SCADA Systems 2012
Integrating SCADA and IT Assets – Business, Security and Reliability Implications

www.scadaaustralia.com.au

Main Conference: 14th & 15th August 2012
Workshops: 14th & 15th and 16th August 2012
Venue: Hilton, Sydney

Speaker Line Up

Graeme Russ
Principal SCADA and Telemetry Engineer
Hunter Water Australia

Tendai Chadyiwa
OT Architecture Engineer
Ergon Energy Corporation

Andrew Lavelle
Project Manager
ISMART Program
State Water Corporation

Andrew West
Chair
DNP TECHNICAL COMMITTEE

Marty Edwards
Director - Control Systems Security
U.S. Department of Homeland Security

Paul Elliot
Manager Systems Operations
Horizon Power

Peter Bouras
Independant Consultant

Ervin Fekovic
Strategic Planner - Secondary Systems
United Energy and Multinet Gas

Patrick Whittington
SCADA Systems Control Officer
Cairns Water

David Bowerman
Manager Electrical & SCADA Engineering
Hunter Water Australia

Andrew Bain
Security Engineer
Transend Networks

Adrian Merkel
Network Operational Control System Manager
Transend Networks

Akhtar Kalam
Prof Energy Systems
Victoria University
Dear SCADA Engineer,

Are you finding that SCADA integration leaves your system open to cyber threats?

Energy & Utilities IQ’s SCADA System is running for the 5th year, consistently delivering a perfect platform for SCADA engineers, IT Architects, Control Systems Professionals to benchmark their SCADA upgrades and advances.

In 2012 the event will tackle some of the most persistent, but not unsolvable issues in SCADA Systems:
- Protecting SCADA Systems from cyber and physical threats
- Fully integrating SCADA System into corporate system
- Improving system reliability and minimising downtime

This should tick all the boxes as to why you should attend the event on 14th & 15th August 2012 in Sydney.

- Hear real case studies on the hottest topics
- Meet relevant delegates for networking
- Learn from experienced industry speakers

I’m looking forward to seeing you in August!

Kind Regards,

Dajana Dikic
Director
Energy & Utilities IQ

Who Will you Meet at Our SCADA Systems?

- SCADA and Communications Engineers
- IT Security Engineers
- Operation Systems Managers
- Distribution Manager
- Asset Manager
- Network Operations Managers

From Transmission & Distribution, Energy Generation, Water Utilities and Mining Companies

“bringing these disparate systems together, new challenges arise which are greater than the sum of the challenges faced by individual systems”

Graeme Russ
Principal SCADA and Telemetry Engineer
Hunter Water Australia Pty Limited
9.00 Opening Remarks from the Conference Chair

9.10 Enhancing Cyber-Security in Control System Communications
Measures to enhance the cyber-security posture of the interface between control systems and corporate IT networks are fairly well understood, but the process or field interface is often ignored. A number of tools and techniques can be applied to control system fieldbus or SCADA networks.

This presentation describes some techniques provided in standards for addressing threats to the control network and mitigations specifically targeted to process control and SCADA communications. In particular, the distinctions between encryption and authentication are explained and the use of stateful deep-packet-inspection firewalls is discussed.

Andrew West
Chair
DNPC TECHNICAL COMMITTEE

9.50 A Holistic Approach to Securing Integrated SCADA and IT Assets
It is well recognised that without effective corporate governance, deployed security solutions will be tactical responses, providing point solutions to meet immediate subordinate needs, which but which typically will not meet the long-term needs of the business as a whole. Such tactical solutions may not scale to meet emerging requirements and may not even integrate with all of the other components of the business infrastructure. This lack of strategic planning and response will undoubtedly cost the business real financial and market returns, through increased operations requirements, lack of integration and failure to realise the full potential of the individual system components.

This presentation looks at the whole picture of securing integrated SCADA and IT systems, providing a top-down approach, starting at the business requirements and considering the SCADA and IT systems in their roles as tools supporting the business requirements.

Dr David Ross
Chief Information Security Officer
BRIDGE POINT COMMUNICATIONS

10.30 Morning Refreshments and Networking Break

11.00 PANEL DISCUSSION: Enforcing Automated Scanning Software to Maintain System Compliance
- Coordinating work between SCADA engineers and IT engineers
- Introducing heavier scans on less critical systems and leveraging redundancy to ensure no system downtime
- Recurring security assessments and evaluation should it encompass internal and external network segments and application and network layers
- Re-evaluate risk reduction goals to ensure continuous improvement

Andrew Lavelle
Project Manager IMSMART Program
STATE WATER CORPORATION
Patrick Whittington
SCADA System Control Officer
CAIRNS WATER
David Bowerman
Manager Electrical & SCADA Engineering
HUNTER WATER AUSTRALIA

11.40 Distribution Automation over Advanced Metering Infrastructure (AMI)
- Leveraging on the Smart Meter investment for Distribution Automation purposes
- Increasing resilience to field communications
- Transitioning to an intelligent utility

Ervin Fekovic
Strategic Planner - Secondary Systems
UNITED ENERGY AND MULTINET GAS

12.20 Lunch and Networking Break

13.20 ROUNDTABLE DISCUSSION: Understanding How SCADA Interacts With the Corporate Network and what Measures Must be Implemented to Separate these Networks
- Reviewing how SCADA can coexist with a business network environment
- Evaluating best practices of building virtual security in a business network environment
- Examining the connections between SCADA and business systems and how you can put security in place without affecting your business processes
- Considering the types of firewalls available for segregating the SCADA and corporate network and where these should be placed

Facilitated by the Conference Chair

14.00 Transend’s Approach to Managing the Security Risks around Scada and Engineering Networks with a look at Corporate Integration
- Transend methodology for managing risk for cyber security.
- IT vs OT or IT and OT, the impact of culture on security.
- Collaborative documentation on standards and companywide responses.
- Transend’s Cyber security
- White listing of Applications and networks.
- Implementation of network segmentation.
- IDS vs IPS
- Implementation of security audit recommendations

Andrew Bain
Security Engineer
TRANSEND NETWORKS

14.40 Afternoon Refreshments and Networking Break

15.10 Conducting a Thorough Risk Analysis of the Necessity of each Connection to the SCADA Network
- Developing a comprehensive understanding of all connections to the SCADA network, and how well these connections are protected
- Identifying and evaluating all types of connections: Internal local area and wide area networks, including business networks
- Assessing and auditing all business networks (e.g. the internet, wireless network devices, satellite uplinks, modem or dial-up connections, connections to business partners, vendors or regulatory agencies)

Tendai Chadyiwa
OT Architecture Engineer
ERGON ENERGY CORPORATION

15.50 ROUNDTABLE DISCUSSION: Examining the Long Term Goals of Smart Grid Standards to Determine how the Industry will have to Adapt
- Identifying what constitutes a critical situation and what your critical cyber assets are to determine what security measures must be implemented
- Providing an insight into how threat profiling can be used to relate to what government agencies are seeing as a threat
- Outlining the problems associated with cyber security best practice versus regulatory compliance
- Fully implementing a compliant risk management framework

Facilitated by the Conference Chair

16.30 Networking Drinks & Conference Day One Close

17.00 Workshop A: How Will Smart Grids Affect SCADA? – A Comprehensive Workshop that Highlights the Key Role SCADA Will Play in the Future Success of Smart Grids
13.20 IEC61850 Fundamentals
This is designed for delegates to upgrade their knowledge and understanding of the functions and applications of the new international standard for substation communications i.e. IEC 61850. This standard will completely change the ways protection, control, monitoring and recording has been traditionally done in the substation. The standard for communication networks and systems in substations also allows the development of high-speed peer-to-peer communications based distributed protection applications that result in significant changes in the ways protection functions are implemented. This replacement of functions implemented in a single device with equivalents using exchange of analog and status information over the substation local area network has revolutionized the conventional power system protection.
- Recognise the role of communications in power systems and identify various communication requirements needed in power system protection and distribution networks
- Outlining a basic understanding of the use of communication media and architectures in power systems
- Understand the value of what global organisations like IEC and EPRI bring to the development of new technologies and structures for the advancement of power systems
- Comprehending system automation and integration concepts
- Demonstrating a basic knowledge about the communication standards, protocols and architectures most commonly employed in power system protection and distribution networks

Akhtar Kalam
Prof Energy Systems
VICTORIA UNIVERSITY

14.20 Afternoon Refreshments and Networking Break

14.50 CASE STUDY WHYDAM POWER STATION
- Challenges of operating SCADA systems in remote areas
- Overcoming communication issues
- Delivering uninterrupted power to remote areas

Paul Elliot
Manager Systems Operations
HORIZON POWER

15.30 ROUNDTABLE DISCUSSION: Improving Operational Reliability, Reducing Costs Through Eased Workforce Requirements and Enhancing Overall Quality of Service
- Analysing SCADA system component connectivity to determine availability of SCADA control
- Best strategies to minimise downtime outage with hot – standby equipment
- Defining project and technical specification to ensure higher reliability and shorter downtime
- Delivering continuous service through system readiness

Facilitated by the Conference Chair

16.10 Closing Remarks from the Chair and End of Conference

16.30 Workshop B: Integrating SCADA and Corporate ICT Systems Considerations, Challenges and Solutions
Workshop A: 14th August 17.00 – 20.00
Integrating data from different sources: IEC 61850 and DNP3

The Smart Grid is a complex system of systems. An EPRI report has identified many different sectors and applications that need to cooperate, with over 40 relevant standards currently being used for various applications. Unfortunately, major obstacles still exist in sharing information between what were previously separate silos. A major works program is currently underway in many standards development organizations to address the need to integrate information and functionality between different areas, in order to allow true integration of these subsystems. One of these activities is near completion: The publication of a new standard, IEEE 1815.1, that defines rules for consistent (and possibly automatic) mapping of data between IEC 61850 and DNP3. This guide is seen as critical to enable integration of new substation automation technologies based on IEC 61850 into the North American power grid where DNP3 is widely used for SCADA.

This workshop looks at what is (and is not) covered by IEEE 1815.1, how it will be used and how to immediately apply its principles to current projects integrating IEC 61850 substation automation systems into Australian utility networks.

FACILITATED BY
Andrew West, Chair, DNP TECHNICAL COMMITTEE

Andrew is an electrical engineer has worked with SCADA systems software for 30 years. His career has included working with electric power utilities, control system product vendors and SCADA software suppliers, consulting and training. He has been involved in SCADA protocol standards since 1996, contributing to Australian and international SCADA standards. He is the spokesperson for the IEC TC57 WG03 committee that is responsible for SCADA standards and WG19, looking at the application of IEC 61850 for substation to control centre applications. He chairs the DNP Technical Committee and has been working with the IEEE committees responsible for the adoption of DNP3 as an IEEE standard and for the development of a mapping between DNP3 and IEC 61850.

Andrew is a frequent contributor to the SCADA maillist and discussion lists on control systems and ICS cyber-security. His interests span all areas of control system communication integrity and cyber-security.

Workshop B: 15th August 16.30 – 19.30
Integrating SCADA and Corporate ICT Systems – Considerations, Challenges and Solutions

The workshop will provide a detailed overview of the key factors that need to be considered when integrating SCADA and IT environments. Integrating SCADA and IT systems is highly organisation specific - participants are encouraged to use this workshop to share their individual experiences, problems and solutions. The objective of the workshop is to highlight the continually evolving field of inter-system integration. While the primary focus of the workshop will be the integration of SCADA and corporate IT systems, additional consideration will be given to:

• Asset and maintenance management systems
• Utilising 3rd parties (e.g. for out-of-hours alarm monitoring)
• Desktop applications within the SCADA environment
• Publishing data beyond the organisation

The following issues will be explored:

• Benefits and risks associates with linking SCADA and IT systems
• Risk mitigation – Network design, procedures, protocols
• Identifying what to link – Data, visualisation, control
• Data transfer mechanisms – Completely manual to fully automated
• Scalability considerations

FACILITATED BY
Graeme Russ, Principle SCADA and Telemetry Engineer, Hunter Water Australia

Graeme currently holds a position as Principle SCADA and Telemetry Engineer for Hunter Water Australia. Graeme has over ten years of experience with SCADA / Telemetry systems and the integration of these systems with other Corporate IT systems. Graeme’s experiences range from simple manual data transfers through to customised SCADA software integrating with RDMS and Web Services providing high-level integration of SCADA and IT systems.

ABOUT OUR SPONSORS

Sourcefire, Inc. (NASDAQ: FIRE), a world leader in intelligent cybersecurity solutions, is transforming the way global large- to mid-size organizations and government agencies manage and minimize network security risks. With solutions from a next-generation network security platform to advanced malware protection, Sourcefire provides customers with Agile Security™ that is as dynamic as the real world it protects and the attackers against which it defends. Trusted for more than 10 years, Sourcefire has been consistently recognized for its innovation and industry leadership with numerous patents, world-class research, and award-winning technology. Today, the name Sourcefire has grown synonymous with innovation, security intelligence and agile end-to-end security protection. For more information about Sourcefire, please visit www.sourcefire.com.

MTL Instruments, a division of Cooper Crouse - Hinds, is a world leader in the development and supply of electronic instrumentation and protection equipment for the process control and telecommunications industries. Many of the world’s critical processes are monitored, controlled or protected by MTL equipment, and the Group is distinguished by the quality and reliability of its products, its global network of sales and support centres and its acknowledged position as a thought leader in this high technology marketplace.

NetComm Wireless Limited (ASX:NTC) is a leading developer of innovative broadband products for telecommunications carriers and ISPs worldwide. Specialising in fixed and mobile broadband technologies, NetComm Wireless customises products to successfully deliver the performance capabilities of world-leading carrier networks to home, business and industrial applications. Customer premises Equipment (CPE) and Edge Technologies are specifically designed to extend a reliable connection to fringe service areas globally. For 30 years NetComm Wireless has engineered a solid portfolio of world-first data communication products and is today a world renowned developer of HSPA+, LTE, machine-to-machine (M2M) and fibre access devices. Headquartered in Sydney, Australia, NetComm Wireless has offices in New Zealand, Canada and the Middle East. For more information about NetComm Wireless visit www.netcommwireless.com

BOOK NOW!  T +61 2 9229 1000  F +61 2 9223 2622  E registration@iqpc.com.au  W www.scadaaustralia.com.au
networks and 30% by underground networks. The size and sophistication in Victoria, 70% of outages are believed to be attributed by overhead networks and 30% by underground networks. The size and sophistication of power systems has increased the failure to locate faults, therefore heightened the importance of fault location. When a fault occurs on a transmission line, it is crucial for the fault location to be identified as accurately as possible, allowing the damage caused by the disturbance to be repaired quickly before the line is put back into service. The average duration for an overhead fault to be repaired is 50-55 minutes, while an underground fault is approximately 65 minutes.

For this reason, engineers ever since the development of the earliest microprocessor based Intelligent Electronic Devices (IEDs), have depended on digital superiority to assist personnel in the precise location of faults. The ability of these IEDs to generate an abundance of valuable network data through information exchange of relays, permits power authorities to capitalise in areas such as control, protection, monitoring, fault recording and communication. The majority of in service substation protocols are still based on MODBUS and DNP3 standards. These standards however are slowly becoming replaced by Ethernet and fibre optic technologies in the form of the IEC61850 protocol.

The workshop challenge is to configure, derive and test a new overhead fault location algorithm using the portable IEC61850 testing unit. The objectives will include:

1. Using a series of vendor specific proprietary tools (i.e. AcSELErator Quickset, AcSELErator Architect, MICOM S1 Studio, PCM600, CCT, QuickCMC and IED Scout) to modify existing ICD files of IEDs. The sender and receiver of GOOSE messages must be specified. At the end of the entire description process the GOOSE messages are stored in a SCD file. Each of the proprietary tools must be able to import the SCD files and extract the information needed for the necessary IEDs. OMICRON's CMC256 test set may be used to capture GOOSE messages.
2. Developing an innovative algorithm for accurate fault location in overhead transmission lines using a time domain method (i.e. Travelling Waves). The algorithm should draw attention to the application of unsymmetrical single phase-to-ground faults by modelling the positive, negative and zero sequence circuits.
3. Practical simulation using the CMC256 or CMC356 test set to inject current and voltage signals.

FACILITATED BY:

Marty Edwards, Director - Control Systems Security
U.S. Department of Homeland Security

Marty Edwards is the director of the U.S. Department of Homeland Security’s (DHS) Control Systems Security Program (CSSP). CSSP is part of DHS’s National Cyber Security Division. CSSP works to reduce industrial control system risks within and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local and tribal governments, as well as industrial control systems owners, operators and vendors. The Control Systems Security Program also operates the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The ICS-CERT responds to and analyzes control systems related incidents, conducts vulnerability and malware analysis, and shares and coordinates vulnerability information and threat analysis through products and alerts.

Mr. Edwards has over 20 years of experience and brings a strong industrial control systems industry focus to DHS. Before coming to CSSP, Mr. Edwards was a program manager focused on control systems security work at Idaho National Laboratory. Prior to his work at the laboratory, Mr. Edwards held a wide variety of roles in the instrumentation and automation fields, including field service, instrument engineering, control systems engineering and project management.

Mr. Edwards has also held various positions in non profit organizations, including Chairman of the Board for one of the automation communities’ largest user group conferences. Mr. Edwards holds a diploma of technology in Process Control and Industrial Automation (Magna cum Laude) from the British Columbia Institute of Technology.
Registrations received without payment or a Government PO will incur a processing fee of $99 + GST = $108.90 per registration. Payment prior to the conference is mandatory. NOTE: PAYMENT IS DUE WITHIN 7 DAYS FROM REGISTRATION TO SECURE YOUR PLACE. Registrations received without payment or a Government PO will incur a processing fee of $99 + GST = $108.90 per registration. Payment must be received by IQPC prior to 5pm AEST on the cut-off date.

To amend your current details, advise of duplicates or to opt out of further mailings, please contact our Database Integrity Maintenance Department, IQPC products and services. From time to time IQPC may share information from our database with other professional organisations (including our event sponsors) to promote similar products and services. Please tick the box below if you do NOT want us to pass on your details.

Any information provided by you in registering for this conference is being collected by IQPC and will be held in the strictest confidence. It will be added to our database and will be used primarily to provide you with further information about IQPC events and services. By supplying your email address and mobile telephone number you are agreeing to IQPC contacting you by these means to provide you further information about IQPC products and services. From time to time IQPC may share information from our database with other professional organisations (including our event sponsors) to promote similar products and services. Please tick the box below if you do NOT want us to pass on your details.

To speed registration, please provide the priority code located on the mailing label or in the box below.

To take advantage of these rates & book direct on the website, please go to www.scadaaustralia.com.au and click on the Venue & Accommodation page.

IQPC recognises the value of learning in teams. IQPC Cancellation and Postponement Policy: For details of IQPC’s Cancellation and Postponement Policy please visit: www.iqpc.com.au © 2011 IQPC ABN 92 071 142 446 All Rights Reserved. The format, design, content and arrangement of this brochure constitute a copyright of IQPC. Unauthorised reproduction will be actionable by law.

### TEAM DISCOUNTS
IQPC recognises the value of learning in teams.

**Discounts are available for multiple registrations.**

- **Register a team of 3 to the conference at the same time from the same company and receive a 50% discount.**
- **Register a team of 4 to the conference at the same time from the same company and receive a free pass for a 5th delegate.**

**Ask about multi-event discounts.** Call +61 2 9229 1000 for more details.

Please note: Only one discount applies.

### ACCOMMODATION
The Lido Group are the official booking agent for the SCADA Systems 2012 event.

To take advantage of these rates & book direct on the website, please go to www.scadaaustralia.com.au and click on the Venue & Accommodation page.

### PACKAGES

<table>
<thead>
<tr>
<th>Packages</th>
<th>Early Bird <em>Register &amp; pay before 15th May 2012</em></th>
<th>Early Bird <em>Register &amp; pay before 5th June 2012</em></th>
<th>Standard Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Only</td>
<td>$2999 + GST = $3298.90</td>
<td>$3299 + GST = $3628.90</td>
<td>$3499 + GST = $3848.90</td>
</tr>
<tr>
<td>Conference + 1 Workshop</td>
<td>$3289 + GST = $3525.90</td>
<td>$3569 + GST = $3925.90</td>
<td>$3769 + GST = $4125.90</td>
</tr>
<tr>
<td>Conference + 2 Workshop</td>
<td>$4389 + GST = $4716.70</td>
<td>$4789 + GST = $5116.70</td>
<td>$5089 + GST = $5516.70</td>
</tr>
<tr>
<td>Conference + 3 Workshop</td>
<td>$5389 + GST = $5725.70</td>
<td>$5789 + GST = $6125.70</td>
<td>$6089 + GST = $6525.70</td>
</tr>
<tr>
<td>Conference + 4 Workshop</td>
<td>$6095 + GST = $6420.50</td>
<td>$6395 + GST = $6730.50</td>
<td>$6695 + GST = $7040.50</td>
</tr>
</tbody>
</table>

*Payment must be received by IQPC prior to 5pm AEST on the cut-off date.

### PRIVACY - YOUR CHOICE
Any information provided by you in registering for this conference is being collected by IQPC and will be held in the strictest confidence. It will be added to our database and will be used primarily to provide you with further information about IQPC events and services. By supplying your email address and mobile telephone number you are agreeing to IQPC contacting you by these means to provide you further information about IQPC products and services. From time to time IQPC may share information from our database with other professional organisations (including our event sponsors) to promote similar products and services. Please tick the box below if you do NOT want us to pass on your details.

### PLACES AVAILABLE

<table>
<thead>
<tr>
<th>Delegate 1</th>
<th>Delegate 2</th>
<th>Delegate 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early Bird</td>
<td>Early Bird</td>
<td>Early Bird</td>
</tr>
<tr>
<td>$3299 + GST</td>
<td>$3569 + GST</td>
<td>$3769 + GST</td>
</tr>
<tr>
<td>$3628.90</td>
<td>$3925.90</td>
<td>$4125.90</td>
</tr>
<tr>
<td>$3848.90</td>
<td>$4125.90</td>
<td>$4398 + GST = $4837.80</td>
</tr>
<tr>
<td>$3848.90</td>
<td>$4125.90</td>
<td>$4398 + GST = $4837.80</td>
</tr>
</tbody>
</table>

2 WAYS TO SAVE!

- Book early to receive huge EARLY BIRD savings.
- Book as a team, save and benefit as a team.

**Quick and Easy Ways to Register**

- **Telephone:** +61 2 9229 1000
- **Fax:** +61 2 9223 2622
- **Email:** registration@iqpc.com.au
- **Website:** www.scadaaustralia.com.au
- **Mail:** IQPC, Level 6, 25 Bligh Street, SYDNEY NSW 2000

### Organisations

- **Address:**
- **Postcode:**

**Telephone:**

**Fax:**

**Approving Manager:**

**Position:**

**Email:**

**Check Enclosed for $**

**Please make cheques payable to IQPC.**

**Please Charge:**

- American Express
- Visa
- MasterCard
- Diners Club

**Credit Card Number:**

**AMEX 4 Digit Code:**

**Expiry Date:**

**Name of Card Holder:**

**Please Print:**

---

**SCADA Systems 2012**

Integrating SCADA and IT Assets – Business, Security and Reliability Implications

www.scadaaustralia.com.au