Типовые ошибки в проектировании систем диспетчеризации и АСУ ТП

Технические задания на системы промышленной автоматизации, в том числе размещенные на тендерных площадках, часто содержат ошибки, реализация которых на практике может снизить качество и безопасность разрабатываемых АСУ, а также необоснованно увеличить их стоимость. В статье рассмотрены такие характерные ошибки, как злоупотребление OPC и веб-интерфейсом, применение протоколов реального времени в телемеханических задачах и некоторые другие.

ООО «АдАстра Рисерч Груп», г. Москва

Анализируя современные технические задания на системы промышленной автоматизации, размещенные на тендерных площадках даже крупными и уважаемыми компаниями, мы часто отмечаем повторяющиеся ошибки, реализация которых на практике может снизить качество и безопасность разрабатываемых АСУ, а также необоснованно увеличить их стоимость. Так как эти ошибки кочуют из ТЗ в ТЗ и на основе этих документов потом создаются реальные системы промышленной автоматики, то представляется актуальным предостеречь проектировщиков от их повторения.

Злоупотребление OPC-технологией при проектировании

Стандарт OPC разработан в 1994 году международной организацией OPC Foundation с целью создать универсальный интерфейс для связи SCADA-систем и УСО с различными коммуникационными протоколами. Термин УСО (устройство связи с объектом) в данной статье мы будем использовать расширительно, включая в него не только промышленные контроллеры – ПЛК, АЦП-ЦАП, счетчики, цифровые датчики, но и полевые шины. Так как промышленные УСО используют сотни различных протоколов для передачи данных на ПК, то технология сведения их всех к одному, то есть к OPC-интерфейсу, была крайне актуальной и востребованной на рынке.

Однако не стоит забывать, что OPC – это технология-посредник, а за посредничество всегда надо платить. На конвертацию каждого сообщения, поступающего из УСО в формат OPC-сервера, а затем и OPC-клиента, расходуется время и системные ресурсы компьютера. Наши тесты, проведенные с одним популярным на рынке OPC-сервером (специально не называем марку этого продукта, так как не в ней дело), показали, что обмен со SCADA TRACE MODE по протоколу Modbus TCP через OPC-интерфейс осуществляется в среднем в два раза медленнее, чем через прямой драйвер. При этом загрузка центрального процессора компьютера возрастала в четыре раза по сравнению с прямым драйвером. Кроме того, при использовании OPC-интерфейса снижается надежность обмена на высоких скоростях – в наших тестах число недоставленных значений при передаче данных по OPC было в два раза выше по сравнению с прямым драйвером Modbus TCP, используемым в TRACE MODE 6.

Настройка OPC-сервера на ПК является трудоемкой процедурой. Технология DCOM, на которой основан наиболее востребованный стандарт OPC DA/HDA, не поддерживается в Windows, начиная с Windows XP. Его установка и настройка требуют усилий, а сохранится ли эта возможность в будущем, вообще неясно. Кроме того, трудоемкой является ручная привязка тегов OPC-сервера к источникам данных SCADA-системы.

OPC-технология обладает рядом уязвимостей, причем это относится и к новой реализации OPC UA, что отмечалось рядом исследователей, в том числе «Лабораторией Касперского» [1].

Также следует учитывать, что OPC-сервер – это не бесплатный продукт (хотя есть исключения). Стоимость OPC-сервера может достигать 1000 евро за один протокол. И платить надо за каждый ПК, где установлен OPC-сервер.

Итак, вышеизложенные аргументы позволяют сформулировать вывод: если в используемой SCADA-системе есть поддержка протокола УСО прямым драйвером, то применение OPC-сервера нерационально и ведет к ухудшению качества АСУ ТП.

На практике мы видим технические задания, где для связи с УСО по распространеннейшим протоколам – Modbus, SNMP, DCON, МЭК 60870-5-104 – требуется использование OPC. Это типичная ошибка проектировщиков, от которой следует отказаться, сформулировав требование к интерфейсу так: «Прямой драйвер

ИЛИ OPC». А лучше вообще оставить это на выбор интеграторам. Авторам известны многие АСУ ТП, в которых связь осуществляется по протоколу Modbus, но через OPC потому, что «так написано в проекте». Давайте от этого избавимся! Иначе АСУ ТП будут работать медленнее, станут менее надежными, требующими больше ресурсов ПК, труднее настраиваемыми и при этом более дорогими.

Злоупотребление веб-интерфейсом

Все мы используем браузеры для получения информации в повседневной жизни, поэтому веб-интерфейс АСУ представляется очевидной и удобной функцией. Это действительно так, но только если речь идет о небольших, исключительно мониторинговых системах для объектов малой значимости. Примерами таких систем могут быть АСУ небольших фермерских хозяйств, домашняя автоматика, системы учета ресурсов и т.д. Причем обязательным критерием правильности применения веб-визуализации является сочетание всех трех условий: малый размер АСУ, отсутствие функций управления и небольшой вред от возможного вывода объекта из строя или компрометации информации. Во всех остальных случаях (а это более 95% всех АСУ) использование веб-доступа недопустимо, так как не отвечает требованиям безопасности.

Дело в том, что АСУ с веб-интерфейсом «открывает» свой IP-адрес для доступа через интернет. Все доступные адреса в сети сканируются роботизированными системами 24 часа в сутки и 7 дней в неделю. Определить принадлежность IP-адреса к АСУ ТП можно, используя ряд признаков, среди которых тип протокола, данные о производителе, используемое ПО. Эти признаки уже давно собраны в базы и активно применяются злоумышленниками. После того как адрес АСУ определен, вас защитит только пароль доступа. Даже если представить, что пароли созданы по всем правилам и регулярно обновляются, вскрыть их – всего лишь дело времени, а время у хакеров есть. Если кто-то сомневается в актуальности данной проблемы, рекомендуем прочитать доклад компании Positive Technologies «Безопасность АСУ ТП: итоги 2017 года» [2]. Хорошо еще, что Россия занимает лишь 28 место по уязвимости национальных АСУ ТП, 42% всех уязвимостей АСУ ТП приходится на США [2]. И пример с них брать не надо.

Несмотря на очевидную небезопасность веб-технологий в АСУ ТП, проектировщики продолжают вносить в ТЗ требование веб-интерфейса. Причем делают это и для крупных, управляющих АСУ, и даже для взрывоопасных производств. Особенно часто подобные требования почему-то встречаются в нефтяной промышленности.

Нам возразят: веб-интерфейс в крупных управляющих АСУ ТП может использоваться внутри предприятия, при этом веб-адреса не выставляются в сеть. Да, если веб-серверы АСУ ТП защищены сетевыми экранами, то безопасность таких систем возрастает. Однако при этом возникает вопрос о целесообразности. Зачем использовать веб внутри операторского зала или административного корпуса? Все достоинства веб-доступа связаны именно с мобильностью персонала, а если ее нет, то остаются лишь недостатки. А они таковы:

1. АСУ ТП с визуализацией на основе браузеров менее безопасны, чем традиционные клиент-серверные системы с «толстым» клиентом. Веб-технология дает унифицированный механизм доступа к АСУ ТП, и хакеру, проникшему внутрь сети, будет проще к ней подключиться, тогда как при использовании традиционного клиент-сервера ему еще понадобится добыть и установить у себя клиентское приложение, то есть пройти еще несколько рубежей защиты (весьма сложных, так как клиенты обычно защищены аппаратными ключами).

2. АСУ ТП с визуализацией на основе браузеров сложны в обслуживании. Дело в том, что при использовании веб-визуализации в отношения между пользователем и производителем SCADA включается непредсказуемый участник – производитель браузера. Он ничего не знает о нашей АСУ ТП, никак не обязан заказчику и действует, исходя из своих представлений о целесообразности. Поэтому он может в любой момент прекратить поддержку той технологии, на которой основан веб-интерфейс вашей АСУ ТП (ActiveX, Java, Flash, HTML 5 и др.), заменив ее на более совершенную с его точки зрения, но не поддерживаемую в SCADA технологию. Так как жизненный цикл АСУ ТП составляет в среднем 15 лет, то вероятность отказа поддержки технологии в браузере близка к 100%. Вспомните, какие были браузеры в 2003 году, а теперь представьте, какими они будут в 2032-м! Использование веб-визуализации в операторских комплексах сулит практически гарантированные проблемы в эксплуатации.

Вот почему мы считаем требование безальтернативности веб-интерфейса в проекте АСУ ТП ошибкой проектирования.

Ошибка выбора коммуникационного протокола

Было время, когда каждый производитель УСО в нашей стране придумывал и развивал свой протокол. Было и прошло. Теперь мы страна победившего Модбаса. Протоколы Modbus RTU и TCP поддерживаются практически всеми отечественными и большинством зарубежных производителей. Протоколы действительно хорошие, проверенные, рабочие.

Однако следует понимать, что Modbus применим только к части систем АСУ, а именно к системам с надежной передачей информации – назовем их системами «реального времени». В основном к ним относятся локальные АСУ ТП, расположенные в пределах одного здания, реже – распределенные системы, обладающие первоклассными коммуникациями.

Если коммуникации не обеспечивают надежной и непрерывной доставки информации (а это обычно территориально распределенные системы с радиосвязью, GSM, интернетом), то в них надо использовать телемеханические протоколы (да и контроллеры со SCADA тоже), обеспечивающие буферизацию информации в период отсутствия связи, а также ее досылку и корректную запись в SCADA-систему. Примерами подобных протоколов являются ГОСТ МЭК 60870-5-101, МЭК 60870-5-104, iNET (TRACE MODE) и ряд других.

Можно возразить, что Modbus используется в малонадежных сетях в целях экономии, так как телемеханические RTU обычно дороже (кстати, не всегда). Но нет – несов-

местимые требования использовать «легкие» протоколы Modbus и SNMP мы видим в технических требованиях к автоматизации месторождений у наших крупнейших нефтяных компаний. При этом выдвигается требование буферизации и довосстановления данных от УСО при восстановлении каналов передачи данных после их отказов. Эти требования несовместимы и являются ошибкой проектирования!

Конечно, и по Modbus можно передать метки времени, а в Modbus-контроллере написать прикладную программу, буферизирующую данные и досылающую их на сервер (кстати, в SCADA TRACE MODE реализована подобная функция [3]). Но вот только зачем создавать препятствия и героически их преодолевать? Зачем ставить системного интегратора в заведомо неудобное положение неуместным требованием? Не всегда его квалификации может хватить для исправления данной ошибки проектировщика.

Заключение

Требования неправильного использования OPC, веб-интерфейса, Modbus и SNMP кочуют из проекта в проект. Устранение этих повторяющихся ошибок, на наш взгляд, позволило бы исправить до 90% противоречий в современных требованиях к программному обеспечению АСУ ТП и системам диспетчеризации и дало бы возможность улучшить их качество на протяжении всего жизненного цикла.

Литература

1. Черемушкин П., Темников С. Исследование безопасности OPC UA // Kaspersky Lab ICS CERT : [сайт]. URL: https://ics-cert.kaspersky.ru/reports/2018/05/10/opc-ua-security-analysis/ (дата обращения: 06.09.2018).

2. Безопасность АСУ ТП: итоги 2017 года. Доклад компании Positive Technologies [Электронный ресурс]. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf (дата обращения: 06.09.2018).

3. Телемеханика // AdAstra Research Group : [сайт]. URL: http://www.adastra.ru/products/overview/remotecontrol/(дата обращения: 06.09.2018).

Л. В. Анзимиров, президент,
А. Ю. Токарев, к. т. н., руководитель учебного центра,
ООО «АдАстра Рисерч Груп», г. Москва,
тел.: +7 (495) 771-7174,
e-mail: secretariat@adastra.ru,
сайт: www.adastra.ru