

Safeguarding Process and SCADA Control Systems Through Service Assurance

Adam Stein, Vice President of Marketing
Mu Security

Most remote monitoring system professionals are fairly confident they know what applications and operating systems are running on their desktops and servers. So when a strategic vendor like Adobe releases an announcement of a new critical vulnerability, obtaining and installing the published patch is a given. While patching is a "necessary evil" of network management, it does not constitute a best practice when it comes to securing critical infrastructure (CI) networks.

For plant operators responsible for attaining ultra high reliability for their CI networks, there is a growing need to make this high wire act less daunting. What they are seeking is a service assurance process that stress tests product deployment lifecycles to weed out any reliability, availability and security weaknesses that have the potential to threaten the public safety and/or interrupt business critical processes.

Unfortunately, simple patching approaches do not provide a service assurance model for control systems running critical infrastructures for essential services such as power, water and transportation. The process control systems running these CI networks often come as proprietary, bundled packages precluding end-users from knowing what needs patching to keep the proverbial wolves away from the security house doors.

Consider these real-world examples: Nearly 10 years ago, an ISS Security Advisory was released called "ICMP Redirects Against Embedded Controllers." Unfortunately, the advisory only noted that "it pertains to an indeterminate class of networked embedded controllers found in a wide variety of automation equipment, using the OS-9 operating system." Remote plant owners were left as the man in the middle since only a few of the vendors of SCADA and PLC products released information about their embedded operating systems. As a result, not a single SCADA engineer knew to contact his or her vendor for patches. And this is the tip of the iceberg.

Because of the inherent weaknesses in SCADA systems, there have been numerous system crashes and multi-million dollar production losses. One of the most prominent culminated nearly eight years later in the emergency shutdown of the Tennessee Valley Authority's (TVA) Browns Ferry Nuclear Plant in August 2006.

In February 2008, a similar sequence of events began with the latest Microsoft Security Bulletin MS08-008, "Critical Vulnerability in OLE Automation Could Allow Remote Code Execution (947890)." While this announcement makes it clear that use of a web browser like IE can leave users vulnerable, it fails to mention that OLE is the underlying component in an industry standard API commonly known as OPC (OLE for Process Control).

Unfortunately, nearly every SCADA and process system depends heavily on OPC for communications between control systems. How will OPC users discover they need an obscure, but critically important patch? If they have a responsible control system vendor (and there are some very good ones) they will get an email in the next 24 hours. But tens of thousands of critical systems likely will go unpatched this week until something messy like this happens again.

What does this all mean for the owners and operators of critical SCADA and control systems? It means that the end-user should not just assume that a control system product is secure just because there are no patch advisories for it. Users need to actively communicate with their vendors and push for full and timely disclosure of all vulnerabilities that could cause unscheduled downtime or larger product safety issues. Users also need to proactively apply service assurance and negative testing to their systems (offline of course) both prior to deployment in the field and on a regular basis by running available service assurance systems against all networked devices and applications. Most importantly, the SCADA industry needs to push for mandated security disclosures for all the products used in the market. Only then will these hidden vulnerabilities stay away.

A Lingering Problem: Ensuring Product Resiliency And Availability

The industrialized world relies on a broad spectrum of vital critical infrastructure sectors. These sectors include agriculture and food, water, public health, emergency services, defense industrial base, telecommunications, energy, transportation, banking and finance, chemical, postal and shipping, and key physical assets such as nuclear power plants, dams, government facilities and commercial assets. In addition to physical safety and security, network security for critical infrastructure is crucial because of its reliance on electronic systems for operational control.



Figure 1: Automating Service Assurance using a Security Analyzer and Dedicated Industrial Control Firewall help Ensure Operator Plant Safety and Maximum Uptime.

Malfunctions to the industrial control systems in these industries, including faults within programmable logic controllers (PLCs), distributed control systems (DCS), remote terminal units (RTUs) and SCADA systems, can cause safety issues including weakened national security, business and social disruption, physical injury or death, and environmental damage, not to mention damage to the reputation of the business, possibly resulting in increased regulation. The US Government Accountability Office (GAO) has described a dramatic new escalation in risks to control systems, citing four areas of concern: (1) adoption of standardized technologies with known vulnerabilities; (2) control networks being connected to other networks; (3) having insecure connections, which exacerbate vulnerabilities; (4) having information about infrastructures and control systems be easily available to the public.

Ignoring or improperly addressing industrial control system security or robustness risks can result in the disruption of critical systems, damage to equipment, and may cause unpredictable operations or failure of critical infrastructure (see GAO specifics here). Simply adding existing IP-based security controls such as firewalls, intrusion detection/prevention, antivirus, encryption, authentication, and other related technologies to control systems will not always ensure plant safety or security. Historically, these technologies are not built into industrial controllers because the systems were considered closed and did not use open networking technologies nor were they accessible from the public Internet.

Today, the reduction of separate control networks and widespread adoption of Ethernet and TCP/IP technologies has exposed these devices to new threats. For example, adding a layer of security technology to older control systems may trigger operational glitches (e.g., due to increased latency). Processing requirements for security can

Remote 2008

CONFERENCE AND EXPO

SCADA, Device Networking, M2M, Wireless Technology, Onsite Power, And Security for Remote Sites and Equipment

No other industry conference brings together technology users that manage remote sites like the Remote 2008 Conference and Expo. Over 50 conference sessions will provide cutting-edge technology direction and application strategies from the companies and users driving the growth in SCADA, M2M, device networking, data communications, system & site security, emerging wireless technology, remote monitoring and automated control, and onsite powering of distributed equipment, networks and facilities.

www.RemoteExpo.com

NOVEMBER 5-6, 2008 - ATLANTA, GA.

exceed close timing tolerances of control systems and cause latency-related delays or even shut down operations. Consequently, manually adding security to process and SCADA control systems plus IP security testing requires substantial engineering, QA and validation efforts. Security and reliability testing for service assurance are critical parts of ensuring safety for process control systems because insecurity of the building-block protocols directly impacts operational safety of the attached process system.

Enabling Safer and More Resilient Process Control

Owners and operators of industrial control systems now have a new tool for testing and analysis that isolates and documents safety concerns, including protocol implementation weaknesses in any IP-based control system. The protocol testing and measurement systems in a service assurance system like the Mu-4000 Security Analyzer ensure reliability by enabling, using, and routinely stressing control system resiliency and security as part of a safety process of continuous improvement. Automating the service assurance process automates risk quantification according to the attack surface for products or services.

The attack surface concept was developed by Microsoft and Carnegie Mellon University, and expresses exposure of that product or service to robustness issues including malicious attack. Attack surfaces of DCS, RTUs and PLCs are becoming increasingly complex with the addition of more complex control protocols (like Modbus/TCP and Ethernet/IP) and traditional IT protocols like HTTP, NTP, SNMP and FTP to many systems. Also, since control systems are no longer isolated islands of proprietary industrial control protocols such as Modbus or IEC 61850, software bugs now expand into exploitable vulnerabilities since they are exposed to an open IP network. Service assurance systems provide safety baseline analysis of the total attack surface of a control system within the context of a methodical process of identifying security and system availability issues for any protocol vital to industrial control operations.

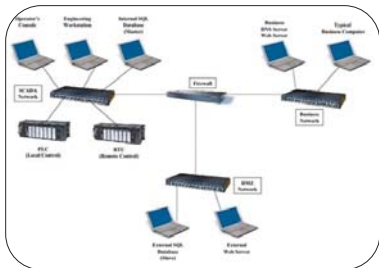


Figure 2: Industrial Control Safety spans the entire Operator network as control networks become integrated with conventional Ethernet networks.

For example, the Distributed Network Protocol (DNP3) used in many facilities defines communications procedures for components of process automation and control systems. The DNP was originally designed for a closed network environments so implementations do not expect to receive improperly formatted frames found in IP based networks (DNP3 refers to the case in which DNP's layer-2 frames are transmitted over TCP/IP). Mutations analyzed and measured by the Mu-4000 security analyzer system ensure that DNP3 implementations are able to tolerate any kind of abuse it might encounter as the DNP frames are transported over intervening IP-based networks (packet loss, duplication, corruption, reordering, etc.) as well as proving that an implementation can handle incorrectly formatted DNP frames from less compliant implementations.

SCADA systems also use Inter-Control Center Communications Protocol (ICCP/TASE.2), which

is another potential source of security vulnerabilities. ICCP/TASE 2 facilitates communications between multiple SCADA control centers. Vulnerabilities include ASN.1 attacks, exploits against the stateful nature of ICCP and possible issues related to the use of SSL-TLS. Integrating service assurance into the product deployment lifecycle automatically locates and documents embedded vulnerabilities in SCADA products and control system implementations to expedite vendor remediation, or to provide information about weaknesses so that other protection can be employed (in cases where it is infeasible to update or patch a faulty controller).

Ensuring Safety in Industrial Control Plants along With Maximum Service Uptime

Operators of industrial control systems share a common goal of safely ensuring secure process and SCADA control systems to preserve service uptime without unscheduled interruptions. Operators face the challenge of providing resilient, robust and secure process control implementations for increasingly complex and older process control systems that lack the processing capability for improved security (either added explicit security protocols or more robust exception handling). Converged IP-based network products for voice and video on the same, shared IP network adds to the complexities of

securing control systems for critical infrastructure and requirement of using security analyzers.

Operators previously had limited visibility into the true product or network attack surface, security, safety or robustness metrics of IP-based products they use in a control system. Automated and repeatable service assurance provides an unbiased benchmark for customized measurement of any product's security readiness, robustness, and resiliency before production purchase, deployment or upgrade. Operators use this assessment capability to hold vendors accountable for unsafe, insecure or non-robust products. The analyzer allows operators to proactively document the extent of a product's safety shortcomings including the use of existing test scripts, and to take preventive measures including the validation of signatures for security products, or the deployment of remediation devices such as firewalls or IPS that are able to block exploitation of the discovered protocol implementation flaws.

Critical infrastructure plant managers and their varied product suppliers are turning to service assurance systems for:

- **Product Selection:** Security and safety readiness is a key metric to support purchase decisions or upgrades, in addition to reliability, functionality, price and performance.

- **Product Deployment:** Securely deploy product features or introduce configuration changes into the network architecture, which provides the ability to proactively identify and remove robustness issues or vulnerabilities before deployment.

- **Change Control:** Analyze new software or firmware releases or bug fixes before production use, and ensure that no published or previously eliminated safety issues or vulnerabilities are inadvertently used in the network.

- **Threat Assessment:** Security crisis management and problem reporting to a vendor is streamlined with a security analyzer's ability to automate and "operationalize" the auditing and vulnerability remediation processes.

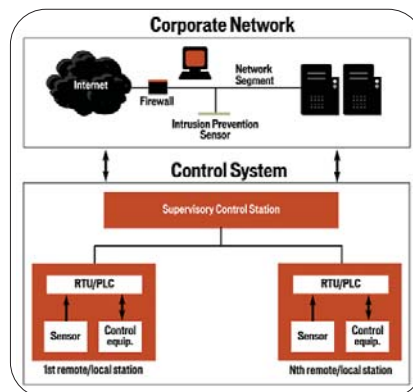


Figure 3: Service Assurance Requirements span the Operator Network and include Network Equipment developers.



Have you received editorial coverage in *Remote Site & Equipment Management*?

When your company is featured in *Remote Site & Equipment Management*, expecting your customers to read your story isn't enough... you need Reprints.



800-290-5460 ext. 183
remotesiteandmanagement@reprintbuyer.com

RMS is the authorized provider of custom Reprints, Eprints and NXPprints for *Remote Site & Equipment Management*.

Vendors of PLCs, DCS, SCADA and other IP-based software or hardware products for managing Industrial Control systems such as Honeywell or ABB use service assurance systems receive actionable feedback from operator users via documentation of specific weaknesses in their products.

This approach includes on-board detailed reporting, packet captures and Linux-executables to quickly tell plant operators, developers and vendors which issues are "hot" and enable the vendor to quickly isolate the root cause of the issue. Internally, product vendors use this actionable suite of remediation tools to repair vulnerabilities, chart robustness or resiliency weak spots, tailor signature development or as input to patch/update development.

SCADA Network Equipment Manufacturers are Using Service Assurance for:

- **Design and Development:** Used by QA and development teams to repair security flaws as early as possible in the development process, with measurable reduction in staffing and support costs.
- **Testing and Customer Problem Resolution:** Safety issues are isolated and information using a service assurance system to bring quick focus to expedited remediation of customer-reported problems – with greatly reduced difficulty to reproduce each issue.
- **Product Upgrades:** Assessment of configuration changes, software upgrades and patches ensure that secu-

rity regressions or robustness issues like memory leaks or CPU utilization spikes are not inadvertently introduced.

- **Threat Assessment:** Every network has unique settings but vendors focus their testing on the most common configurations. Mutation analysis with published vulnerability analysis provides unprecedented threat assessment coverage.

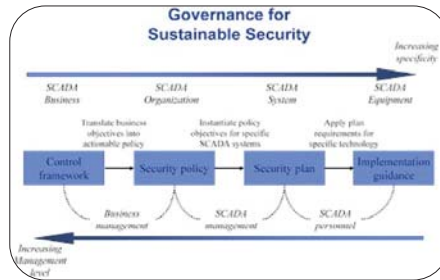


Figure 4: Sustainable Security and Safety for Plant Operators.

Robustness Testing Ensures Service Security of Critical Infrastructure

A resilient service assurance process offers operators of Industrial Control systems a customizable system for maximizing operational safety and efficiency over IP networks. It helps achieve 99.999 percent uptime, reduces time spent on product safety workarounds or costly security breaches by averting successful exploits of IP-related vulnerabilities, and limits problems caused by non-robust

implementations of the protocols. A service assurance process and product helps both operator users and their product vendor suppliers with the identification and timely repair of safety, robustness and vulnerability issues.

The result of consistent plant use of service assurance is the constant improving of safety of industrial control systems. Several benefits include proactive and early discovery of industrial control resiliency issues; documentation of SCADA and Process Control Vulnerabilities; and preventative occurrence of zero-day attacks network resiliency issues to enable nearly 24x7x365 continuity of critical services. Cost-effective and wide-ranging test suites allow the operators service assurance system to address all major protocols affecting critical infrastructure. Security Analyzers, as an example of service assurance in a box, are an essential and easy-to-deploy way to benchmark system safety and enable security as a process of continuous improvement.

Adam Stein is vice president of marketing for Mu Security Reach him at astein@musecurity.com.

Mu Security offers a new class of security analysis system, delivering a rigorous and streamlined methodology for verifying the robustness and security readiness of any IP-based product or application. Founded by the pioneers of intrusion detection and prevention technology, Mu Security is backed by preeminent venture capital firms that include Accel Partners, Benchmark Capital and DAG Ventures. The company is headquartered in Sunnyvale, Calif. For more information, visit the company's website at <http://www.musecurity.com>

WEB GUIDES

www.dcbnet.com



Data Comm for Business, Inc. (DCB) manufactures and distributes a broad line of data communications equipment including DSU, Stat Mux, Statistical Multiplexer, FRAD, Routers, Wireless, Remote Access, RS-232, modems, FRADs, SCADA, and remote interconnection equipment. The DCB Website includes complete data sheets for all DCB products, PDF versions of all product manuals; and most importantly, in the education section, hundreds of white papers and tutorials covering communications technologies and methodologies.

www.sensaphone.com



Sensaphone provides a variety of standalone remote monitoring products. Complete solutions are available with web access, data logging, alarm notification, wireless sensors, and more.

www.digi.com/rdm



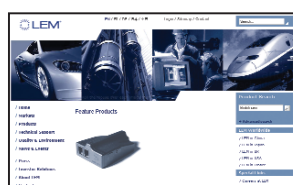
Leveraging expertise in cellular, Wi-Fi, ZigBee/802.15.4 and proprietary RF technologies, Digi offers reliable wireless device connectivity solutions. From simple cable replacement, to sophisticated end-to-end wireless device connectivity and management with our unsurpassed Drop-in Networking family of products, Digi knows wireless.

www.sel-com.com/fiber



Schweitzer Engineering Laboratories, Inc. provides innovative devices, including fiber-optic transceivers, serial to Ethernet transceivers, voice annunciators, and remote I/O products. Our electrical substation-grade equipment surpasses the requirements for most environments. The sel-com.com website includes descriptions, prices, and ordering information for our communications products. Read about our 10-year worldwide warranty and ISO-9001 Certified Quality Management System. It also links to the corporate SEL website for electric utility products and services.

www.lem.com



LEM is a market leader in providing innovative and high quality solutions for measuring electrical parameters. Its core products – current and voltage transducers – are used in a broad range of applications in industrial, traction, energy and automotive markets.

www.telsource.com



A leading network integrator and field service organization, Telsource provides comprehensive voice and data product and service solutions nationwide. Telsource's PremGate™ Remote Access Manager provides integrated in-band and out-of-band access to remote systems and devices to help you securely, reliably and flexibly manage them. It proactively monitors systems and devices and offers real-time alerts to rapidly detect critical problems and, ultimately, increase system availability and reduce opportunities for lost revenue. With PremGate, you can remotely access up to six devices directly connected to serial interfaces via an Ethernet interface or modem. Because it is managed remotely through serial interfaces, access is not contingent upon the availability of an IP Network.

www.phoenixcon.com



Phoenix Contact Inc. is a world leader in the manufacture of specialized electronic components and connection systems. The Phoenix Contact website is a user-friendly site complete with a variety of information. It offers a comprehensive online catalog with over 10,000 part numbers, CAD drawings, data sheets and detailed technical information.

www.uppi-ups.com



UPPI designs, manufactures and markets products that detect, correct, and improve AC power quality. Preventing the hazardous nature of today's electrical environment from weakening the integrity of your critical process is what we are all about. Whether protecting data, communications, security, or production equipment, UPPI products reduce the risks caused by faults in the AC power delivery system.