УДК 681.5

Е.В. Бабешко, И. Эльяси Комари

Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»

АНАЛИЗ БЕЗОПАСНОСТИ И УЯЗВИМОСТИ КОМПОНЕНТОВ СОВРЕМЕННЫХ SCADA-СИСТЕМ

Рассмотрены современные системы диспетчерского управления и сбора информации (SCADA-системы). Проанализированы их уязвимости и существующие методы борьбы с ними.

автоматизация, АСУ ТП, SCADA-системы, OPC, уязвимости

Введение

Необходимым элементом современных автоматизированных систем управления технологическими процессами (АСУ ТП) являются системы диспетчерского управления и сбора данных (SCADA, Supervisory Control And Data Acquisition). Основные функции, возлагаемые на SCADA-системы, следуют из их названия – это сбор данных о контролируемом технологическом процессе и управление этим технологическим процессом, реализуемое ответственными лицами на основе собранных данных и правил (критериев) [1, 2]. В последнее время достаточно остро встал вопрос обеспечения информационной безопасности существующих SCADA-систем [3]. Это обусловлено тем, что большинство внедряемых в настоящее время SCADA управляет сложными критическими объектами. Поэтому любые некорректные действия SCADA-системы, атакованной злоумышленником, могут привести к крайне негативным последствиям. Кроме того, последние исследования показали ряд серьезных уязвимостей основных элементов SCADA-систем.

Различные аспекты информационной безопасности обсуждались в ряде работ, однако детальный системный анализ уязвимостей SCADA-систем и методов их устранения не проводился. Поэтому целью данной статьи является проведение такого анализа. Для достижения поставленной цели решается ряд задач: в первом разделе проводится обзор существующих SCADA-систем, типичных архитектур и необходимых компонентов; во втором и третьем разделах анализируются вопросы безопасности SCADA-систем, уязвимости их компонентов; в четвертом разделе даются рекомендации по защите.

1x Обзор существующих SCADA-систем

SCADA-системы появились как результат интереса к проблемам построения высокоэффективных и высоконадежных систем диспетчерского управления и сбора данных. Прообразом современных систем SCADA на ранних стадиях развития автоматизированных систем управления являлись системы телеметрии и сигнализации [4].

Управление технологическими процессами на основе SCADA-систем стало осуществляться в западных странах в 80-е годы XX века. В Украине переход к управлению на основе SCADA стал осуществляться несколько позднее, в 90-е годы.

Практически все существующие SCADA-системы реализованы на платформах Microsoft Windows. Однако многие фирмы-разработчики одним из приоритетных направлений дальнейшего развития SCADA-систем считают реализацию SCADA на операционных систем реального времени, что позволит собирать более точную информацию о технологическом процессе. Мировые лидеры по производству SCADA-систем, согласно ARC Advisory Group, показаны на рис. 1. Лидирующими странами-производителями SCADA являются США (Wonderware – InTouch; GE Fanuc – Cimplicity, iFix; Rockwell Automation – RSView; ICONICS – Genesis), Германия (Siemens – WinCC) и Франция (Schneider Electric – Monitor Pro, Citect). Рынок отечественных SCADA-систем невелик и находится в начальной стадии развития. Из отечественных SCADA-систем можно выделить, например, систему «КОНТУР II», производимую ООО «SCADA-системы Украины». Проекты на основе этой SCADA-системы внедрены на многих промышленных объектах по всей территории Украины [5].

Российский рынок SCADA значительно шире и представлен следующими системами: Trace Mode (AdAstra), Круг-2000 (НПФ «Круг»), САРГОН (НВТ-Автоматика), Master SCADA (НПФ «ИнСАТ»). Последняя, например, выпускается серийно уже шесть лет и имеет множество внедрений на территории России и Украины [6]

Преимуществом украинских и российских SCADA-систем являются русскоязычная техническая поддержка пользователей и русскоязычная документация. Это актуально, поскольку далеко не все зарубежные системы имеют локализованные версии и русскоязычные учебные курсы. Еще одним преимуществом является относительно низкая стоимость по сравнению с зарубежными. Основным недостатком является то, что по функциональности и удобству использования такие SCADA-системы все же пока уступают зарубежным аналогам, хотя и наблюдается тенденция к значительному повышению их качества.

В целом же можно отметить, что по функциональным возможностям все SCADA-системы вполне сопоставимы. Технология программирования близка к интуитивному восприятию автоматизированного процесса [7]. Объектно-ориентированное программирование, используемое в большинстве пакетов, делает SCADA-системы достаточно легкими в освоении и доступными широкому кругу потребителей. SCADA-системы имеют открытую архитектуру [8] с возможностью дополнения функциями собственной разработки, открытый протокол для создания драйверов аппаратных средств автоматизации, развитую сетевую поддержку, доступность к базам данных и т.п.

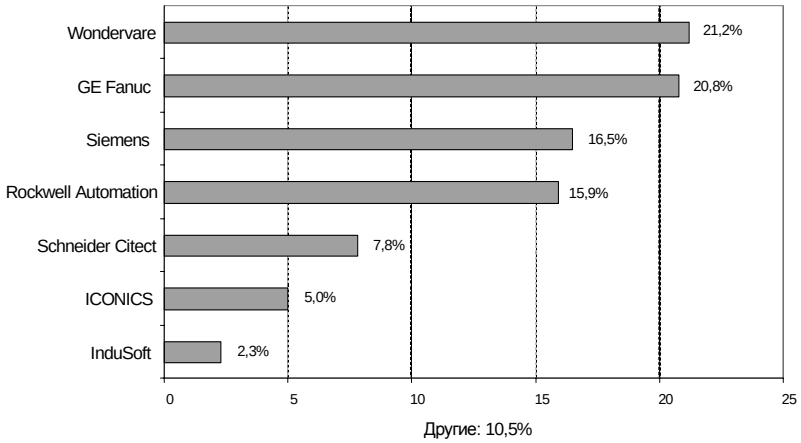

Рис. 1. Ведущие производители SCADA-систем

Все современные SCADA-системы включают следующие основные структурные компоненты – сервер, автоматизированное рабочее место, каналы связи (рис. 2).

Сервер осуществляет обработку поступающих данных в режиме реального времени. Автоматизированное рабочее место (АРМ) обеспечивает человеко-машинный интерфейс (ЧМИ), представляя собой пульт диспетчерского управления. В зависимости от конкретной реализации в системе может быть один или несколько объединенных в локальную сеть АРМов. Каналы связи SCADA необходимы для передачи данных от удаленных точек на центральный интерфейс оператора-диспетчера и передачи сигналов управления.

Ниже приведен далеко не полный перечень функций, выполняемых SCADA-системами (рис. 2): прием информации о контролируемых технологических параметрах от контроллеров, архивирование принятой информации, графическое представление хода технологического процесса в удобной для восприятия форме, прием команд оператора и передача их контроллерам управления, разграничение уровней доступа пользователей, регистрация событий контролируемого технологического процесса, оповещение эксплуатационного и обслуживающего персонала об обнаруженных аварийных событиях и т.д.

При выборе SCADA-системы, как правило, руководствуются следующими критериями [9]: надежность (отсутствие претензий пользователей, количество инсталляций в различных отраслях промышленности); обмен данными (поддержка стандартных сетевых протоколов и форматов данных, наличие встроенных драйверов к аппаратным средствам автоматизации, производительность); удобство работы (возможность автоматического построения проекта, универсальность и наличие стандартных языков математического описания данных и процессов, удобство пользовательского интерфейса); техническая поддержка (возможность поддержки от разработчиков); стоимость (зависимость стоимости системы от конфигурации, возможность получения новых версий и бесплатного обновления релизов, наличие бесплатной системы разработки).

SCADA-системы представляют собой достаточно сложный программный продукт, что, разумеется, делает их подверженными многим атакам. Анализ возможных уязвимостей SCADA-систем приведен в следующих разделах данной статьи.

2х Безопаснос2ь Sп ADA-сис2ем

С целью повышения удобства работы доступ к сетям SCADA-систем часто предоставляют из информационных сетей предприятия через, например, WEB-интерфейс. Это позволяет, не имея на своем компьютере установленной SCADA-системы и другого специального программного обеспечения, производить мониторинг состояния технологического процесса. Однако соединение технологической и информационной сетей вносит потенциальные уязвимости, которыми может воспользоваться злоумышленник для получения доступа к информации и реализации атак «отказ в обслуживании». В работе [10] именно отсутствие гарантии безопасности при передаче данных отмечено одним из основных недостатков применения WEB-технологий в SCADA-системах.

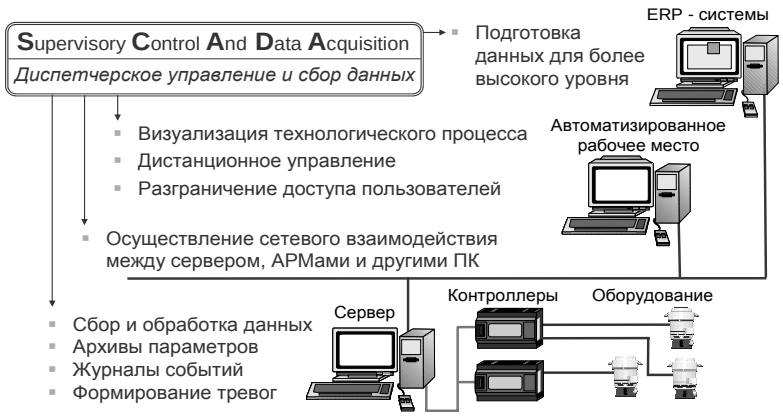

Рис. 2. Основные компоненты SCADA-систем и их функции

Сетевые протоколы современных SCADA-систем, возможные атаки, рекомендации по защите рассмотрены в работе [11]. Над решением проблем безопасности сетей SCADA-систем плодотворно работает ряд организаций (Instrumentation Systems and Automation (ISA) Society, American Gas Association (AGA), IEC Technical Committee 57 и др.). Несмотря на значительное число выпущенных публикаций, далеко не все проблемы решены на данный момент.

В работе [12] отмечено, что технологии информационной безопасности SCADA-систем отстают на 5-10 лет от технологий других IT-систем. Это обусловлено рядом факторов. Во-первых, изначально SCADA-системы имели закрытые архитектуры и обеспечение безопасности возлагалось на фирменные протоколы передачи данных. После перехода к открытым системам вопросам обеспечения безопасности был определен недостаточный приоритет. Вторым фактором является сложность установки патчей и обновлений безопасности. Дело в том, что SCADA-системы предназначены для непрерывной работы в течение нескольких лет, а установка обновления может вызвать необходимость остановки/перезагрузки сервера.

Детальный анализ информационной безопасности отечественных SCADA-систем еще не проводился ввиду относительно малого количества внедрений. Однако по имеющимся данным следует отметить, что для отечественных разработчиков SCADA характерен принцип «функциональность над безопасностью». Иными словами, вычислительные мощности существующих систем используются для достижения максимальной функциональности, при этом вопросы обеспечения безопасности отходят на второй план.

По нашему мнению, для анализа безопасности SCADA-систем необходим комплексный подход, базирующийся на общепринятых методиках оценки [13,14], и, в частности, на применении F(I)MEA-технологии [15].

3. Уязвимость OPC-серверов

Для связи SCADA-систем с контроллерным оборудованием чаще всего используется спецификация OPC (OLE for Process Control). Спецификация OPC не привязана к конкретным устройствам, предназначена для облегчения взаимосвязи компонентов системы управления. Доступ к данным осуществляется через определенный набор сетевых интерфейсов. OPC позволяет контроллерному оборудованию АРМам, серверам производить обмен информацией.

Несмотря на то, что OPC является открытым протоколом с доступной бесплатно спецификацией, решение вопросов обеспечения безопасности вызывает определенные трудности у пользователей SCADA-систем. Отчасти это объясняется тем, что производители OPC-серверов не уделяют указанным вопросам достаточного внимания. OPC-серверы, как правило, поставляются с настройками, обеспечивающими максимальную производительность, а не безопасность. Кроме того, в эксплуатационной документации настройки безопасности освещены недостаточно или же вообще не рассматриваются.

В конце 2006 – начале 2007 года компанией Neutralbit проводилось тестирование протокола OPC на подверженность уязвимостям, результатом которого стал ряд публикаций (например, [16], [17]). Согласно [16], более 20% рассмотренных OPC-серверов подвержены хотя бы одной из возможных атак. Это говорит о том, что безопасность OPC-серверов и, следовательно, SCADA-систем, находится под угрозой. Разумеется, такие результаты неприемлемы, поскольку большинство SCADA-систем управляют критическими объектами.

Подобные тестирования проводились совместной исследовательской группой British Columbia Institute of Technology, Byres Research и Digital Bond [18]. Согласно их данным, OPC используется не только в рамках локальной сети предприятия. Около 10% компаний используют OPC для получения информации и управлении системой через Internet. При этом потеря обмена по OPC приведет к значительным убыткам вследствие останова производства или некорректного управления системой более чем в 25% случаев.

Таким образом, интерфейс OPC является одним из наиболее уязвимых элементов SCADA-систем.

4. Защита SCADA-системы

В качестве примера комплекса мероприятий по обеспечению необходимого уровня защиты информации в системах управления производством можно рассмотреть методический материал Министерства энергетики США и Совета по защите критичной инфраструктуры при Президенте США «21 Steps to Improve Cyber Security of SCADA Networks» [19]. Данная брошюра содержит следующие указания и рекомендации:

- определите все точки входа в сеть SCADA-системы, оставьте только самые необходимые, оцените уровень информационной защищенности и по возможности усильте его;
- повысьте безопасность сети SCADA-системы при помощи отключения всех необязательных сетевых сервисов;
- не рассчитывайте на то, что секретные фирменные протоколы передачи данных являются гарантией защиты вашей системы;
- активируйте все возможности по защите информации, предоставляемые поставщиками программных и аппаратных средств;
- проверяйте каждое устройство SCADA, чтобы определить, встроены ли в него защитные

функции. Кроме того, заводские установки часто оптимизированы под максимальное удобство/быстродействие, а не под максимальную безопасность. Установите все настройки безопасности на максимально возможный уровень;

- установите жесткий контроль над всеми каналами, которые злоумышленник может использовать для нештатного проникновения в сеть SCADA-системы;
- внедрите системы обнаружения внешних и внутренних вторжений;
- проведите проверки физической безопасности и определите все удаленные терминалы, подключенные к сети SCADA-системы, чтобы оценить их безопасность;
- организуйте «диверсионные подразделения» для SCADA-системы, чтобы выявить и оценить возможные сценарии атаки на систему.

Украинского или российского аналога данной публикации пока не выпущено.

Мы предлагаем дополнить рассмотренный выше комплекс следующими мероприятиями:

- установка антивирусного программного обеспечения на все компьютеры системы с возможностью обновления антивирусных баз;
- организация защиты от «неправильных действий» SCADA-систем на уровне управляющих контроллеров путем внедрения в них дополнительного кода, проверяющего корректность поступающих от SCADA-системы данных.

Второй способ является достаточно перспективным и позволит значительно повысить гарантоспособность SCADA-систем.

Выводыя

SCADA-системы позволяют разрабатывать автоматизированные системы в распределенной, как правило, клиент-серверной архитектуре.

Большинство SCADA-систем работает под управлением ОС Windows в режиме «мягкого» (псевдо-) реального времени.

Основными составляющими SCADA-систем являются диспетчерский пункт управления (АРМ), подсистема получения и архивирования информации (Сервер), коммуникационные средства (сетевые протоколы, интерфейсы обмена данными). Любой из этих элементов может быть подвержен атаке злоумышленника и, соответственно, должен быть защищен. Однако вопросы информационной безопасности современных SCADA-систем все еще недостаточно проработаны и требуют решений.

Одним из вариантов решения рассмотренных проблем предлагается защита от «неправильных действий» SCADA-системы, подвергшейся атаке злоумышленника, на уровне управляющих контроллеров.

Списокяли2ера23рыя

1. *Кузнецов А. SCADA — мифы и реальность // Промышленные и встраиваемые системы. – 2001. – № 19.*
2. *Локотков А. Что должна уметь система SCADA // Современные технологии автоматизации. – 1998. – №3. – С. 44-46.*
3. *Robert Lemos. SCADA system makers pushed toward security. – [Электрон. ресурс]. – Режим доступа: http://www.securityfocus.com/print/news/11402.*
4. *Системы диспетчерского управления и сбора данных (SCADA-системы) // Мир компьютерной автоматизации. – 1999. – №3.*
5. *Никитин А.В. Отечественные SCADA-системы есть. «КОНТУР II» // ПИКАД. – 2004. – №4. – С. 32-38.*
6. *Аблин И.Е. Master SCADA – от простого к сложному // ПИКАД. – 2007. – №2. – С. 10-13.*
7. *Радкевич В. Опыт проектирования и внедрения систем управления // Промышленные АСУ и контроллеры. – 2006. – №2. –С. 10-16.*
8. *Куцевич Н. SCADA-системы, или Муки выбора // Промышленные и встраиваемые системы. – 1998. – № 32-33.*
9. *Деменков Н.П. SCADA-системы как инструмент проектирования АСУ ТП // Информационные технологии. – 2002. – №11. – С. 2-24.*
10. *Сухов С.А., Ухов В.И. Подходы к созданию АСУТП на основе WEB-технологий // Автоматизация и современные технологии. – 2006. – №10. – С. 24-28.*
11. *Vinay M. Igure, Sean A. Laughter, Ronald D. Williams. Security issues in SCADA networks // Computers & Security, 25 (2006). – P. 498-506.*
12. *Jason Stamp, Phil Campbell, Jennifer DePoy, John Dillinger, William Young. Sustainable Security for Infrastructure SCADA. – [Электрон. ресурс]. – Режим доступа: http://www.tswg.gov/tswg/ip/SustainableSecurity.pdf.*
13. *Общий подход к безопасности. – [Электрон. ресурс]. – Режим доступа: http://kiev-security.org.ua/box/12/110.shtml.*
14. *Александровская Л.Н., Аронов И.З., Елизаров А.И. и др. Статистические методы анализа безопасности сложных технических систем. – М., 2001. – 232 с.*
15. *Anatoliy Gorbenko, Vyacheslav Kharchenko, Olga Tarasyuk, Alexey Furmanov. F(I)MEA-technique of Web Services Analysis and Dependability Ensuring // Lecture Notes in Computer Science. – Vol. 4157/2006. , P. 153-167.*
16. *Lluis Mora. OPC Server security considerations. – [Электрон. ресурс]. – Режим доступа: http://www.neutralbit.com.*
17. *Lluis Mora. Security vulnerabilities in SCADA systems // SIC. – №71. – P. 98-100.*
18. *OPC Security Whitepaper. – [Электрон. ресурс]. – Режим доступа: http://www.byressecurity.com.*
19. *Steps to Improve Cyber Security of SCADA Networks . – [Электрон. ресурс]. – Режим доступа: http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.*

Поступила в редколлегию 11.10.2007

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. Петра Василенко, Харьков.