SCADA Systems – Looking Ahead

Control Microsystems White Paper August 2005

This white paper provides insight into the evolution of the modern SCADA system and looks to the very near future by discussing such timely topics as:

- Improving system efficiency and security
- Managing field data and
- Open standards

CONTROL MICROSYSTEMS
SCADA products...
for the distance

Author: Peter King

Date: August 2005

SCADA Systems – Looking Ahead

Supervisory Control and Data Acquisition (SCADA) systems are used in a wide range of applications to provide monitoring and control of remote equipment and assets. A SCADA system's primary function is to transfer and present information to/from a range of sources and locations, while ensuring that data integrity and appropriate update rates are maintained.

SCADA System Evolution

SCADA systems have evolved from early telemetry systems that used tone-based modulation techniques to transfer analog and digital values at low data rates over telephone lines and radio links. Modern SCADA systems are able to provide 'near real-time' updates from thousands of Remote Terminal Units (RTUs) that are often spread over large geographical areas, using a range of secure communications media, to multiple 'users' that may also be remotely located.

Until recently SCADA systems were most often used in a reactive manner to identify system faults as they occurred and to record system data and events for later analysis. Present demands on all types of businesses for increased efficiencies and particularly on utility companies for increased security of their assets and products means SCADA systems must now be pro-active and include a lot of data management and security functionality that allows problems to be avoided - rather than just recorded.

Improving Efficiency and Security

Increasing the efficiency of a business and the security of a SCADA system both require increased monitoring. Increasing the security requires more than removing access to the system from the Internet! Increased monitoring with greater security creates various challenges to SCADA system users and system vendors that include:

- Managing larger data traffic loads due to increased monitoring of local and remote assets,
- Implementing standby/backup servers and communications links for critical system infrastructure,
- Securing the communications traffic between various devices and users,
- Restricting and authenticating access to both the system and the field assets,
- Management of on-line configuration processes to avoid induced system errors (most system failures occur when system maintenance/upgrades are being deployed),
- Managing the collected data for display, storage and access by users and other business systems, including event/alarm escalation (important events must receive attention promptly).

As an example, it is no longer acceptable to simply monitor the level of a suburban water reservoir to be assured that the operational state is normal. Now the SCADA system monitoring must also include the physical security of the location - using video surveillance and intruder detection, the water quality - using online analysers, the time in storage (age of the unused water) - to avoid bacterial contamination, and the 'health' of the communications link and field equipment.

Managing Field Data

In the past, field devices such as RTUs collected analog and digital input data from various transducers and status switches and stored values in a data table that was routinely uploaded by the SCADA host for further processing via a communications link. As more values were read by each RTU and more RTUs were added to the system, update rates slowed.

Latest generation RTUs use secure protocols and data transfer philosophies that move data based on priority - and in most cases, only if it has changed. This frees up communications links and allows important events to be sent from the RTU to the SCADA host when they occur. Data values include data quality flags, a time stamp with millisecond resolution to indicate when the event occurred and a class/priority to indicate how it should be handled. The use of time stamped data has two important benefits - it allows less important data to be buffered by the RTU until it is convenient for the SCADA host to receive it, and it also allows the system to tolerate failure of the communications links and/or use non-continuous type communications links such as dialup or cellular. When the SCADA host receives time-stamped data, it is able to accurately build/replay trend and event files based on actual time of occurrence, rather than time of receipt of the data.

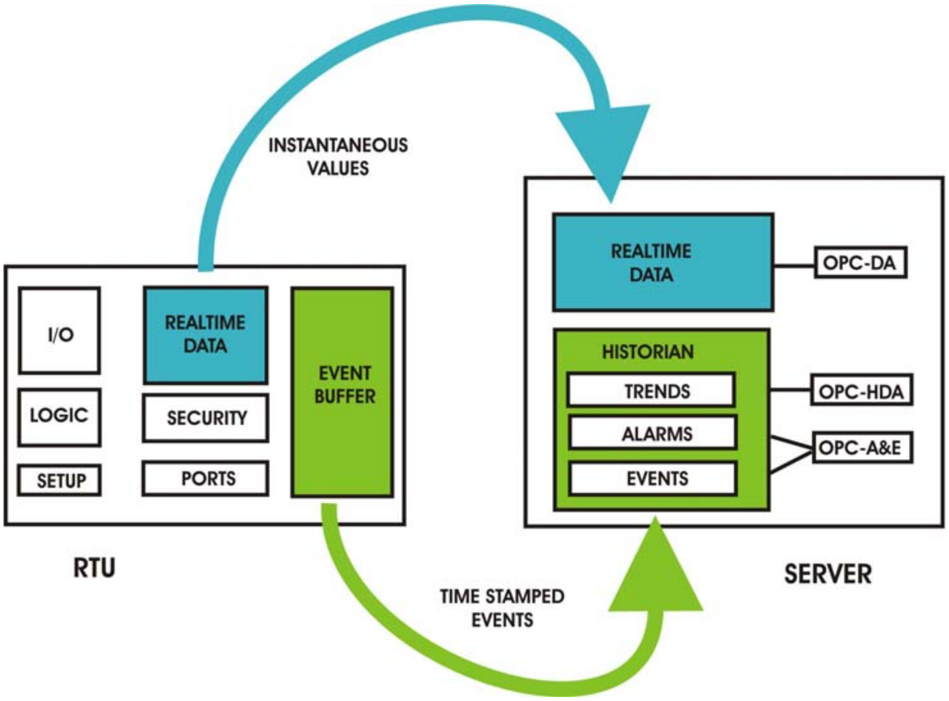

Figure 1. Data Transfer Concepts – RTU to Server

SCADA System Standards

Development of SCADA standards by industry user groups and international standards bodies has allowed increased 'interoperability' of devices and components within SCADA systems. Open protocols like DNP3 allow equipment from multiple vendors to communicate with the SCADA host and system 'peers' while standards defining programming methods like IEC 61131-3 allow systems engineers to re-use code for logic operations and move easily between configuration interfaces. The American Gas Association has released AGA-12 a report defining encryption and authentication methods for use with the DNP3 SCADA protocol. The power industry is developing the IEC 61850 standard that defines SCADA communications and device objects in substations.
At the SCADA host level, the OPC (Open Connectivity via Open Standards) series of standards specifications have been widely accepted. The OPC Foundation comprises of a large group of vendor representatives dedicated to ensuring interoperability in industrial automation systems. OPC standards include OPC-DA (Data Access), OPC-AE (Alarms and Events) and OPC-HDA (Historical Data Access). The latest generation of SCADA system hosts use these OPC standards to provide advanced connectivity to user clients.

Modern SCADA System Architecture

The architecture of a modern SCADA system includes object data structures and a range of system security, availability and WAN features in-built rather than 'tacked on'. Object based data structures allow rapid deployment and updating of 'instances' of plant and equipment. The objects represent devices that may be simple such as a motor overload status, or they may be complex and contain multiple attributes such as a pump station. The security features manage access to data based on privilege levels that can be assigned to both the data objects and the user/s. Availability features relate to inherent support for redundant servers and redundant communications links. WAN features include ‘clustering’ that allows user clients to connect concurrently to multiple servers, as local or web clients and redundant server operation via WAN connections.

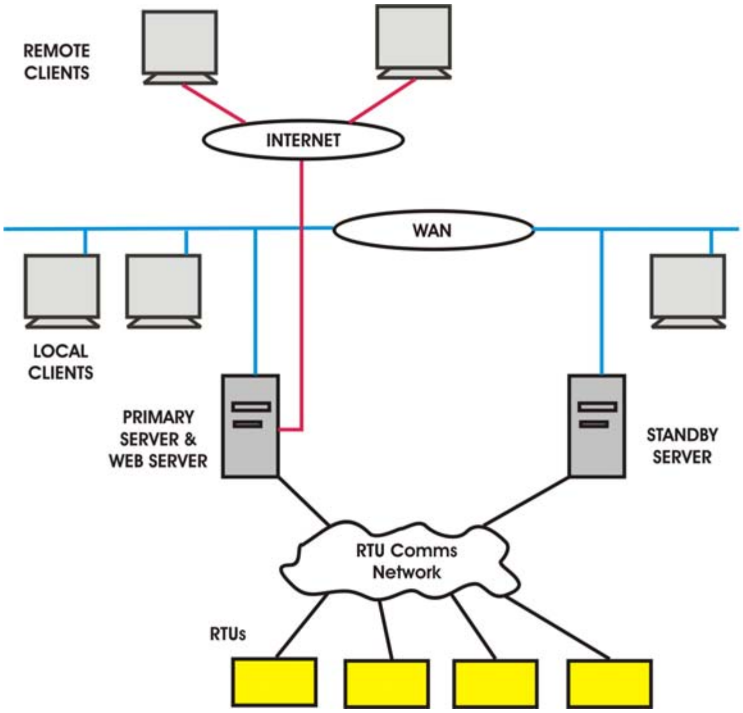

Figure 2. Modern SCADA System Overview

Looking Ahead

The development and adoption of a range of standards to ensure secure and open connectivity, that allow interoperability of SCADA components and devices from multiple vendors is not enough to ‘future-proof’ a SCADA system! As systems grow larger and more complex the management and administration of the SCADA system itself becomes very important. Latest and next generation SCADA systems need to do more than gather and present data - they must also manage the expansion, maintenance and access for all parts of the system.

Peter King
Manager, Asia Pacific Region
Control Microsystems
pking@controlmicrosystems.com

Contact Us

Name:	**Martin Chartrand**
Address:	**Control Microsystems** **Corporate Headquarters** **48 Steacie Drive** **Ottawa, Ontario, Canada,** **K2K 2A9**
E-mail:	**mchartrand@controlmicrosystems.com**
Tel: Toll Free:	**1-888-CMSCADA (1-888-267-2232)** **1-613-591-1943 xt. 254**
Fax:	**(613) 591-1022**