The Future of SCADA

Blair P. Sooley

"There hasn't been any real advancement in SCADA technology for 20 years"

– Consulting Electrical Engineer, Georgia, USA

Today, both public and private sector organizations are under greater pressure to provide increasing quality of service under ever-tightening budgets. Also, governmental regulations require stricter monitoring, greater energy efficiencies and detailed reporting. In this challenging environment, the organization's supervisory control and data acquisition (SCADA) system offers new and exciting means to wring additional benefits out of a proven workhorse.

To understand the potential of SCADA, we must look beyond its traditional roots as a simple human-machine interface (HMI), a method to convey low-level process data to the operations team. Indeed, some see the user interface alone as the SCADA system, with little understanding of its many vital components (instrumentation, control devices, software algorithms, communications and integration services.)

While the HMI continues to be an integral part of the system, its relative value as a SCADA component has been declining continuously as new value-added benefits have become financially more attainable. As a result of this increase in affordability, larger and more complex SCADA systems have arisen.

A system that once displayed 500 raw values now includes thousands of raw, calculated, and summary values. Soon operators will be unable to synthesize such a large amount of data to make decisions. With this problem growing in intensity each year, the need for ease-of use has never been greater.

SCADA of the Future

In a darkened control room, a single green light illuminates the HMI of the future. Below this light, a few simple statements convey summary information to the operator: "There are no alarms." "All maintenance is complete." "System is running at peak efficiency." Suddenly, the light turns red. The summary statements have changed: "Alarm: Station 4 level readings are invalid." "Maintenance dispatched. Estimated service interruption is two hours." "Pumping algorithms adjusted to compensate."

This sounds like science fiction: the utopian world of SCADA. A system-wide control loop reacts to alarms automatically and tunes itself constantly, based on high-level operational set points and real-time process response. Users are freed from day-to-day operational duties to focus on systemic improvements: developing new power efficiency models, tuning the SCADA's decision-making criteria, and working with the planning team on strategic initiatives. The future may be closer than we think.

Evolution

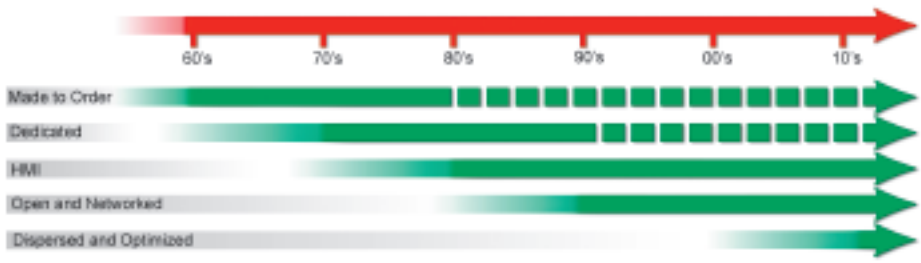
To understand how such a level of future SCADA sophistication is possible requires only a simple analysis of our progress to date. Since the introduction of computerized control systems in the 1960s, five generations of SCADA evolution can be clearly defined, as shown in Figure 1.

Generation 1: Bespoke (Made-to-order beginning approximately 1960s)

Made-to-order SCADA systems were developed for special-purpose applications such as NASA's Johnson Space Center launch system in Houston. In the 1960s, Houston had a problem: The Space Center had a large number of essential variables to monitor, and there existed no off-the-shelf technology capable of providing the functionality required.

In response, NASA developed a one-time solution of relatively low capability compared to today's standards. Such systems combined the latest in sensors, user interfaces, and direct-wired controls. Large numbers of operators were required to extract raw data and perform manual calculations. The Johnson launch center control system was replaced in 1997 for $250 million (NASA, unknown date), offering some appreciation for the original price paid in 1965.

Figure 1: Chronology of generational evolution in the SCADA industry.



Generation 2: Dedicated (widespread adoption in 1970s)

A new generation of control emerged in the 1970s with the introduction of distributed control systems (DCS), including the Honeywell TDC 2000 and Bailey Net 90. These systems reduced design and development time by providing common components that could be installed and configured by highly trained specialists.

Instrumentation and control device concentrators on the plant floor significantly reduced hard wiring. High-speed process loop control was taken on by the highly coupled elements of the DCS, allowing a smaller operations team to manage larger systems. While still largely unaffordable to most, the resultant drop in overall costs made control systems economically feasible for a growing number of companies.

Generation 3: Human Machine Interface (widespread adoption in 1980s)

With the general availability of computers

Continued on page 30

Blair P. Sooley, M.B.A., P. E., is a pre-sales engineer with Trihedral Engineering Limited, headquartered in New Bedford, Nova Scotia. *This article was presented as a technical paper at the Atlantic Canada Water & Wastewater Association Annual Conference in 2009 and was subsequently published in Water Online, a digital marketplace newsletter for professionals in the water industry.*

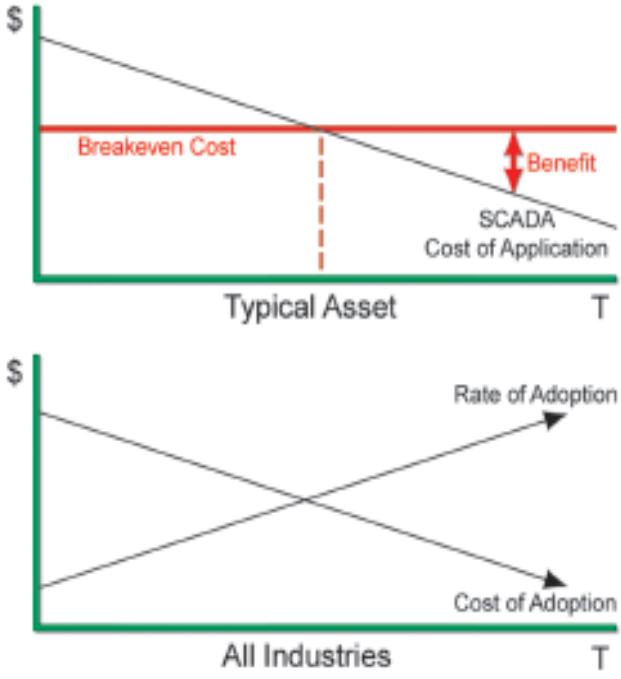


Figure 2: Top—Reduction of SCADA costs over time will eventually make SCADA feasible for any asset. Bottom—Industry adoption of SCADA will continue to increase over time as the cost of adoption decreases.

Continued from page 28

and programmable logic controllers (PLCs) in the 1980s, there came a revolution against the DCS. Control components could now be installed, configured, and maintained by independent systems integrators. Lower-cost PLCs could be dedicated to, and mounted near, specific process equipment, further reducing expensive wiring.

High functional programming languages allowed PLCs to provide local equipment control and interact with one another on proprietary networks, while operators viewed system data on computer screens and adjusted process set points. Remote telemetry units (RTUs), based on the PLC platform, allowed local control of remote assets while data gathering and supervisory control activities utilized low-speed radio channels. With the proliferation of these changes, SCADA became an affordable option for organizations of all sizes.

Generation 4: Open & Networked (widespread adoption in 1990s)

The adoption of open communication standards during the 1990s offered organizations a myriad of SCADA component choices. All components, including integration services, became generally available from a growing number of providers. Prices dropped dramatically for instrumentation and computers, decreasing by an order of magnitude in some cases. The emergence of cellular, satellite, and other communication options provided new means to connect more geographically dispersed devices, while Ethernet and common interface protocols provided a platform to leverage SCADA data in disparate business systems (e.g. GIS, ERP).

Generation 5: Dispersed & Optimized (emerging)

As new communication options continue to arise and existing choices become more affordable (e.g. municipal WiFi, cellular IP), the ability to accumulate data from dispersed locations for real-time, high-level decision making will become correspondingly more affordable. Interconnecting autonomous plants and other assets into a centralized-management/decentralized-control paradigm will provide a platform for enterprise-wide cost management without intrusive operational micro-management.

This 'Mothership' approach will be further aided by increased miniaturization of telemetry devices, reduced costs for basic instrumentation, and the increased availability of highly stable server and networking equipment. As a result, systems will become smarter, incorporating rule-based decision-making functionality to help users deal with the increased data load.

Industry Trends

A review of SCADA evolution illuminates three important trends:

1. The incremental cost to apply SCADA to additional assets is decreasing.
2. The amount of data being gathered is increasing.
3. Basic logic and control is becoming decoupled from the operator, reducing the relative importance of the HMI component of SCADA software.

As Figure 2 demonstrates, decreasing costs are the primary driving factor, resulting in the increased adoption of SCADA. In turn, increased adoption has led to a need to push direct machine interface further from the operator.

For example, a SCADA application installed at Air Products and Chemicals of Allentown, PA uses Trihedral's Visual Tag System (VTS) software to accumulate nationwide real-time data from 6000 tanks. Product usage history is used to forecast refill date ranges for each tank. The information is communicated to the organization's SAP enterprise resource planning system. It is then summarized to schedule delivery routing to cut down product waste and make best use of the company's fleet of $1 million cryogenic gas delivery trucks. The reduced cost of monitoring these widely dispersed assets made the application feasible, but at this time the company is still using human-based decision making to control daily functions.

Such geographically widespread asset management is not limited to million-dollar assets. As the cost of SCADA continues to decline on a per-asset basis, low cost assets such as vending machine inventories, department store inventories, restaurant grease traps, and many other items that could not be monitored feasibly in the past will become increasingly easier to incorporate into the SCADA model. One can only imagine a future in which telemetry devices as small as a grain of sand are used as locating beacons on personal jewelry.

From Obstacles Arise Opportunities

To expect that entry into the utopian SCADA world would be without peril would be naive. Indeed, the following sizable obstacles lay in the path ahead.

Legacy & Proprietary Systems

Legacy SCADA systems are those that continue to be used despite relatively poor performance and a lack of compatibility with other systems. Often, replacing hardware components is an expensive, unpalatable option for the customer. Proprietary SCADA systems tie the customer to one specific control device manufacturer, creating a difficult negotiating position for the customer during future purchases.

For these systems, the increased flexibility of new computer hardware and SCADA software offers an opportunity. While most SCADA software products support industry-standard control protocols, products such as VTS also support protocols for proprietary and legacy control products. These disparate systems can now be integrated into the same centralized management model while allowing customers the time to develop a plan for migration away from legacy and proprietary SCADA.

Continued on page 32

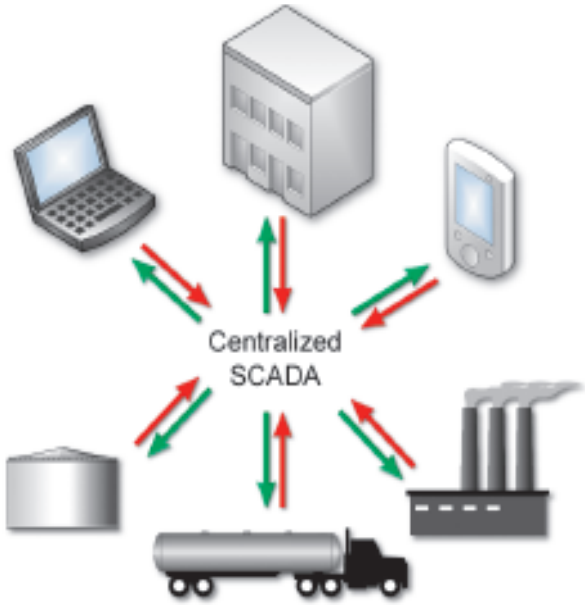


Figure 3: Simplified integration allows incorporation of more disparate systems and assets into a centralized SCADA.

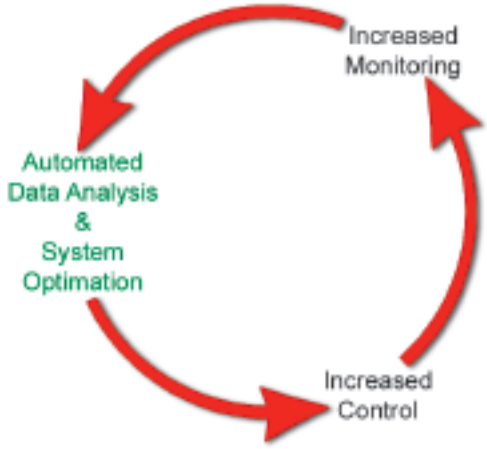


Figure 4: Increased monitoring and control requires greater automation tools in SCADA software.

Continued from page 30

Security

The increased use of open standards for communications and interconnectivity has led to security concerns. New technologies leveraged for remote SCADA access, including wide area networks (WANs), wireless application protocol (WAP), and the myriad of wireless Ethernet connectivity options have opened the door for hacking and other malicious activity.

In response, the traditional divide between SCADA administration and information technology (IT) has narrowed, and will continue to do so. SCADA systems that enable remote connectivity must support the security paradigms of the IT industry, such as secure socket layer (SSL), demilitarized zoning (DMZ), virtual private network (VPN) and firewalls.

Also, industry specific compliance with government standards such as the Critical Infrastructure Protection (CIP) (NERC, various dates), the Roadmap to Secure Control Systems in the Water Sector (WSCCCSWG, 2008) and Title 21 CFR Part 11 (FDA, 2003) suggest the importance of reliable, safe service to those who depend on SCADA. Adhering to these regulations will drive the need for integrated configuration management and traceability tools, methods traditionally imposed by IT.

The most reasonable response to security risk is not a policy of elimination, but rather mitigation. No SCADA system can ever be perfectly secure, and to eliminate all risks, no matter how small, would be to negate all emerging technological advances in the industry and ultimately eliminate the SCADA system altogether. As such, the cost-benefit ratio needs to be considered carefully.

Costs for security are of two forms. First, there are the direct costs of implementation and maintenance. Second, it is the cost of lower functionality of the SCADA system that is the subject of the security. Removal of convenient access to the SCADA system can sometimes be so detrimental to the overall efficiency of the operation that it is not justified to introduce excessive security measures for the benefit of a very low security risk.

An example might be a power plant in Brazil that has implemented an IT policy barring remote access to the system in order to eliminate potential hacking. As a result, issues detected within the system require a troubleshooting team to travel to the site for debugging, potentially resulting in days or weeks of service interruption.

Had this system been designed so that the operator could allow remote access when necessary and otherwise bar such access, the problem may have been diagnosed from an offsite location within hours and fixed remotely. In this case, an excessively strict IT policy applied without reasonable due diligence has eliminated a relatively low risk at excessive cost to the organization.

Increased Size means Increased Complexity

SCADA systems of the future will be more complex as the need to support much larger systems continues. Historical data storage is unlikely to be a cause for concern because computer drive space, like other components, will continue to erode in price. Thus, the challenges of the future lay instead in device connectivity and system integration costs.

Device connectivity represents a monumental challenge. The lessons of the past suggest new products and communication protocols will continue to emerge in concert with a variety of new communications mediums.

SCADA not only must be able to support the many new products and protocols, but also must be able to tune communications to combine low- and high-cost communications mediums in a cost-effective manner. Telemetry and PLC base-stations will disappear as the SCADA software applies smart logic to manage the increasingly complex asset polling and report-by-exception alarm handling.

As SCADA systems increase in size and interconnectivity, new components such as networking equipment, self-aware sensors, and smart radios are beginning to support standardized protocols for component status interrogation. As SCADA software products begin to support these protocols, the SCADA system will become capable of system-wide health monitoring at the component level, including radio signal-strength indication, network link monitoring, computer resource usage, uninterruptible backup power supply status, instrument health, and a variety of other information.

As the number of assets in the SCADA system increases (Figure 3), the amount of low-level integration work required to tie in each asset must be reduced. Otherwise, as systems escalate toward an infinite number of monitored values, the integration time required and the propensity for basic human error when completing repetitive tasks threaten to make such systems unrealizable.

To avoid this pitfall, the high-speed processing and error-free repetition strengths of computers will be leveraged to automate basic integration tasks. SCADA software developers

Continued on page 34

Continued from page 32
and equipment manufacturers will cooperate to automate device connectivity, tag creation, and display building. Accordingly, the goal of the integrators will switch to system tuning and interconnecting SCADA and business systems.

Finally, ensuring that data, alarms, and SCADA displays are synchronized across the entire SCADA system will be essential. Constant system improvements and growth will make online configuration and automatic data synchronization essential. New graphical changes must be distributed easily, such that displays are reconfigured automatically by the SCADA software and redistributed in real-time to each user interface, whether a local client console, a remote internet connection, a hand-held device, or one of the many new devices that will arise.

Turning Data into Value – System Optimizations

If we revisit our vision of the future SCADA system as a large control loop (Figure 4), more process feedback and more control will, in turn, generate the need for improved real-time response. Reams of additional data must be analyzed; many new, interdependent decisions must be made; real-time process adjustments must be applied.

The ability of organizations to manage this data without hiring legions of operators and analysts will lie in the SCADA software's ability to apply advanced algorithms and rule-based logic at a much higher level than has been possible previously. Modular components will summarize data in real time and will apply automated decision criteria to make possible real-time logistics management, interpretive process adjustments, energy management schemes, maintenance scheduling, and a variety of other benefits.

For example, a typical sewage system can be modeled as a hierarchical set of nodes, each including one or more control devices that allow autonomous control of the node. By combining system-wide historical trends, real-time data, and additional monitoring points, the SCADA software will be able to identify minor anomalies such as inflow and infiltration before they worsen, will assist maintenance in identifying the location of these anomalies, and will forecast the benefits to be achieved in addressing them. By further allowing the software to apply control strategies to manage power use and flow, utilities will reduce equipment maintenance costs, increase energy efficiency, and reclaim wasted capacity.

While the scenario changes for each industry, the potential for improvement remains. As the number of additional devices being monitored increases, optimization methodologies will be applied more effectively.

Conclusion

Costs for basic SCADA components are expected to continue to decline in the future. This trend will support SCADA use in organizations with assets of lower individual value, leading to larger, more dispersed SCADA systems. Simultaneously, larger organizations will take advantage of the growing number of value-priced, wide-area communications options to interconnect geographically dispersed SCADA and business systems. SCADA software developers must understand how to leverage new technological advances in communications without excluding legacy systems.

Low-level SCADA integration will be simplified. The size and complexity of SCADA will increase at an accelerating rate, requiring the creation of tools and integration methods that provide fast, error-free replication for common SCADA tasks. Successful cooperation between vendors will be essential in providing the maximum benefit to the customer.

Finally, the SCADA system will function more and more as a large control loop, able to operate autonomously at increasingly higher levels, based on fewer inputs from operational personnel. Optimization methodologies will be applied in a myriad of situations, allowing organizations to develop larger SCADA systems without incurring unreasonable operational costs or significant staffing increases. As such, the value of the pure HMI component of SCADA software, as we know it today, will decline relative to the many other emerging benefits SCADA systems will offer.

References

- NASA (Unknown date). Johnson Space Center Mission Control, USA Launch System Specifications, Retrieved October 8, 2009, from http://www.aerospace-technology.com/projects/johnsoon/
- NERC (various dates), CIP Standards, Retrieved October 8, 2009, from http://www.nerc.com/page.php?cid=2|20
- Water Sector Coordinating Council Cyber Security Working Group (March, 2008), Roadmap to Secure Control Systems in the Water Sector, Retrieved October 8, 2009, from http://www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf
- FDA (August, 2008), Guidance for Industry Part 11, Electronic Records; Electronic Signatures – Scope and Application, Retrieved October 11, 2009, from http://www.fda.gov/downloads/RegulatoryInformation/Guidances/ucm125125.pdf