартизации интерфейсов. В основном речь о программных интерфейсах - на основе XML и WebServices. Не буду вдаваться в детали - все они пока на весьма ранней стадии. Для интересующихся перечислю основные названия: ANSI/SIA OSIPS (особенно интересны видеорасширения), OASIS oBIX, OASIS WSDM, OASIS EDXL, AXIS/SONY/BOSCH ONVIF. Подробности легко найти в Интернете. Все эти интерфейсы ориентированы на использование довольно мощных компьютеров, но я опасаюсь, что когда какой-то из них получит широкое распространение, опять пожарный извещатель станет мощнее современного компьютера и опять эти интерфейсы будут тормозом прогресса.

Опубликовано: Журнал "Системы безопасности" #5, 2009