

Технология OPC в системах безопасности

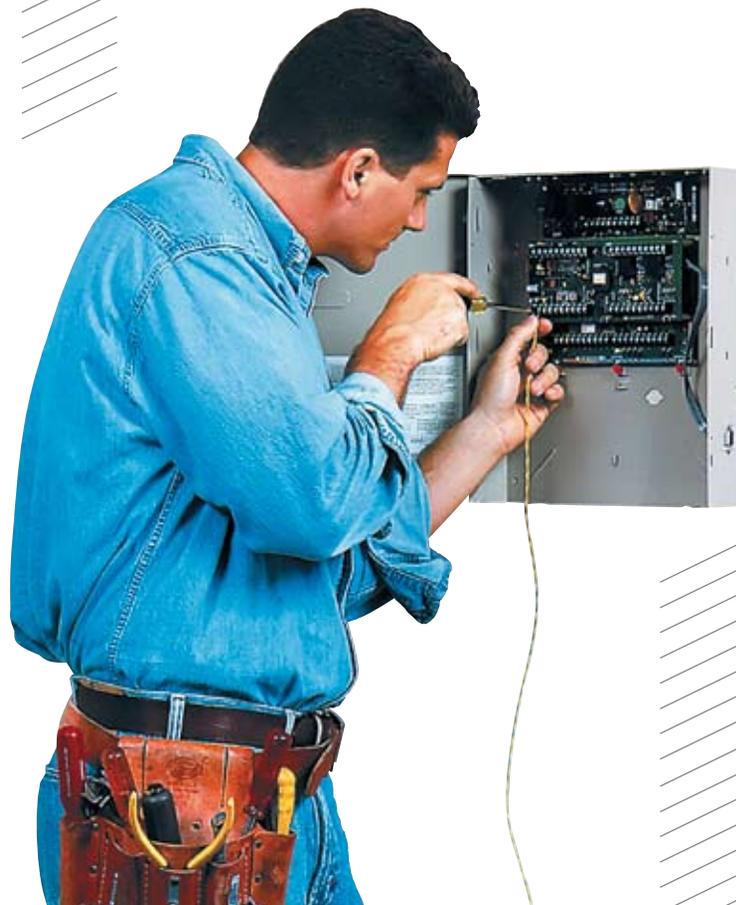
ЧТО ТАКОЕ OPC

OLE for Process Control, или сокращенно OPC, — это программная технология, которая определяет правила взаимодействия оборудования и программного обеспечения верхнего уровня. В расшифровке названия OPC содержится еще одна аббревиатура: OLE — Object Linking and Embedding, это технология Microsoft, предназначенная для использования ресурсов одних программ внутри других. Например, проигрывание звукового файла, внедренного в текстовый документ Word, реализуется как раз с помощью OLE. В настоящее время эта технология известна под названием ActiveX и широко применяется, например, в web-программировании. Создание и поддержку спецификаций OPC координирует международная некоммерческая организация OPC Foundation, созданная в 1994 г. ведущими производителями средств промышленной автоматизации. В тот момент задача стандартизации передачи данных из оборудования на уровень диспетчеризации встала уже в полный рост и требовала безотлагательного решения. В основном реализации OPC базируются на технологиях Microsoft, таких как COM/DCOM, ActiveX, но есть и платформенно независимые решения. Кроме Windows существуют реализации под Unix подобные системы, QNX и некоторые другие.

На самом деле OPC включает в себя целое семейство стандартов — всего около десятка. Каждый реализует определенный набор сервисов. Самый популярный из них OPC DA (Data Access), который отвечает за обмен данными с различным технологическим оборудованием. Чаще всего, когда упоминают стандарт OPC, имеют в виду именно OPC DA. Здесь нужно отметить, что так как OPC родом из мира автоматизации производства, то в основном в качестве оборудования выступают программируемые логические контроллеры (ПЛК), различного рода системы управления, а также средства организации интерфейса с оператором. Хотя это вовсе не исключает возможность использовать OPC для задач из других областей, например для систем безопасности, о чем и будет рассказано ниже.

С программной точки зрения в OPC можно выделить два основных компонента: OPC-сервер и OPC-клиент. Сервер отвечает за работу с оборудованием, а клиент

Сергей ЛЕВИН,
главный конструктор СИГМА-ИС



находится на стороне программного обеспечения, которое получает данные от этого оборудования. То есть мы видим классический пример клиентсерверной архитектуры.

Работает это так. Оборудование, пусть это будет ПЛК или контроллер, подключается к компьютеру, на котором запускается приложение OPC-сервер. Физический канал подключения может быть любым, это стандартом не регламентируется. Это может быть последовательный интерфейс RS-485 или сеть Ethernet, не столь важно. Для обмена данными между контроллером и сервером нужен драйвер, который предоставляется либо производителем контроллера, либо пишется разработчиками сервера. Процесс обмена данными с оборудованием, в общем, также остается за рамками стандарта OPC. А вот дальше уже все делается так, как требует OPC DA. Информация, полученная от контроллера, в сервере организуется в виде специальных переменных, часто называемых тегами. Переменные могут быть самого различного типа. Например, логическая переменная определяет два состояния: 0 или 1 и подойдет для описания простого дискретного входа. Для описания цифровых входов со многими состояниями или аналоговых входов используются переменные целого типа Int или вещественного Float. Также можно передавать значение различных перечислителей, внутренних переменных и объектов оборудования. Кроме этого, имеются переменные, хранящие дату и время, строковые данные, массивы и т. п. Помимо непосредственно значения в переменной сервера имеются некоторые дополнительные данные. Например, метка времени (timestamp), которая показывает, когда было последнее обновление значения переменной. Это бывает полезно, когда данные имеют определенное «время жизни» и клиент по метке времени может проверить актуальность информации. Канал обмена данными в OPC двухсторонний, поэтому то же самое справедливо и для данных, передающихся в другом направлении — из сервера в оборудование. Запись данных в оборудование позволяет реализовать задание параметров работы или конфигурирование контроллера, а также команды управления. Например, для выполнения команды, которая должна изменить состояние физического выхода в контроллере, OPC-клиент должен записать нужное значение в соответствующую переменную, которая в сервере будет трансформирована в аппаратно зависимую команду через драйвер оборудования. При этом, что крайне важно, OPC-клиент не знает и не должен знать особенностей работы с конкретным контроллером или терминалом. Все происходит совершенно стандартным образом.

Дальше полученные от оборудования данные должны быть переданы из OPC-сервера в OPC-клиент. Собственно, реализация этого процесса передачи данных и представление самих данных в виде переменных и есть основная суть стандарта OPC DA. Согласно спецификации OPC любые данные, представленные в сервере, могут быть стандартным способом переданы в клиентское приложение. В качестве клиента в основном выступают ПО диспетчерского управления и сбора данных (SCADA — SupervisoryControlAndDataAcquisition). OPC-клиент может получать данные от OPC-сервера несколькими способами: простой синхронный запрос, когда клиент отправляет в сервер список переменных и дожидается ответа, в котором передаются их текущие значения, а также дополнительная информация (например, метка времени). Очевидно, что при этом на время выполнения запроса сервером соответствующий программный интерфейс клиента «подвисает». При асинхронном запросе клиент не дожидается ответа от сервера, а получает его по мере готовности через специальный интерфейс COM-объекта. И, наконец, существует механизм подписки, с помощью которого сервер автоматически передает клиенту интересующие его переменные через определенные промежутки времени. Скорость обновления может настраиваться. Запись данных производится аналогично, с помощью синхронных и асинхронных запросов. Механизм подписки для записи не используется.

OPC И СИСТЕМА БЕЗОПАСНОСТИ

Как видно из первой части, стандарт OPC разработан и применяется в системах управления и автоматизации технологических процессов. Какое же отношение это может иметь к системам безопасности?

Во-первых, OPC можно рассматривать как стандарт подключения оборудования к верхнему уровню системы безопасности. Не секрет, что сейчас в этом вопросе согласия среди производителей нет. Поставщикам оборудования для систем видеонаблюдения повезло несколько больше. Здесь развиваются сразу два альтернативных стандарта по коммуникациям японо-европейский ONVIF и американский PSIA. Для производителей и пользователей ОПС и СКУД ничего подобного нет, и всякий раз, когда возникает задача построения системы безопасности на основе оборудования и программного обеспечения от разных производителей, возникают проблемы, зачастую непреодолимые. Речь не идет о том, чтобы поголовно перейти всем на OPC, избрав его единственным способом взаимодействия. Но вот если производители оборудования будут снабжать свой прибор или систему OPC-сервером, а разработчики интегрирующего ПО предусмотрят в своих программах реализацию OPC-клиента, жизнь интеграторов, инсталляторов и пользователей станет намного легче. Причем это не касается весь спектр выпускаемого оборудования — извещатели, оповещатели, датчики, считыватели и тому подобные объектовые устройства не требуется переводить на OPC. Речь идет только об уровне систем сбора и обработки информации (ССОИ). При этом тревожные и информационные события от приемно-контрольного оборудования будут представлены в виде соответствующих переменных OPC-сервера. Также через переменные можно передавать состояния отдельных объектов, организовывать управление и, если необходимо, конфигурирование оборудования.

Во-вторых, оборудование систем безопасности может быть интегрировано с инженерными и технологическими системами объекта. Это позволит реализовать автоматизированные алгоритмы совместной работы. Чаще всего это связано с работой пожарной сигнализации. Например, в случае выдачи сигнала «Пожар» перевести технологическое оборудование в безопасный режим работы, отключить, если необходимо, электропитание, задействовать дополнительные системы безопасности. Иногда нужно в зависимости от текущего режима работы технологических систем изменить определенные параметры настройки пожарной сигнализации. Это может быть отключение одного из каналов обнаружения возгорания. Тогда при кратковременном допустимом с точки зрения технологического процесса повышении уровня задымленности или запыленности помещения можно автоматически отключать дымовые извещатели в пожарной сигнализации, чтобы исключить выдачу ложных извещений о пожаре.

И, наконец, самое главное — появляется возможность объединить систему безопасности вместе с технологическими и инженерными системами в единый комплекс управления предприятием. Это позволит создать единое информационное пространство, повысить эффективность управления и снизить эксплуатационные издержки. Данные от всех систем комплекса становятся доступными для выдачи диспетчеру или автоматической централизованной обработки в реальном времени. Все это существенно повышает качество принятия решений диспетчерскими службами предприятия.

Таким образом, девиз организации OPC Foundation — «Открытые коммуникации по открытым протоколам» целиком и полностью может быть распространен и на системы безопасности. 