

The Top Three Criteria To Look For In Your Next Water/Wastewater SCADA System

By Hany Fouda, VP of Marketing, Control Microsystems Inc.

Water utilities have been using Supervisory Control and Data Acquisition (SCADA) for many years during which SCADA systems have evolved from simple tone telemetry to web-centric solutions. A SCADA system's primary function is to monitor and control the conditions of remote assets, such as pumps and lift stations, distribution networks, and treatment plants while ensuring data integrity, overall system visibility, and security. If you are expanding, upgrading, or developing a new SCADA system, selecting the right hardware and software components can help you cope with ever-changing demands in securing your infrastructure and improving data collection and reporting.

Here are the top three criteria to focus on when specifying an advanced SCADA system:

1. Intelligent Field Controllers

Everyone claims that they offer intelligent hardware, but are they really that "smart"? Remote programming and configuration over the SCADA network is no longer an indication of smartness.

An integrated hardware and software solution that is able to detect and adapt to changes as they happen across the infrastructure represents the intelligence many utilities are looking for. For example, bringing a new remote pump station online in a traditional SCADA system would require manual downloading of the control logic application, customizing the HMI/SCADA host software at the central monitoring station to accommodate the new site, and manually integrating the pump station in all reports. An intelligent SCADA system has the ability to detect the newly added remote controller and automatically download the proper control application, provided that a communication link is available. Using templates, the existing screens and reports can be easily adapted to integrate the new site.

Other daily events such as losing the communication link between the remote controller and the control center would be immediately detected by the remote controller. To mitigate the risk of losing critical data and facing possible fines from regulatory agencies, the controller will log and time stamp data in its non-volatile memory during the time communication is down. Once the communication link is re-established, the controller will automatically upload the logged data to the SCADA host software to populate trend and event files based on actual time of occurrence rather than time of receipt of the data. If the communication loss persists for a longer period of time, the controller may automatically report critical data to an alternate server or even a mobile operator.

2. Tight Security Suite

Water utilities, large and small, are part of the national critical infrastructure. Cyber security threats against this infrastructure can take different forms:

- Potential destructive cyber malware including viruses, Trojans, and worm attacks.

- Network spoofing and “denial of service” threats causing network performance implications.
- Confidentiality breach with eavesdropping and password cracking.
- Data integrity including data tampering and packet modification.

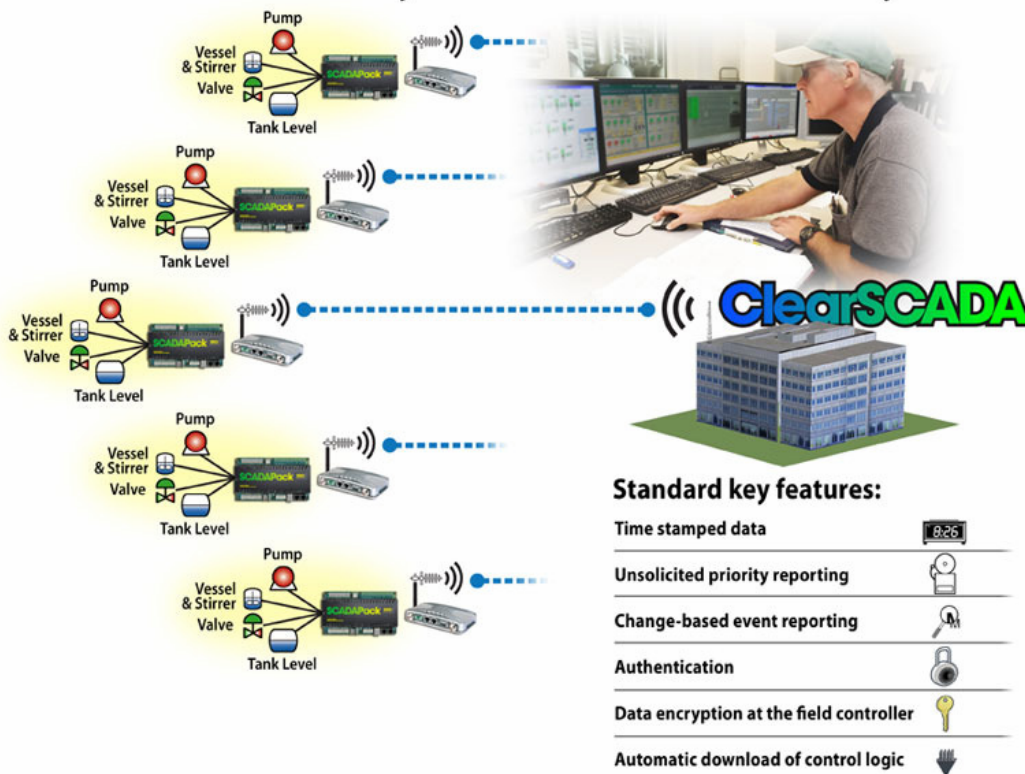
Intelligent field controllers are now capable of encrypting data before it is transmitted over the communication link using industry standard, government-grade encryption algorithms. The controller can also authenticate messages received from external devices and reject those from unidentified sources. This protects the infrastructure from eavesdropping, interception, and intrusion attacks.

3. Integrated Host Software







An integrated host software is designed from the ground up to manage small and large Wide Area SCADA systems and address critical issues such as unreliable communication links, security, data integrity, and ease of deployment. It includes, as a standard, all the needed components required to effectively operate a SCADA system such as:

- Alarm redirection engine to alert mobile users of operation disruptions via email and mobile phones;
- Efficient trending and audit trail engines that are capable of dealing with communication link interruptions and data retrieval delays;
- Integrated reporting engine capable of meshing-up data from multiple sources to produce operation and compliance reports with ease.

Advanced SCADA System from Control Microsystems



Standard key features:

- Time stamped data 
- Unsolicited priority reporting 
- Change-based event reporting 
- Authentication 
- Data encryption at the field controller 
- Automatic download of control logic 

For the past 30 years, Control Microsystems has been the leader in developing intelligent field controllers for telemetry, SCADA, and remote asset monitoring. The Control Microsystems SCADAPack Series of rugged, cost-effective, programmable field controllers is designed specifically to operate in harsh remote environments. Control Microsystems' offering also includes ClearSCADA, an advanced SCADA Host Software platform. Even though SCADAPack controllers and ClearSCADA software can be integrated with a variety of third party HMI/SCADA software and PLCs respectively, an integrated solution combining the two products drives substantial cost savings and dramatically increases system efficiency.

The SCADAPack E-Series is a line of remote field controllers that has an embedded historian allowing time-stamped event logging for extended periods of time. Events can be logged in the unit's internal memory and are easily accessible to the user. With multiple serial and Ethernet ports on-board, the SCADAPack E-Series is well-suited for concurrent communications with multiple field devices. It can simultaneously report to several master servers based on user preferences. Additionally, it can share information with other peer units in the field, thereby reducing network traffic to the main server and increasing the system's overall reliability. Control algorithms are developed using an IEC 61131-compliant programming package and downloaded to the field controller remotely over any communication link.



The SCADAPack E-Series uses a secure, standard communication protocol and data transfer mechanism that transfers the data based on priority and event changes. This frees up communication links to be used for other demanding services such as remote asset video surveillance. 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 by the SCADA host.

To realize the concept of Intelligent SCADA, ClearSCADA was designed from the ground up to manage small and large Wide Area SCADA systems and address critical issues such as unreliable communication

links, security, data integrity, and ease of deployment. The product is optimized for low and high bandwidth communication links over public networks, such as dial-up landlines, mobile networks, and WiMAX. It is also well-suited for private serial and Ethernet radio networks. Extensive diagnostics features are available for monitoring the performance of the communication network. ClearSCADA supports main and standby communication links to remote devices for uninterrupted monitoring and control.

Data integrity is maintained across the system as a result of its inherent ability to synchronize historical events in its database after a communication loss with the intelligent field controllers, such as SCADAPack E-Series. Since all data is time stamped in the intelligent field controller, less important data can be buffered by the controller until it is convenient for the SCADA host to receive it. In addition, time-stamped data allows the system to tolerate failure of the communication links. Eliminating gaps in data helps users to comply with regulatory requirements by providing accurate reporting and maintaining a high level of data availability.

Multiple security models are available in ClearSCADA. Security is configured to the object level where a wide range of permissions are applied to discrete system points. For example, depending on the permission policies, a group of users may see details on a screen that are not available to another group that has a lower level of security permissions. This level of intelligence and flexibility allows users to offer access to a much larger group of internal and external stakeholders without compromising system security and integrity.

Furthermore, to reduce deployment time and ongoing maintenance, ClearSCADA offers a zero-configuration Web client that is ideal for monitoring and controlling the SCADA system through a standard web browser. All features, including full mimic display support, control and trending capabilities, and alarms and reporting, are made accessible through a secure SSL connection that is managed by security login privileges.

For more information on Control Microsystems' products, please visit www.controlmicrosystems.com

About the author:

Hany Fouda is the VP of Marketing at Control Microsystems Inc. He holds a Masters degree in Engineering from Carleton University, Ottawa, Canada and has over 20 years experience in industrial automation, SCADA, and telecommunications.