The Sage Advisor

SCADA, SECURITY & AUTOMATION NEWSLETTER

Volume 14, Issue 2 • Fall/Winter 2004 A Publication of Sage Designs, Inc.

Reducing Infrastructure Vulnerability Post-9/11

In July, **Sage Designs**, **Pure Technologies**, **Southwest Microwave**, and **Stantec**, teamed up with guest speakers, **Rick Hahn**, **Vic Opincar**, and **John Saunders** to provide two thought-provoking seminars focused on post-9/11 dangers to our country's water supply.

Keynote speaker, **Rick Hahn**, of **Secure Strategies International** and **Terrorism Analyst for MSNBC**, addressed the need to carefully consider potential threats from both inside and outside our water facilities. Mr. Richard Hahn retired from the FBI after a distinguished career spanning 32 years. As an agent, Hahn investigated domestic and international terrorist organizations and specialized in events carried out by Puerto Rican independence organizations. Hahn organized multi-agency task forces which brought about the arrest and successful prosecution of terrorists. From 1987 through 1993, Hahn was assigned to the FBI Laboratory Explosives Unit as a Supervisory Agent and Examiner of Explosive and Hazardous Devices. While there, Hahn traveled extensively and was involved in the forensic aspects of a number of terrorist bombings against U.S. targets around the world, including the attack aboard the vessel *City of Poros* in the Mediterranean, the bombing of Pan Am Flight 103 over Lockerbie, Scotland, and the 1993 bombing of the World Trade Center in New York. Hahn was also called upon to manage the crime scene at the Murrah Federal Building in Oklahoma City. Mr. Hahn serves as a terrorism analyst for MSNBC and appears regularly both on MSNBC News and several other NBC programs, and is an occasional contributing author to various business publications on the topics of terrorism and security.

In addition to moderating the event, **Victor Opincar**, of **Victor Opincar Associates**, discussed the assessment of weakness at water facilities, as well as the development and testing of an adequate emergency response plan (ERP). As Chairman of **ACWA's Water Fundamental Panel on Security**, Mr. Opincar initiated sessions on water system security in 1999, based on the Clinton Administration's information that U.S. water infrastructure was at risk. He formed a team with former FBI and Secret Service Agents to perform RAM-WSM vulnerability assessments mandated after 9/11. Opincar is also a founding member of **ACWA's Statewide Security Task Force** and continues to consult with water agencies involving forensic issues, planning, and operational analysis.

Water utilities security consultant, **John Saunders**, of **Enterprise Protection Associates**, spoke about Water and Wastewater Security Problems and Solutions, and the need

(Continued on Page 2)

For those who missed the July seminars, we will be co-hosting a second round of Security Seminars for Water Utilities to qualified water utility professionals in November. Further information about upcoming events can be found in this issue, or on our website, www.SageDesignsInc.com. In consideration of public safety, some of the proceedings of these events may be made available to qualified individuals on an as-requested basis.

IVC Provides Security for the Democratic National Convention

IV&C Industrial Video and Control

In preparation for the 2004 Democratic National Convention, the Boston Police Department (BPD), purchased ten, field deployable, pan tilt zoom, IP cameras from IVC. The DNC outlined a set of requirements for a video system that could be quickly and easily deployed to monitor various scheduled activities around the city, as well as unforeseen events, such as fires and riots.

The ten camera units were placed at different locations around the areas of Boston where the four-day DNC took place. Although the cameras were located on the roofs of tall buildings, the 100X zoom provided excellent close-up views of activity on the streets. A permanent wireless network was installed to collect video streams transmitted from the cameras to an ethernet radio located on the top of the Hancock Building, Boston's tallest structure. From there, the video was sent by wireless backhaul to an IVC Relay Server located at police headquarters. The IVC View Station Software allowed the Police Department to view the video and control the PTZ cameras at their headquarters. Additionally, authorized personnel could view and control any of the cameras from any PC connected anywhere on the city IP network. This enables improved coordination between fire, police and other response teams and can vastly reduce response time. The systems are stored in rugged latch-cases that can be carried to a new location and completely set up in minutes, including the connection to the wireless network. A small gas-powered generator accompanies each camera system to make the deployment completely independent of outside services.

Bill Richards, a Vice President at IVC, commented, *"The versatility of the systems, both in their operation and their ease of deployment, have met every requirement set forth by the BPD, and we were able to deliver the systems within their tight schedule. The Canopy wireless network makes it possible to deploy the cameras to unanticipated locations anywhere in Boston quickly and easily."*

Based in Watertown, Massachusetts, IVC is a manufacturer of IP-based video systems and a developer of advanced software for managing networks of video cameras. Their video systems are used in a broad variety of applications, including water infrastructure surveillance. IVC offers a range of IP cameras including pan-tilt zoom, fixed, remote zoom and varifocal (manual zoom) cameras. For further information, please contact Sage Designs, your IVC distributor.

Free Educational Security & SCADA Seminars

November 8	Security Seminar, Concord, CA
November 8	SCADA Seminar, Concord, CA
November 9	Security Seminar, Ontario, CA
November 9	SCADA Seminar,

Details & Registration Information Inside

Reducing Infrastructure Vulnerability, cont.

to now consider sabotage of water and wastewater systems as not only a viable threat, but also a plausible one. Mr. Saunders is a Certified Protection Professional (CPP), member of the American Society for Industrial Security International, a Certified Information Systems Security Professional (CISSP), and member of the Computer Security Institute. Saunders is qualified in the Risk Assessment Methodology for Water/Wastewater infrastructure (RAM-W) delivered through U.S. Government-Sandia National Laboratories, NM. He has over twenty years experience in policing, corporate security and public safety.

As the Department of Homeland Security continues to concentrate on protecting our country's greatest assets, it is incumbent upon this industry to consider the vulnerabilities that could be exploited by terrorists at less-protected public facilities. Mr. Jack Eldridge, of Michael Baker, Jr. Inc., one of the attendees, cut to the quick in the question-and-answer period to ask his colleagues, *"Who among us wants to be the Three Mile Island of water systems?"* Rick Hahn concluded, "*The likelihood of terrorist events occurring inside the U.S. continues to increase. Being prepared is our only means of averting or mitigating disaster."*

Pure Technologies Ltd. is an international technology company, that has become a world leader in providing information and communications technology for infrastructure management and surveillance. Pure has developed a suite of complementary technologies, that provide infrastructure owners with comprehensive state-of-the-art management information. Pure Technologies designs and provides continuous remote monitoring systems and technical support from its offices in Columbia, MD, Phoenix, AZ, and Calgary, AB

Southwest Microwave, Inc. is a leading global provider of exterior perimeter security solutions. The company produces a broad range of perimeter intrusion detection equipment, including volumetric microwave sensors, infrared sensors, state-of-the-art fence detection systems and wireless CCTV transmission systems that perform reliably in harsh environments. With over 30 years of experience, Southwest Microwave's perimeter security products are trusted across a diverse market spectrum, from critical utilities, military / government and correctional applications to the transportation, industrial and communications sectors. Recognized for world-class customer support, Southwest Microwave's technical services group offers comprehensive site planning, design assistance, product training, system commissioning and tech support services.

Stantec provides professional design and consulting services in planning, engineering, architecture, interior design, landscape architecture, surveying, and project management. Continually striving to balance economic, environmental, and social responsibilities, Stantec is recognized as a world-class leader and innovator in the delivery of sustainable solutions. Stantec's 50 years of experience is now being utilized in the study of water supply risk assessment and contingency planning.

Sage Designs, Inc. is a SBE/WBE distributor/rep firm focused on providing SCADA, Security & Industrial Automation products, as well as educational seminars, training programs and referrals, to utility professionals seeking solutions for their SCADA, Security & IA needs. According to Dena Cornett, CEO of Sage Designs, *"As today's technology has evolved, it is becoming incumbent upon SCADA and MIS departments to infuse their knowledge to security managers, in order to bridge the gap between process monitoring and control and traditional security system methodology at our utility infrastructures."*

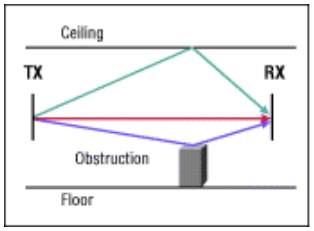
Although Sage Designs is not a consulting firm, the company seeks to educate its customer base by providing referrals to qualified third-parties, and by offering intelligent, open-systems, solutions to meet many of these needs. Tony Sannella, President of Sage Designs, has lectured widely on the topic of Open Architecture SCADA Systems at California Polytechnic University's Irrigation Training & Research Center (ITRC), the Instituto Mexicano de Tecnología del Agua (IMTA), and at numerous Instrument Society of America (ISA) and California water association conferences, such as those sponsored by ACWA, CA-AWWA, and CWEA.

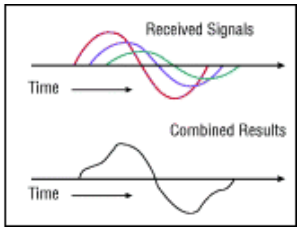
Sage Advice

What is Multi-path Interference?

Multi-path interference occurs when an RF signal has more than one path between a receiver and a transmitter. This occurs in sites that have a large amount of metallic or other RF reflective surfaces. Just as light and sound bounce off of objects, so does RF. This means there can be more than one path that RF takes when going from a TX to an RX antenna. These multiple signals combine in the RX antenna and receiver to cause distortion of the signal.

Multi-path interference can cause the RF energy of an antenna to be very high, rendering the data unrecoverable. Changing the type of antenna and relocating the antenna can eliminate multi-path interference.





You can relate this to a common occurrence in your car. As you pull up to a stop, you may notice static on the radio. But as you move forward a few inches or feet, the station starts to come in more clearly. By rolling forward, you move the antenna slightly, out of the point where the multiple signals converge.

An antenna diversity system such as found in Locus industrial radios, can be compared to a switch that selects one antenna or another, never both at the same time. The radio in receive mode will continually switch between antennas, listening for a valid radio packet. After the beginning sync of a valid packet is heard, the radio will evaluate the sync signal of the packet on one antenna, then switch to the other antenna and evaluate. Then the radio will select the best antenna, and use only that antenna for the remaining portion of that packet.

On transmit, the radio will select the same antenna it used the last time it communicated to that given radio. If a packet fails, it will switch to the other antenna and retry the packet. One caution with antenna diversity, it is *not* designed for using two antennas, covering two *different* coverage cells. The problem in using it this way, is that if antenna #1 is communicating to device #1, while device #2 (which is in the antenna #2 cell) tries to communicate, antenna #2 is not connected (due to the position of the switch), and the communication fails.

Antenna diversity should cover the same area, from only a slightly different location. This explains why the antennas on top of a Locus radio are just a few inches apart!

Sage News

A SAGE MOVE… In July, Sage Designs moved its Northern California office to a larger, more efficient space in the building next door. All phone numbers remain the same; only our suite number has changed. We genuinely appreciate the patience shown by our customers and vendors during this transition.

WBE & SBE CERTIFICATION… Sage Designs was recently certified as a Woman-managed Business Enterprise (WBE) by the Supplier Clearinghouse for the Utility Supplier Diversity Program of the California Public Utilities Commission. We have also been certified as a Small Business Enterprise (SBE) by The Metropolitan Water District of Southern California.

The Role of SCADA in Security

Supervisory Control and Data Acquisition Systems (SCADA) are critical to the safe, reliable and efficient operation of power plants, drinking water systems, wastewater treatment facilities, oil and gas production and distribution as well as other essential services that affect the life of millions of people in North America. These systems typically include standalone or networked computers, application software, communication mediums and protocols, field controllers such as PLCs/RTUs, sensors, back-up batteries and other auxiliary equipment. System size and complexity range between a few remote sites and a handful of parameters to several hundred sites and thousands of parameters that are measured and controlled. By using SCADA systems instead of human control, the result is greater efficiency, faster and more coordinated system control, lower operational costs and better use of scarce human and financial resources.

The Secure Facts: The primary role of SCADA systems is to monitor and control dispersed assets from a central location. Commonly, many sites are remotely secluded and thus ideal targets for intruders and vandalism. Making matters worse are the adoption of standard technologies, off-the-shelf equipment and Internet-based connectivity, all with known vulnerabilities. This makes systems vulnerable to physical and cyber attacks resulting in disruption of service, process redirection or manipulation of data, putting public safety at risk.

Over the past decade, many highly publicized incidents support the need for effective physical and cyber security in SCADA Systems.

SCADA's Security Role: Since most utilities operate under tight budgets and limited staff, securing remote equipment and resources is a common challenge. Fortunately, modern SCADA systems provide a solution that can significantly mitigate risks while extending the ability to secure remote assets.

■ **Physical Security**, which relates to access control, intrusion detection and perimeter control, can be tied to existing SCADA systems to offer an effective monitoring and response system. For example, a keyless entry device, such as a card reader connected serially to a PLC/RTU, would allow site access to be automatically logged with time and date in the controller, as well as at the central site. A motion or intrusion detector can be connected to the PLC/RTU digital input board, providing instant alarm notification and logging at the central site. Intrusion sensors can be deployed at access gates, doors, ladders and manholes. Alarm records can be correlated with operational information to a get a precise picture of the situation. Furthermore, due to the widespread use of high bandwidth Wide Area Networks, inexpensive IP based web cameras can be utilized to provide video frames from remote locations over wireless IP networks such as Ethernet Spread Spectrum radios and Wi-Fi technologies or using conventional wire based networks such as fiber optic and high speed leased lines.

Physical security can also be part of the SCADA system comprehensive control and operation strategy. For example, if a site has been breached, the SCADA system can automatically perform a safe shutdown of the remote assets to isolate the problem and limit widespread service disruption or contamination. SCADA systems can also be utilized as an advance warning and response system against biological and chemical threats such as the release of harmful chemicals or agents into public drinking systems. A SCADA-based water system that continuously monitors and logs water quality parameters such as pH, turbidity, chlorine level and dissolved oxygen can quickly detect equipment malfunction, contamination or raw sewage spillage.

■ **Network Security** is an equally important aspect of secure operations and must not be ignored. Traditionally, physical and cyber security were two completely independent functions handled by separate groups in medium to large utilities. Recently, the line separating both functions has disappeared, bringing an increased focus on protecting bricks and bytes. SCADA systems, like all other computer networks, are vulnerable to hacking, intrusions, viruses, loss of data, data alteration and more. The reliance on standard technologies such as common operating systems and networking protocols used by the Internet has dramatically increased vulnerability, even for standalone, non-networked, systems.

Addressing network security starts by identifying all available connections to the SCADA systems, including local access to enterprise networks, remote access via modems and wireless radios and the Internet. Intrusion Detection Systems (IDS) are the first line of defense. IDS are like burglar alarms for the computer network, as they detect unauthorized access attempts. There are basically two types of IDS being used today: Network based (a packet monitor), and Host based which as an example, look at system logs for evidence of malicious or suspicious application activity in real time. Firewalls, when properly configured, provide protection against intrusion at a point of entry. A firewall monitors traffic across the network and

examines every packet of data before allowing it to pass. Remote Access Service (RAS), which allow legitimate users to access the SCADA system from off-site locations, should be in a call back mode only. When an attempt is made by an administrator to dial-in to check alarms or system status, the RAS hangs up and initiates a call back from a pre-configured list of phone numbers. Anti-virus protection software should be deployed and regularly updated on the network to protect the system from virus threats, spyware and keystroke loggers.

The above mentioned tools must be augmented by strict password practices. Modern PLCs/RTUs support multi-level password authorization to protect against program/application changes. Also, PLCs/RTUs can push data using standard protocols such as DNP 3.0 to multiple locations allowing data sharing/dissemination among a number of pre-selected users/operators in a secure environment. Since the user is only allowed to receive the data but can not talk directly to the RTU, the security risk is lower. This scenario is common in oil or gas custody transfer stations.

Authentication, a method by which the system ensures that the user is, in fact, legitimate, is supported by most industrial software applications which normally reside at the central location. A security-based authentication scheme enforces account policies and provides seamless integrated security throughout the system.

Wireless Communications in SCADA systems is another security issue that must be considered. Wireless radio networks that use spread spectrum technology are inherently secure to attacks by outsiders. Spread spectrum radios normally transmit while hopping among a number of unique frequencies in a pseudo-random sequence, making it difficult to intercept. In addition to frequency hopping, most radio manufacturers use a proprietary modulation technique that is not published. Without proper documentation, hackers need very sophisticated and expensive equipment to record and analyze the wireless transmission. For additional security, some radio manufactures encode a unique serial number or identification number into the firmware of the radio, allowing the user to determine which other radios a given site will communicate with. If a radio is stolen, the user can eliminate its serial number immediately from the master radio list, blocking it from accessing the communication traffic. Furthermore, third party Encryptor/Decryptor modules that encrypt data before it gets to the radio network can be deployed for added security.

Leveraging SCADA: Hardening the security of critical infrastructure utilizing existing infrastructure such as SCADA Systems is an attractive value proposition for any utility. Since most utilities have already invested in building SCADA systems, coupling them with strong physical and network security measures is a natural progression. Conducting routine self-assessments and scenario planning can help identify security risks and develop counter measures before incidents occur.

For more information on how SCADA systems can help secure your critical infrastructure, visit www.controlmicrosystems.com.

Sage Designs, Inc.
SCADA & Industrial Automation Products

Free Seminars

Security Seminars

Nov. 8, 2004
Holiday Inn
1050 Burnett Ave.
Concord, CA
1:00 – 5:00 PM

Nov. 9, 2004
Holiday Inn
3400 Shelby St.
Ontario, CA
1:00 – 5:00 PM

Sage Designs, Pure Technologies, Southwest Microwave, and Stantec will be teeming up with guest speakers, Ron Williams and John Saunders to provide two thought-provoking seminars focused on post-9/11 dangers to our country's water supply. These seminars feature speakers who have worked with municipal water utilities to perform vulnerability and risk assessments that were mandated by the EPA after the tragic events of September 11th. These same speakers are now designing security systems utilizing the latest technology for CCTV, access control, biometrics and video surveillance.

Ron Williams, Keynote Speaker

Protecting Against Terrorism – The Insider & Outsider Threat

As a United States Secret Service agent, Mr. Ron Williams operated in two primary arenas: credit card/check fraud counterfeiting, and the Counter Assault Team (CAT) for anti-terrorism addressing threats against the President of the United States. At the time of his retirement, Williams was responsible for all advance security plans and logistics coordination for Presidential, Vice-Presidential, and foreign heads-of-state visits to Los Angeles. He personally protected Presidents Ford, Reagan, Bush, and Clinton, as well as such noted dignitaries as Queen Elizabeth, Yitzhak Shamir, and Pope John Paul. Williams is the recipient of numerous awards, including the U.S. Secret Service Director's Award for Special Achievement on eight occasions.

Because of his expertise in the field of anti-terrorism, Williams was asked by Governor Gray Davis to join a California delegation to meet with Tom Ridge regarding homeland security. His association with AFAUSS (Association of Former Agents of the United States Secret Service), ASIS (American Society of Industry Security), and ATAP (Association of Threat Assessment Professionals) to name a few, keeps him abreast of all matters involving security and threat assessment. He is also an active member of the FBI's InfraGard program, and OCPST (Orange County Private Sector Terrorist Response). A frequent speaker, Williams has made presentations to the California Association of Water Agencies, which included a white paper, and has been called upon numerous times as an expert on terrorism by FOX News.

John Saunders, Guest Speaker

Water and Wastewater Security Problems and Solutions

Water utilities security consultant, John Saunders, of **Enterprise Protection Associates**, is a Certified Protection Professional (CPP), member of the American Society for Industrial Security International, a Certified Information Systems Security Professional (CISSP), and member of the Computer Security Institute. Saunders is qualified in the Risk Assessment Methodology for Water/Wastewater infrastructure (RAM-W) delivered through U.S. Government-Sandia National Laboratories, NM. He has over twenty years experience in policing, corporate security and public safety.

These seminars will conclude with a demonstration of Automated Video Surveillance Technology and a Question & Answer Session.

To Register . . . . . .

Complete a registration form obtained from the Events page on our website (www.sagedesignsinc.com/events/index.htm) or call 1-888-ASK-SAGE to request a faxed registration form. ***There is no charge for this event, but we would appreciate a call if you need to cancel your reservation.***

Pre-registration Required.
Registration Deadline: Nov. 1, 2004

SCADA Seminars

Nov. 8, 2004
Holiday Inn
1050 Burnett Ave.
Concord, CA
8:00 AM - Noon

Nov. 9, 2004
Holiday Inn
3400 Shelby St.
Ontario, CA
8:00 AM - Noon

These seminars are designed to educate utility managers and staff who are planning new, upgraded, or replacement SCADA systems. Guest speakers will be on hand to present and discuss issues and products for a modern, secure, open architecture system.

Keynote Speakers

Tony Burgarino, Ph.D., P.E. *Concord Seminar*
Project Manager, Carollo Engineers, Walnut Creek, CA
Planning for a Radio Telemetry System
Planning for a radio telemetry system means different things to managers, designers, and users. Dr. Burgarino will discuss objectives for implementing a successful system fromthese these perspectives.

Gene Heyer, P.E. *Ontario Seminar*
Control Systems Engineer, Carollo Engineers, Fountain Valley, CA
Evolving SCADA Systems: Functional Integration of Security, Surveillance, GIS, Modeling, MCC and by the way, Supervisory Control and Data Acquisition
Mr. Heyer's presentation will examine recent SCADA system applications that integrate security, video surveillance, GIS, modeling and field instrumentation into the SCADA system design. The objective is to look at real life current applications and evaluate the effectiveness of some new technology. This will show the variety of uses for traditional "SCADA" systems made possible by current developments in software and computer technology.

Other Presentations

- Learn about DNP Protocol and see the latest Control Microsystems products — the Wireless Series of SCADAPacks. These products have been designed with open architecture and open protocols in mind, and have been ruggedized for severe environmental conditions. The Control Microsystems' SCADAPack line has been proven in SCADA systems throughout the west and the world.
- Learn about licensed and unlicensed radios and how they can provide reliable communications throughout your SCADA system. See the Locus High-Speed Ethernet Spread Spectrum radio, with over-the-air data rates of up to 11 Mbps and range of up to 20+ miles.
- See a range of security and surveillance products, featuring IVC PTZ security camera and the PureLink Automated Surveillance & Alarm Management Systems from Pure Technologies.
- See a demonstration of the newest version of National Instruments' Lookout SCADA software, Version 6.x, which is powerful, yet easy to configure. Lookout provides all the flexibility and power of the other top HMI/SCADA products, without the complexity that generally accompanies this type of program.

To Register . . . . . .

Complete a registration form obtained from the Events page on our website (www.sagedesignsinc.com/events/index.htm) or call 1-888-ASK-SAGE to request a faxed registration form. ***There is no charge for our SCADA Seminars, but we would appreciate a call if you need to cancel your reservation.***

Pre-registration Required.
Registration Deadline: Nov. 1, 2004

Sage Designs, Inc.
SCADA & Industrial Automation Products

Training Classes

SCADAPack & Ladder Logic Training Class

October 26-28, 2004
Long Beach, CA

Sage Designs is holding a 3-day, factory-certified, training course designed for people evaluating an economical way to implement a new or upgraded SCADA system, or for people wanting to best utilize their Control Microsystems' SCADAPack controllers. An optional SCADAPack or SCADAPack32 is available at a special price with the course — an excellent way to get started using Control Microsystems' Controllers.

Instructor: Tony Sannella, Sage Designs, CMI factory-certified instructor.

Location: Holiday Inn/Long Beach Airport, 2640 Lakewood Blvd., Long Beach, CA. *Those requiring overnight hotel accommodations may book a room at the Holiday Inn by calling the hotel directly at 562-498-5411 to make your reservations.*

Who should attend? Individuals interested in participating in a highly technical, in-depth course on Ladder Logic and how it applies to Control Microsystems' products.

What should I bring? It is a requirement of the course to bring a Laptop Computer – minimum of Win98 with 15mb free disk space, CD-ROM and serial port.

What is provided? Daily breakfast and lunch, coffee, soft drinks and snacks during the breaks.

Cost:

3-Day Training Class without a SCADAPack Demo	$ 975
3-Day Training Class with a SCADAPack SPT Demo*	$ 1,700
3-Day Training Class with a SCADAPack SPT32 Demo*	$ 1,800

** SPT Demo, a $3,180 value, consists of a SCADAPack Controller with extra RAM (#P1-120-01-0-0), TelePACE Ladders, Hardware Manual (on CD-ROM), 5699 I/O Simulator board, AC/2 Transformer, & programming cable. SPT32 Demo, a $3,960 value, consists of a SCADAPack32 Controller (P4-100-01-0-0), TelePACE Ladders, Hardware Manual (on CD-ROM), 5699 I/O Simulator board, AC/2 Transformer, & programming cable. Demos will be shipped N/C to training facility. (Sales taxes are payable on the demo portion of the class.)*

To Register . . . . . .

Complete a registration form obtained from the Events page on our website (www.sagedesignsinc.com/events/index.htm) or call 1-888-ASK-SAGE to request a faxed registration form.

Seating is limited to 15 students.
Registration Deadline: October 1, 2004

Lookout Training Classes

Lookout Basics — **Nov. 2-3 2004**
Lookout Advanced — **Nov. 4-5, 2004**
Mill Valley, CA

Sage Designs is holding two 2-day Lookout Training classes in November at our Mill Valley office. The Basic training unit will provide someone familiar with computers and your SCADA system's functions the necessary knowledge to enhance and customize the existing application to better suit your needs. The advanced course will provide the necessary knowledge for students to expand a Lookout system to accommodate new RTUs, migrate an older Lookout application to allow access to new features provided by current Lookout versions, allow for redundancy, produce reports and serve web-based clients.

Instructor: Tony Sannella, Sage Designs, National Instruments' factory-certified instructor.

Location: Sage Designs, 150 Shoreline Highway, Building A, Suite 8, Mill Valley. *Those requiring overnight hotel accommodations may book a room at the Holiday Inn Express next door (160 Shoreline Hwy) by calling 415-332-5700.*

Who should attend? Individuals interested in participating in a highly technical, in-depth course on National Instruments' Lookout HMI/SCADA software. Class size is limited to 6.

What should I bring? It is a requirement of the course to bring a Laptop Computer – minimum of Windows 2000 with 15mb free disk space, CD-ROM and serial port.

What is provided? Daily lunch, coffee, soft drinks and snacks during the breaks; Demo copies of the current version of Lookout; Modbus-compatible RTU/PLCs for the training exercises; Lookout course guides, including hands-on exercises for all portions of the Basic course.

Cost:

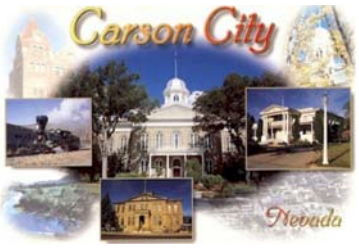
2-Day Lookout Basic Training Course	$ 1,500
1½--Day Advanced Lookout Training Course	$ 1,200
Both Lookout Basic & Advanced Courses	$ 2,400

To Register . . . . . .

Complete a registration form obtained from the Events page on our website (www.sagedesignsinc.com/events/index.htm) or call 1-888-ASK-SAGE to request a faxed registration form.

Seating is limited to 6 students.
Registration Deadline: Oct. 22, 2004

Sage Siting



Carson City SCADA System

The Nevada Capitol, Carson City, sits at the eastern edge of the Sierras just south of Reno, in Carson Valley, Nevada. In order to supply water to the 56,000 residents, the water system has 27 wells, 10 water tanks, 7 boosters (two of which have 3 booster pumps each) and a water treatment plant. VHF radio links all of the sites to the central office located adjacent to the city's wastewater treatment plant.

One of the problems facing the City in the implementation of the SCADA system was the wide range of climatic conditions. The RTUs chosen for the system had to be able to withstand summer highs often over 100º F and winter lows that can fall below 0º F, with an average winter snowfall of 22". Another factor in choosing the remotes was the need to accommodate solar powered units on 7 of the water tanks.

Using the Control Microsystems' RTUs allowed the city a cost-effective solution to each of these problems. The environmental specs on the units allows for temperatures ranging from -40º F to 158º F, and when the question of power savings was the issue, the RTUs were programmed to use their sleep mode, reducing the power draw to 10 mA during most of their operation. The sleep mode is used to power-down the RTUs for 15 minutes, at which time they "wake up" and wait for a poll from the master RTU. Once polled, they repeat this cycle. If no poll is received for 30 minutes, they then revert to the sleep mode for one hour and try again for 30 minutes, repeating this cycle until normal polling resumes. The city has also connected the battery voltage in these units to an analog input that allows them to monitor the health of the batteries, providing information about the buildup of snow on the solar panels.

Recently, the city has added some Locus OS2400-HSE Ethernet radios to connect the HMIs at the water treatment and wastewater treatment plants to the central office over an 11 Mbps link that reaches 8 miles across town. A forth radio will soon include the connection of the landfill to the city's network, and provide for live video feeds from their security cameras.

At this point, there are over 50 Control Microsystems' RTUs in the system ranging from the older TeleSAFE 6000 and VS2 Series, up to the most current SCADAPack 32.

— Alan Kotsull, City of Carson City Utilities Operation

What's New in Lookout 6

National Instruments' Lookout continues to be the easiest HMI program to configure, and the new 6 version continues to prove this with a number of enhancements. A floating toolbox, the ability to export a CSV file with all objects and more control of the archived data make the development of a system and management of archived data easier than ever. The following additions and changes are a partial list of enhancements in Lookout 6.

New Toolbox

The new floating toolbox in Lookout gives you quick access to some of the most common menu commands and objects.

New Object Explorer Icons

New distinctive icons help you identify different objects in the Object Explorer and anywhere the Lookout object navigation tree appears.

Diagnostics Menu Option Added for Ethernet Objects

When you create a driver object that communicates via Ethernet, an Options»Ethernet Object Options menu item appears so that you can choose to generate a diagnostic file.

New HyperTrend Data Members

Start, StartTime, CursorPos

New CitadelControl Remote Archiving

In Lookout 6, you now can archive data remotely with the CitadelControl object. You cannot do that in Lookout 5.1 or earlier.

New Menu Items File»Export Process Data Members

Edit mode only. This command exports all data members used in a process to a CSV file.

***A friendly reminder to our Lookout users**: This would be a good time to make sure that you have a current Software Subscription Plan (SSP) for your Lookout licenses. An SSP entitles you to receive priority technical phone support and all upgrades that occur within a 12-month period. Call Sage Designs @ 888-ASK-SAGE to renew or add this benefit.*

The Sage Advisor

SCADA, SECURITY & AUTOMATION NEWSLETTER

Seminars & Events

Sept. 13	***CA-NV AWWA Northern Regional Training Conference***, Sparks, NV.
Sept. 14	***San Diego County Water Works Group***, 2004 Vendor's Fair, Poway, CA.
Sept. 14	***Surveillance over Wireless SCADA Systems*** session by Sage Designs, at the CA-NV AWWA Northern Regional Training Conference, Sparks, NV.
Oct. 12-13	***CA-NV AWWA Annual Fall Conference,*** American Water Works Association, Sacramento, CA.
Oct . 26-28	***SCADAPack Training Class*,*** Long Beach, CA.
Oct . 27-29	***2004 Water Quality Conference,*** sponsored by East Valley Water District & AWWA Research Foundation, Ontario, CA.
Nov. 2-3	***Lookout 2-Day Basics Course****, Mill Valley.
Nov. 4-5	***Lookout 1½-Day Advanced Course*,*** Mill Valley.
Nov. 8	***Free SCADA Seminar****, Holiday Inn, Concord, CA, 8-Noon.
Nov. 8	***Free Security Seminar for Water Utilities*,*** Holiday Inn, Concord, CA, 1-5 PM.
Nov. 9	***Free SCADA Seminar*,*** Holiday Inn, Ontario, CA, 8-Noon.
Nov. 9	***Security Seminar for Water Utilities*,*** Holiday Inn, Ontario, CA, 1-5 PM.
Dec. 1-3	***ACWA Fall Conference***, Association of CA Water Agencies, Palm Springs, CA.
Feb 2005	***SCADAPack Training Class*,*** Mill Valley, CA. (TBA)
Mar 30	***United States Committee on Irrigation & Drainage (USCID) 3rd Annual Conference***, San Diego, CA.
May 10-13	***California Rural Water User Association (CRWUA), 3rd Annual Operator Expo***, Lake Tahoe, CA.

** Download the **registration form** from our website or call for more information.*

Sage Designs, Inc.
SCADA & Industrial Automation Products
150 Shoreline Hwy., Suite #8A
Mill Valley, CA 94941-3634

PRESORTED
STANDARD MAIL
US POSTAGE PAID
POINT TO POINT

Address Service Requested