Top Ten Internet Scada Mistakes

Veterans Describe Common Mistakes That Sink Internet SCADA Projects

By:
Bob Forbes
Vice President
M2M Data Corporation

Introduction

In our business, we constantly come across companies that have taken a run at leveraging the Internet for their SCADA (Supervisory Control And Data Acquisition) systems, either by Internet-enabling existing SCADA systems or building new applications from scratch. Internet SCADA champions have sold their managers on the cost benefits of using the public Internet instead of expensive, dedicated lines. They have also won support by explaining how the use of open Internet standards makes it easier to integrate SCADA with other corporate systems and avoids technology obsolescence by allowing the use of technology from multiple vendors.

However, all too often, such implementation efforts fail, embarrassing both the engineers who proposed them and the senior managers who backed them.

Most industry experts agree that IP networks and the public Internet will soon play a role in virtually all SCADA systems. The economics are overwhelming, considering that virtually every organization already has a link to the Web and an IP-based internal network it can leverage at relatively low-cost for its SCADA applications. But many companies are still fearful of Internet SCADA, having heard countless stories of projects that failed to meet the required high levels of reliability, performance and security.

Over the past year we've canvassed our customers, partners and our own staff about their worst moments with Internet SCADA to document all of the hurdles to success. Time and time again we find the same short list of common mistakes that are serious enough to destroy the corporate sponsorship, return on investment or technical feasibility of an Internet SCADA solution. Avoid these, and you've vastly improved your chances of making Internet SCADA pay off for your employer and its customers.

Figure 1: Trending of real-time transformer conditions via a standard Web browser.

One: Not Setting Appropriate Expectations

A common cause of Internet SCADA project failure is promising a system based on traditional SCADA technical parameters, that may be more than you can deliver or more than the end-user needs. It is important to understand how the timing and availability characteristics of the Internet differ from traditional SCADA systems, and to communicate those differences and their ramifications to all project stakeholders.

"Leaving people to assume the Internet SCADA system will perform in the same way as a traditional system, whether the application warrants it or not, may be setting yourself up for failure," says one industry veteran. While it is true the Internet cannot guarantee the sub-second response times of traditional SCADA networks, a properly engineered system that relies on the Internet can provide more than adequate response times for most SCADA applications. And several current generation Internet SCADA systems are capable of consistently achieving 99 percent or higher levels of availability.

Two: Building the Internet SCADA System Around Polling

Traditionally, SCADA systems have operated within a "master/slave" architecture, the "master" being a central computer programmed to gather data and transmit instructions to "slaves". These "slaves" are remote terminal units (RTUs) programmed to provide local data gathering and control under the supervision of the "master". This approach minimized bandwidth usage and ensured predictable operation over a shared communication medium such as leased telephone lines.

However, Internet protocols, services and techniques make this architecture ineffective and obsolete. Because Web servers are designed to accept and process requests from many Web clients simultaneously, Internet SCADA is best built on a "push" architecture where each remote field device is programmed to intelligently transmit its data to the master system. The transmission can take place at set intervals (such as every five seconds) or when certain conditions occur, such as a device reaching a certain temperature or the voltage in an electric line reaching a critical point.

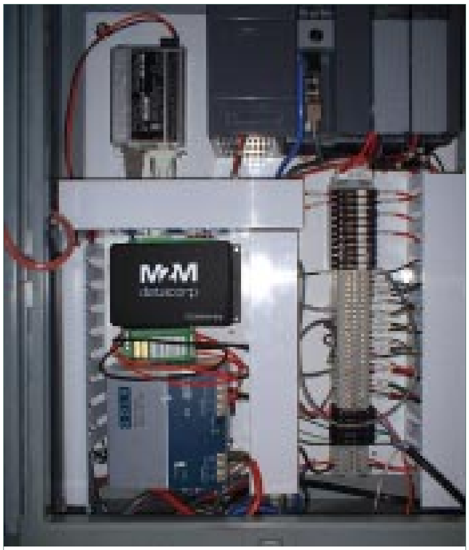

Figure 2: Typical PLC panel assembly with a "push" Internet gateway device.

Internet SCADA Security Checklist

From *Implementing a Local Security Program to Protect National Infrastructure System Companies and Facilities* by the **SANS Institute,** a cooperative research and education organization.

The paper discusses trends such as the migration of SCADA systems to the Internet, and includes a checklist for security. Highlights from the list:

1) Do a vulnerability assessment of your current computer, communications, and control network.

2) Check Security sites for various security related bulletins and to keep up to date on hacking trends and treats.

3) Harden your operating system. Make sure you have an OS that is "security Friendly". The object is to build a secure configuration for your Network OS.

4) Implement a multi-layered defense of Firewall, Intrusion Detection, and/or Virus Scanning software and systems.

5) Use encryption and Virtual Private Networks (VPNs)

6) Implement incident handling plans and procedures.

7) Implement a system of program/data backup and recovery.

Link to full article:
http://www.sans.org/rr/paper.php?id=822

Failing to adopt a "push" architecture has doomed many projects. For example, over the course of three years, a top natural gas field services provider tried polling-based Internet SCADA systems from five separate vendors to monitor compressors along its pipelines, using satellite IP communications links. "Every time there was a communications glitch, the entire poll started over," remembers the senior field engineer, which rendered each system "totally unreliable" and "sent the satellite service fees through the roof".

Three: Rolling Over the End Users

The move to Internet SCADA is a big change, especially for field managers who may have done their jobs in the same way for decades. Those who are used to hands-on troubleshooting at a remote site might feel less valuable when a dispatcher can give them detailed repair information before they even get into their truck. They may remember earlier, failed attempts at Internet SCADA and not realize that new software, hardware and methodologies make Internet SCADA much more feasible than before.

At one oil and gas company, the automation manager championed an Internet SCADA project from headquarters and began with a pilot project to prove the ROI of the system and attract the necessary support for a full deployment. The project died, however, when users who hadn't been consulted or educated about the new system refused to use it, while managers of existing SCADA implementations battled the new system fearing it might cost them their jobs.

In an effort to plow through the project, you may be tempted to simply avoid the messy work of listening to users' fears and addressing their concerns. Don't. Without the support of your end users, you can lose the corporate support that is so critical for the project's success. If you are working with an Internet SCADA vendor that has worked with many users in your industry, consider tapping their experiences and insight in the process.

Four: Not Bothering With SCADA "Surety"

SCADA "surety" means the combination of security and continuity, both of which are major issues for a company monitoring a critical asset such as a transmission line over the Web. The public Internet exposes SCADA systems to a host of security and reliability threats that can be expensive to deal with, if not handled correctly.

Internet-based applications are prime targets for viruses, worms and denial of service attacks. Furthermore, hackers can exploit any vulnerable data streams they can "sniff" online, and SCADA systems are particularly attractive prey. If a determined attacker manages to break into a SCADA data stream, they could change the data, trigger false alarms, suppress actual alarms or send false controls to the remote devices. Each of these security breaches can be potentially devastating to your SCADA system and the operations it serves.

Your Internet SCADA effort could backfire if you don't have the infrastructure to continuously monitor the system, lock down every node, encrypt the information, and back-up the data that has been gathered. If you have any doubts that your own data center can provide these capabilities, consider a reliable, proven outsourcer with experience hosting Internet SCADA systems.

Five: Assuming that Any SCADA Solution Can Do the Job

Most SCADA applications are good at generic data acquisition and control functions. However, different industries require that information be assembled, filtered and displayed in very specific ways. For example, the type and format of information used for alarming, trending and reporting about a gas plant may be very different than for a transformer in an electric substation.

The work required to customize and configure a generic SCADA application for a specific industry can destroy all the benefits promised by Internet SCADA. For example, one rural electric cooperative took months of extra time, and the help of expensive specialized staff, to configure and customize an Internet SCADA system for low voltage distribution automation. In addition to exceeding their schedule and budget, the coop was then tied to a custom, proprietary application. Savvy project managers avoid such problems by choosing an Internet SCADA solution that includes modules already customized for their vertical market.

Six: Buying Into Proprietary Technology

The Internet SCADA-wares of many vendors are simply tools that provide a limited Web interface into existing proprietary applications. For example, one major utility decided on an Internet SCADA system to monitor aging transformers to maximize their throughput and reliability. Rather than utilize an open, extensible framework for Internet SCADA, they used Web "snap-ons" to legacy SCADA applications and remote monitoring units. As a result, they were unable to later extend or integrate what were, in effect, standalone Web applications.

You're better off choosing a vendor who treats Internet SCADA as a central, open, accessible monitoring framework for the enterprise. Products and services built on such a philosophy give you full access to the real benefit of open interoperability across IP-based networks, so you can change your monitoring, alarming, analysis and control functions as your business changes.

Seven: Overbuilding the User Interface and Overwhelming the User

Internet SCADA designers, excited by the bells and whistles of Web development tools and a fresh canvas on which to paint their new application, consistently overbuild the screens that the user will interact with. The resulting screens - mixtures of web graphics, asset illustrations, schematics, traditional SCADA graphics, and raw data - often obscure the critical information the end-user needs.

Further, on the theory that more data means better analysis, some Internet SCADA designers collect and model far too much data. Again, in many cases the result is too much data, overloading both people and systems.

"A fully populated RTU may have only 10% of its register values that are critical to the operation of the site" says one T&D SCADA veteran. "When the users have to dig through the screens to find those values, it makes it tough to get them onboard with the application, and ultimately means we're spending more time training and supporting them."

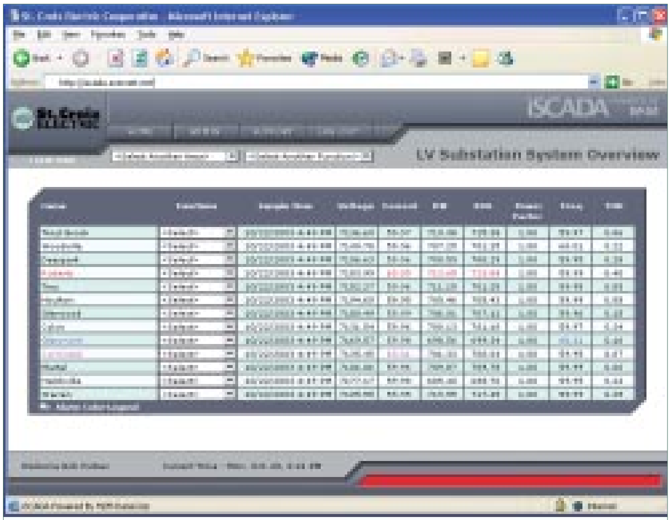

Figure 3: Aggregated view of key conditions for 13 low voltage distribution substations. Alarm bar on bottom of webpage prominently displays condition, and colored text within data provide alarm specifics.

Rather than overwhelm the operator with every piece of available data and clever graphics, get his buy-in by keeping the user interface simple, displaying important data upfront, and using colors sparingly and only to highlight critical alarm conditions. This type of design is more data-driven than traditional SCADA systems and "thinner" on the client (much like e-Commerce applications), and has the added benefits of being less costly to develop, easier to maintain, and more open and flexible.

Eight: Choosing a Vendor Based Only On Price

Buying only on price is almost never a good idea, and is particularly dangerous in a relatively new market such as Internet SCADA. Low bidders may be small companies who are giving business away to establish them in the market and may not have enough money to stay in business until the end of your project, or to help with ongoing support and upgrade issues. Such small companies may also be outsourcing development work overseas without the ability to manage the associated language, culture or quality of workforce issues. Oftentimes high bidders may be young companies charging the highest prices they think they can get, or that need to charge high prices or accelerate payment terms to make their next payroll.

Experienced buyers who have completed many automation projects and evaluated hundreds of proposals recommend discarding the highest-priced and lowest-priced bids, instead aiming for a partnership with a vendor who can deliver the optimum price-performance.

Nine: Not Planning For Support After the Project

Buying service and support for Internet SCADA systems after the system is complete can be very expensive, because you are already committed to the vendor's products. The vendor has little incentive to bargain, since their next sale to you is probably years away. And once you have begun purchasing Internet SCADA as a service from an outsourcer, it's far more difficult to negotiate SLAs (Service Level Agreements.)

The time to think about such needs is before the project begins. Before signing a contract for Internet SCADA hardware or software, be sure to negotiate a warranty. When purchasing it as a service, negotiate an SLA with uptime guarantees that match the reliability needs of your application.

Ten: Treating Internet SCADA as a Technology Rather Than a Business Issue

SCADA is a business-critical technology because it can reduce expensive diagnostic and repair visits to remote sites, enhance the reliability and efficiency of the systems being monitored, and increase the mean-time-between-failure for critical equipment.

Using the Internet as a platform for SCADA delivers these benefits more quickly, while reducing capital expenses and risk. It also provides dynamic data access to applications, giving designers the flexibility to provide operators with only the information they need.

Many or all of these benefits can be lost, though, if an Internet SCADA project is allowed to evolve into a purely technical endeavor, in which an IT or engineering group is left to focus only on nuts and bolts, such as the inner workings of Internet protocols and technology implementation issues. The most successful Internet SCADA initiatives base their architecture, design and purchasing decisions on the business drivers that make Internet SCADA so compelling.

The Internet SCADA market has matured to the point where deployed systems can become strategic business assets, and many of the common technical and design risks can be recognized and avoided. By keeping a constant eye on the business drivers, and being armed with the knowledge of the most common Internet SCADA pitfalls, you'll be well positioned to pull off a successful project and quickly begin reaping the benefits of this evolving SCADA standard. ■

About the Author

Bob Forbes is vice president for M2M Data Corporation in Denver, Colorado. His responsibilities include research, strategic planning and the introduction of new technologies to the market. Forbes and his colleagues at M2M have pioneered of many of the security, sensor and application delivery methodologies in use on Internet SCADA systems today. The electric power, oil and gas, defense, homeland security, and national research and development sectors use M2M's Internet and satellite-based SCADA products and services. Prior to M2M, Forbes was founder and executive vice president of strategic initiatives for Authentor Systems, an Internet security company. Before that, Forbes held senior executive positions with several private energy and information technology firms. Mr. Forbes has a Bachelor of Science degree in Finance and International Business from the University of Colorado.