

ПРОМЫШЛЕННЫЙ INTERNET ВЕЩЕЙ И ОБЛАЧНЫЕ ТЕХНОЛОГИИ В СОВРЕМЕННЫХ SCADA-СИСТЕМАХ

К.С. Климков (Компания ИнСАТ)

Рассмотрена возможность реализации технологий Internet вещей с использованием SCADA-систем четвертого поколения на примере MasterSCADA 4D. Особый акцент сделан на кибербезопасности.

Ключевые слова: SCADA-система, IoT, IIoT, облачные сервисы, OPC UA, кроссплатформенность, кибербезопасность.

С каждым годом Internet оказывает все большее влияние на бизнес, образование, производство и жизнь в целом. Об Internet вещей (IoT) говорят уже на протяжении почти 20 лет, однако никогда спрос на него не был таким высоким, как сейчас. Согласно идеи IoT, различные объекты подключаются друг другу и обмениваются информацией как между собой, так и с пользователями. Например, холодильник может уведомлять хозяина о состоянии продуктов и отправлять в магазин заказ на пополнение их запаса. IoT нашел применение и в промышленных отраслях, характеризующихся высокой степенью автоматизации. После 40 лет использования трех поколений SCADA-систем — автономных, распределенных и сетевых — многие производственные отрасли стали нуждаться в SCADA-системах четвертого поколения с технологией IoT.

Промышленный Internet вещей (IIoT) в SCADA четвертого поколения

SCADA-система третьего поколения состоит из условно нижнего, среднего и верхнего уровней. На нижнем и среднем уровне расположены ПЛК и модули с подключенными к ним датчиками, а также средства сбора данных, такие как OPC или драйверы устройств. На верхнем уровне находятся системы управления и мониторинга, позволяющие в реальном времени управлять оборудованием нижнего уровня, принимать сигналы тревог с датчиков, обеспечивать оптимальное функционирование оборудования. Обычно визуализация развернута на локальном компьютере с ограниченным внешним доступом, поэтому SCADA третьего поколения идеально подходит для ежедневного мониторинга процессов на самом производстве. IoT начинается там, где заканчиваются возможности классической SCADA-системы. IoT использует последние дости-

жения в области аппаратного обеспечения соединений, сетей передачи данных, облачных вычислений и обработки больших объемов данных, позволяющие SCADA-системам выполнять более сложные задачи.

Преимущества IoT, реализованные в MasterSCADA 4D

На производстве существует множество проблем, связанных с использованием оборудования от разных производителей и сразу нескольких SCADA-систем; с ограничением на хранение и использование большого объема данных на жестких дисках локальных и сетевых систем. Реализация вертикальной и горизонтальной интеграции разнообразных устройств распределенных систем управления в MasterSCADA 4D позволяет решить первую проблему. В программе внедрен набор подключаемых к различному оборудованию драйверов и осуществлена поддержка стандартных протоколов, списки которых постоянно расширяются. Благодаря этому пользователь может одновременно получать и обрабатывать данные со всех контроллеров, модулей, датчиков, счетчиков, баз данных (рис. 1).

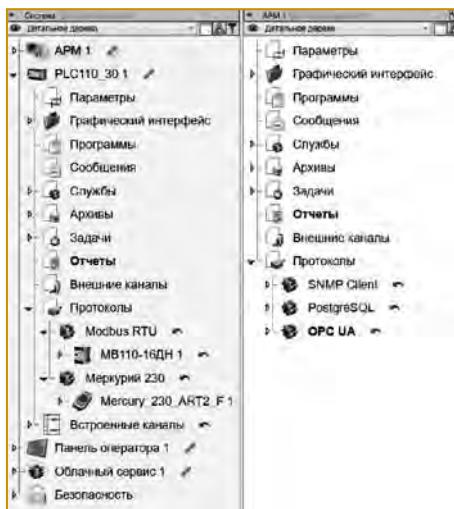


Рис. 1. Дерево физической структуры проекта с подключаемым оборудованием в MasterSCADA 4D

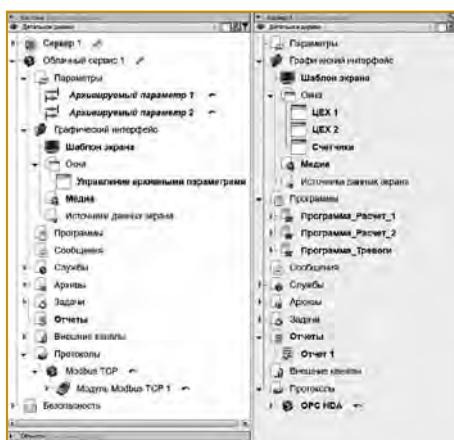


Рис. 2. Узлы «Сервер» и «Облачный сервис» в MasterSCADA 4D

Для решения проблем, связанных с хранением большого числа архивируемых данных и доступом к ним различных групп пользователей, в MasterSCADA 4D реализованы системные узлы «Сервер» и «Облачный сервис» (рис. 2). Рассмотрим более подробно основные преимущества поддержки IoT в SCADA-системах.

- Снижаются сетевые накладные расходы. SCADA третьего поколения предусматривает совместное использование статических IP-адресов. По мере увеличения числа пользователей увеличивается нагрузка на сеть, падает производительность. С помощью IoT получение данных между узлами происходит посредством групповых запросов, благодаря чему снижается сетевой трафик и объемы вычислительных ресурсов [1].

- Улучшается качество обслуживания системы. Анализ данных с оборудования позволяет продлить срок его службы, сократить время простоя, в целом позволяет существенно снизить затраты.

- Появляется возможность интегрировать в единый проект множество удаленных предприятий. Крупные промышленные производства имеют большое число удаленных филиалов, и консолидация данных может быть затруднена. Проблема решается установлением связи между облачными сервисами с загруженной на них информацией по каждому филиалу и серверами, развернутыми в головных центрах управления и мониторинга.

- Пользователям предоставляется полный доступ к данным со всего оборудования на производстве. Это позволяет аналитикам получать подробную информацию о состоянии производственных процессов, проводить более качественный анализ данных и, таким образом, улучшать производительность на всех этапах производства, инженерам — принимать мгновенные решения, а руководству — наблюдать за производством в целом.

Визуализация в MasterSCADA 4D

Для получения доступа к большим объемам данных и их представления в легко интерпретируемой форме пользователю нужен удобный инструмент. Таким является Web-браузер, поддерживающий стандарт HTML5, с помощью которого в MasterSCADA 4D организован человеко-машинный интерфейс. Кроссплатформенный встроенный Web-сервер обеспечивает связь между исполнительной системой и графическим клиентом, поэтому для отображения проекта могут использоваться планшет, телефон, сенсорная панель, компьютер как с собственным графическим клиентом MasterSCADA 4D, так и с установленными стандартными браузерами [2].

OPC UA как технология Internet вещей

OPC UA является одним из ключевых протоколов IoT, так как с его помощью в режиме реального времени работает связь между устройствами от разных производителей. OPC UA — это расширение протокола OPC, который используется в SCADA-системах третьего поколения. Однако технология OPC UA обладает рядом преимуществ по сравнению с OPC:

- реализована безопасность с поддержкой протоколов HTTPS, SSL и связанных с ними функций



Рис. 3. Редактор OPC UA в MasterSCADA 4D

- сертификации, шифрования и аутентификации;

- OPC UA не полагается на технологию OLE или DCOM и может работать на любом устройстве, способном разворачивать Web-сервер. Это могут быть ОС Windows, WinCE, Embedded, Linux и др.;

- возможность адаптации OPC UA как в небольших, так и в крупных сложных системах.

Все эти факторы делают OPC UA чрезвычайно дружественным к IoT. В MasterSCADA 4D также встроена технология OPC UA: можно подключиться клиентом к OPC UA серверу, получать и использовать его данные; любой узел в дереве системы может стать OPC UA сервером и передавать данные другим клиентам (рис. 3).

Internet вещей и кибербезопасность

Рост применения IoT в промышленности ограничивается требованиями к безопасности обмена данными. В SCADA-системах используется множество коммуникационных протоколов, и в первую очередь это открытый стандарт TCP/IP. SCADA может стать мишенью для злоумышленников: ее уязвимость связана как с установкой на ОС Windows, так и с тем, что она имеет доступ к другим локальным компьютерам и ПЛК. Регулятор в лице правительства РФ также предусматривает процедуры по защите информационных систем, о чем свидетельствует «Доктрина информационной безопасности РФ» (<https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>), а также пакет нормативно-правовых актов, главным из которых является Законопроект № 475717 «О безопасности критической информационной структуры РФ». На основании указанных документов к уже имеющимся требованиям по быстродействию и отказоустойчивости для объектов критической инфраструктуры добавляется еще одно — информационная безопасность.

Существует ряд мер предотвращения угроз в SCADA-системах [3]. Необходимо применять комплексный подход к проектированию подобных систем, чтобы система защиты информации (ЗИ) не оказывала влияние на быстродействие системы, что достигается путем максимальной интеграции отдельных компонентов. Помимо сегментации сетей, антивирусных решений, аппаратных или программно-аппаратных средств криптографической защиты информации немаловажную роль играют средства аутентификации пользователей, возможность

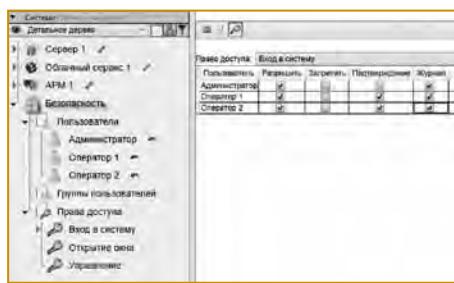


Рис.4. Раздел «Безопасность» в MasterSCADA 4D

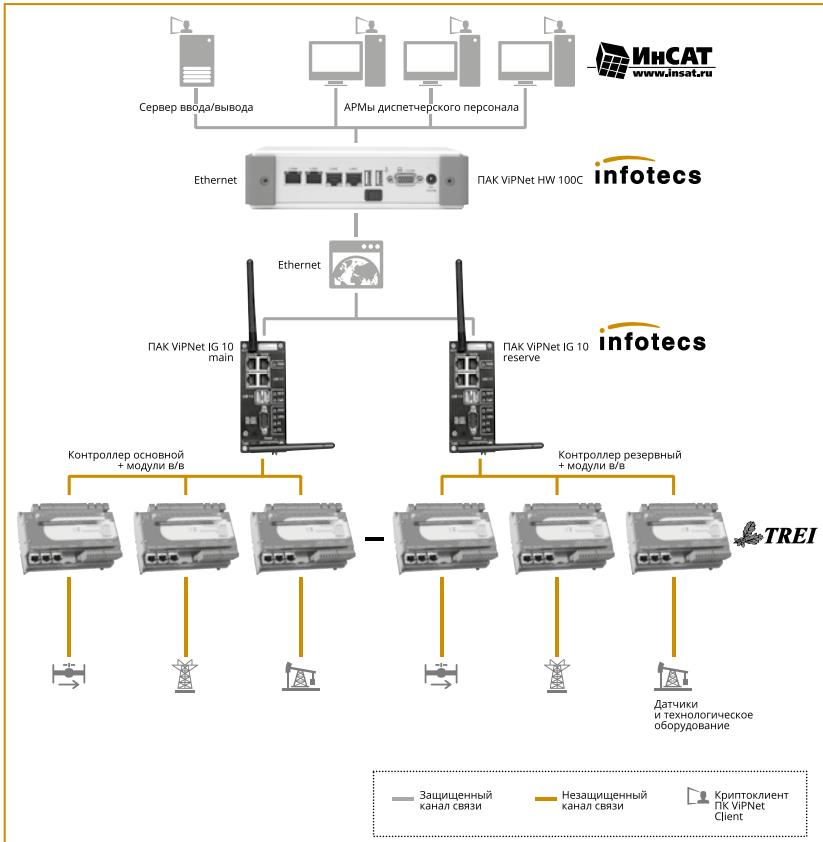


Рис. 5. Структурная схема ПТК

отделить пользователей от администраторов и представлять им различные уровни доступа. Администратор должен контролировать состояние всей системы, видеть взаимодействие пользователей со всеми частями проекта и быстро реагировать на появляющиеся угрозы. В MasterSCADA 4D в разделе «Безопасность» реализовано разделение на пользователей с ограничением прав (рис. 4). Логирование всех действий операторов осуществляется в отдельном журнале, также в ближайшее время станет возможно использование двухфакторной аутентификации и цифровых криптографических подписей, что позволит с максимальной достоверностью анализировать нештатные ситуации для выявления конкретных лиц, которые оказали то или иное воздействие на систему. В графическом клиенте предлагается выбрать пользователя и ввести пароль. В зависимости от заданных прав можно ограничивать открытие окон, запрашивывать подтверждение каких-либо действий.

При правильном использовании указанных мер можно спроектировать объект с периметром безопасности, который станет достаточно серьезной преградой для сетевого нарушителя. Учитывая это, компания ИнСАТ совместно с компаниями ИнфоТеКС (Москва) и ТРЭИ (г. Пенза) разработали решение, сочетающее самые современные наработки в области автоматизированных систем и защиты информации (рис. 5). Для опроса оборудования в ПТК используются ПЛК серии ТРЕИ-5

Кирилл Сергеевич Климков – инженер по тестированию компании ИнСАТ.

В-05, которые комплектуются необходимым набором модулей ввода/вывода. В данные контроллеры установлен исполнительный файл MasterSCADA, который позволяет запрограммировать их на языках стандарта МЭК 61131-3 из единой среды разработки. Сервером может быть любой компьютер, в том числе и на базе микропроцессора Эльбрус, поскольку MasterSCADA является кроссплатформенной системой. В качестве наложенных средств защиты используются сетевые шлюзы безопасности от компании ИнфоТеКС – VIPNet Coordinator IG10 и HW100 в индустриальном исполнении, которые организуют виртуальные защищенные сети (VPN) в промышленных системах и сегментируют их на домены. Разработанный ПТК благодаря гибким возможностям оборудования может быть использован для любых объектов диспетчеризации и автоматизации в различных отраслях промышленности.

Заключение

Масштабный переход на SCADA с поддержкой ПоТ не означает полного отхода от SCADA третьего поколения. Модернизация существующих SCADA-систем – достаточно сложный и длительный процесс, и многие отрасли промышленности продолжают полагаться на существующие решения, например MasterSCADA 3.X. Реализация ПоТ – это следующий этап в эволюции SCADA, обеспечивающий повышенную эффективность при меньших затратах на разработку и внедрение. SCADA четвертого поколения позволяет получать и хранить большой объем данных со всех устройств и давать к нему контролируемый доступ. Поддержка OPC UA, облачных сервисов, HTML5 и защита от киберугроз – неотъемлемая часть функций современных SCADA-систем. Такой является MasterSCADA 4D, позволяющая создавать классические АСУТП с поддержанными технологиями промышленного Internet вещей.

Список литературы

1. Леонов А.В. Интернет вещей: проблемы безопасности // Омский научный вестник. 2015. № 2 (140). стр. 215–218.
2. Варламов И.Г. SCADA нового поколения. Эволюция технологий – революция системостроения // Автоматизированные информационно-управляющие системы в энергетике. 2016. №2 (79).
3. Tryfonas Li, S., T., & Li, H. () The Internet of Things: A Security Point of View. Internet Research. 2016. 26(2). pp. 337–359. DOI: 10.1108/IntR-07- 2014-0173.

Контактный телефон 7(495) 989-22-49.
E-mail:info@insat.ru http://www.insat.ru