УДК 681.51

# СОВРЕМЕННЫХ SCADA-СИСТЕМЫ: СТРУКТУРА, ВОЗМОЖНОСТИ, ПРОБЛЕМЫ

*Татолов Е.Р.*
*Донецкий национальный технический университет*

Автоматизация деятельности современных предприятий лежит в четком разделении базовых функций технологической обработки между отдельными, достаточно независимыми уровнями. Каждый уровень имеет свое значение в производственном процессе и интерфейс связи с другими уровнями, для унификации деятельности предприятия в целом.

Производственные процессы требуют настолько сложных и трудоемких функций контроля, что зачастую они возлагаются на специальные автоматизированные системы контроля, работающие в реальном времени и позволяющие адекватно отражать значения важнейших параметров технологического процесса. Нетрудно заметить, что автоматизированная система контроля должна осуществлять:

- сбор данных на каждом уровне производственного процесса;
- управление производственным процессом в целом;
- предоставление удобного интерфейса для обслуживающего персонала.

Кроме того, необходимо отметить, что неотъемлемой частью крупных предприятий является их территориальная распределенность. Поэтому возникает необходимость в применении телеметрии для функционального объединения оборудования и систем, находящихся на значительном расстоянии. При этом, такое расстояние может варьироваться от нескольких метров до нескольких километров. Телеметрия является еще одним фактором работы системы контроля.

В качестве таких автоматизированных систем контроля могут выступать SCADA-системы (Supervisory Control And Data Acquisition – Диспетчерский контроль и сбор данных). SCADA-системы являются сложными программно-аппаратными комплексами, которые выполняют сбор информации и передачу ее к центральному звену, практически любой анализ технологических параметров и управление ими, а также вывод данных на произвольное число мест операторов [1].

SCADA-системы обладают некоторым числом удаленных терминалов, в английской терминологии называемых RTUs (Remote Terminal Units), которые занимаются сбором данных в контролируемой области и отправлением их на главную станцию, через коммуникационную систему. Коммуникационная система определяет путь между главной станцией и RTUs. В качестве этой системы могут выступать шины, оптоволоконные кабели, радиоканалы, телефонные линии. Главная станция отображает полученные данные на терминалах пользователей и дает возможность операторам их контролировать. В общем случае в SCADA-системах выделяют пять уровней иерархии аппаратуры [1]:

1. инструментарий области контроля;
2. RTUs;
3. система коммуникации;
4. главные станции;
5. компьютерные системы обрабоки данных.

Программное обеспечение SCADA-систем обладает следующими особенностями [1]:

1. удобный пользовательский интерфейс;
2. сигналы тревоги;

3. масштабируемость;
4. наличие баз данных;
5. использование сетевых технологий;
6. встроенные языки программирования;
7. клиент-серверная архитектура.

Например, существуют и поддерживаются программные продукты InTouch, Citect, FIX, Genesis, Factory Link, RealFlex, Sitex, TraceMode, Cimplicity, САРГОН.

Наиболее общая структурная схема типичной SCADA-системы, взятая из [1] с изменениями, приведена на рис. 1.

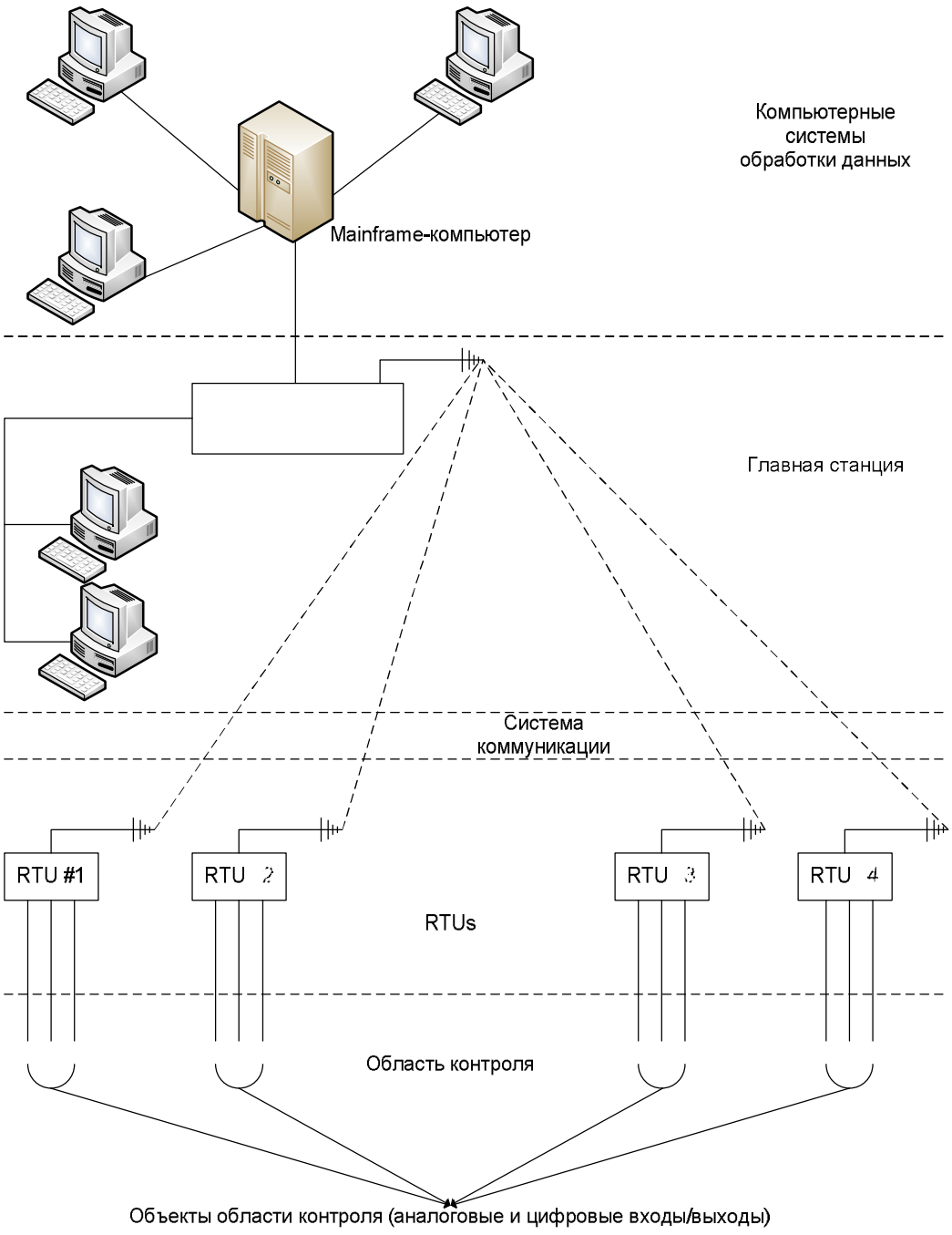


Рисунок 1 – Структурная схема типичной SCADA-системы

К одним из самых мощных средств SCADA-систем относятся встроенные языки программирования, предоставляющее разработчику гибкий инструмент для разработки сложных приложений. Первые версии SCADA-систем либо не имели подобных языков, либо эти языки реализовывали небогатый набор функций. В современных версиях систем функциональные возможности языков становятся существенно богаче. Явно выделяются два подхода:

1. ориентация встроенных языков программирования на технологов. Функции в таких языках являются высокоуровневыми, не требующими профессиональных навыков программирования при их использовании;
2. ориентация на системного интегратора. Языки программирования при таком подходе являются, как правило, Basic-подобными и требуют определенного уровня программистского мастерства [2].

Базы данных – неотъемлемая характеристика SCADA-систем. Однако, с точки зрения организации информации, промышленная автоматизация несколько отстает от автоматизации других задач. В [2] приведено несколько основных причин такого отставания:

1. производственные процессы генерируют данные очень быстро;
2. обьем производственной информация очень велик;
3. традиционные языки запросов не подходят для обработки временных или периодических данных.

SCADA-системы взаимодействуют со многими внешними факторами. Такие факторы приведены на рисунке 2 [3].

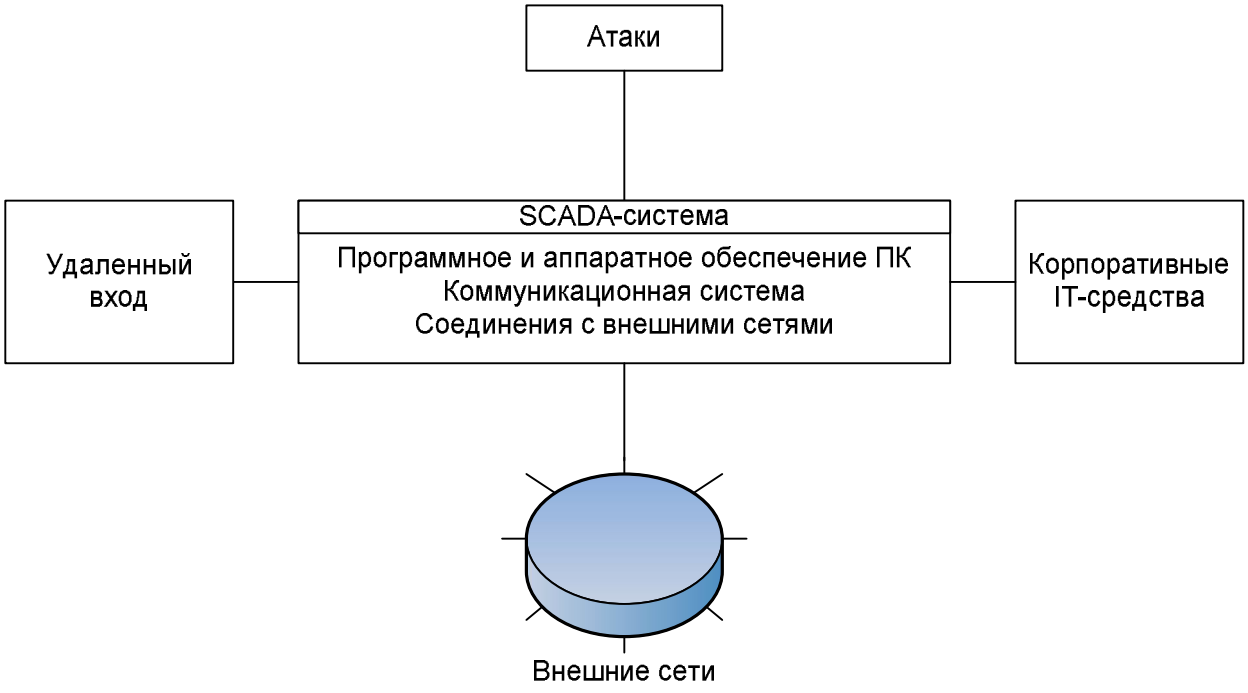


Рисунок 2 – Внешние связи SCADA-системы

SCADA-система связана со внешними сетями, корпоративными IT-средствами и внешними, потенциально опасными точками входа, например, модемами. Так как используются стандартные аппаратные и программные решения, то они могут быть подвергнуты атакам, которые ранее имели место для обыкновенных ПК.

Важнейшим фактором функционирования SCADA-систем, тесно связанным с их внешними связями, является безопасность данных. Этому вопросу целиком посвящена

работа [3]. В частности, в ней выделяются основные потенциально опасные компонеты системы:

1. соединения с дополнительными, возможно уязвимыми сетями;
2. использование стандартных аппаратных платформ с известными уязвимостями;
3. использование стандратных программных платформ с известными уязвимостями;
4. противоречие между требованиями безопасности данных, которые могут приводить к задержкам, и требованиями функционирования реального режима.

**Литература**


[1] Bailey D., Wright E., Practical SCADA for Industry – Oxford: ELSEVIER, 2003. – 288 p.: il.

[2] Андреев Е.Б., Куцевич Н.А., Синенко О.В. SCADA-системы: взгляд изнутри – М.: Издательство «РТСофт», 2004. – 176 с.: ил.

[3] Krutz R.L. Securing SCADA Systems – Indiana: Wiley Publishing, 2006. – 218 p.: il.