# Remote Monitoring and Control Conference (REMOTE 2015)

Las Vegas, Nevada, USA
5-6 November 2015

ISBN: 978-1-5108-1545-2

**Printed from e-media with permission by:**

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571


**Some format issues inherent in the e-media version may also appear in this print version.**



Printed by Curran Associates, Inc. (2016)



Webcom Communications
7355 E. Orchard Road, Suite 100
Greenwood Village, Colorado 80111

Phone: 800-803-9488
Fax: 720-528-3771

general@webcomcommunications.com

**Additional copies of this publication are available from:**

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

# Conference Program

**Exhibit Hall Hours**
Nov. 5th – 10:00 am – 6:00 pm
Nov. 6th – 8:00 am – 12:00 pm

**Thursday, Nov. 5th 2015**

7:00 am – Registration and Continental Breakfast

8:30 am – Keynote
**M2M: Remote Monitoring and Control – Multi-National Deployments…..1**
As more and more devices become "internet aware", manufacturers are developing platforms to enable peer to peer communication for many devices thus producing new and unique solutions for all types of customers and partners. In order to develop a strategy that capitalizes on this trend of IOT/M2M technology, companies need to secure and develop key capabilities including physical and human networks, remote and centralized data visualization, big data analytics and much more.

M2M deployment could be very complex, which requires hardware procurement and development, connectivity management as well as vertical application delivery. In addition, it is important to manage M2M environment with management platform, which is capable of providing near real time information on wireless security, detailed network information, provisioning, reporting and much more.

During the session, we will demonstrate a single source of information that allows all companies with the industrial ecosystem salient information to build complex solutions by referring to specific use cases.

*Larry Tichavksy, M2M Application Engineer/Solution Architect – Vodafone M2M*

9:15 am
**The Industrial Internet Delivering Real Outcomes…..15**
The Industrial Internet helps manufacturers connect their machines, which then gather data and insights that can empower operators and business managers to make smarter, more informed decisions to save time and money. Taking advantage of secure cloud services has provided a jump start to expand many manufacturers' current revenue streams.

For example, TempuTech, an OEM of grain processing equipment for manufacturing, incorporated a cloud-based remote monitoring and mobility solution from GE Intelligent Platforms in its grain processors. This has driven business growth as they can now provide customers with asset monitoring capabilities through a subscription-based cloud service. The cloud-based solution quickly and cost-effectively transforms raw data into actionable information, maximizing operational efficiency, productivity and profitability.

This presentation will discuss how industrial OEMs can leverage cloud-based remote monitoring for business growth, enabling greater value to their customers.

*Ken Crawford, Chief Innovation Officer – GE Intelligent Platforms*

10:00 am – Networking Break/Exhibit Hall Opens

11:00 am

**The "App Revolution" is coming to SCADA – or is it?…..27**

Today's app environment, embracing rich HTML5 UI and performant back-end systems designed to scale as big as the Internet, enables some power gen SCADA/HMI vendors to quickly and flexibly evolve their products to meet the changing needs of the generation industry, while at the same time reducing the need for expensive professional services projects – projects which are all too common with the legacy approaches.

We will explore deeply the web-technology "stack," including the latest advances from Google, Facebook, and other high-scale software leaders. This stack is then shown to apply in a carefully architected OT framework, designed to maintain or exceed NERC CIP requirements, yet support rapid development and deployment of secured UI displays, enabling monitor and control of an increasingly complex grid. Both Generation and Transmission as well as Distribution use-cases will be considered. Special attention will be paid to the increasing demand on OT software as grid diversity and power flow complexity grow.

*Brad Harkavy, General Manager - LiveData Utilities, Inc.*

11:30 am

**Leveraging Technology to Redefine Critical Data Acquisition…..42**

Traditional SCADA requires a persistent communication link with every field device, which is both very costly and limits the coverage area of the data network. Traditional remote monitoring is very cost effective for monitoring devices outside of the SCADA network, but lacks the data density and real-time data acquisition necessary for critical data acquisition. A new class of monitoring devices have the capability to take measurements at sub-second data rates, store data locally and forward it to the host upon request, provide immediate notification of non-critical incremental changes in critical systems, and provide real-time alarm notification of critical value changes; in effect, combining the data acquisition model of the SCADA system with the communication model of the remote monitoring system.

This presentation focuses on this new class of monitoring systems combining the data acquisition requirements of traditional SCADA (rapid scan rates, large quantities of data), with the data transmission model of exception based remote monitoring (periodic reporting, low-cost/low bandwidth non-persistent connections). Leveraging the measurement and communication advances incorporated into this new class of monitoring systems allow organizations to extend critical system monitoring far beyond the reach of the traditional SCADA network in a reliable, cost-effective manner

providing real-time visibility to previously unmonitored devices and systems at remote locations.

*Jamey Hilleary, Director of M2M Technology – Elecsys Corp.*

12:00 – Networking Lunch

1:00 pm
**Requirements, Approaches, and Best Practices for Meeting the Challenges of Secure, Interactive Remote Access…..50**
While the NERC CIP standard takes a comprehensive approach to cyber security, there remain areas where the specific implications of security vulnerabilities are not understood by the industry at large. This course looks at the specific area of Interactive Remote Acce ss Management as covered by NERC CIP-□005.

NERC does not currently provide any requirements or guidance documents on how to accomplish a secure, interactive remote access solution. However, NERC does define the key requirements that must be met by an interactive remote access solution in CIP-□005.

Stated requirements of CIP-□005 include:

1. Implementing an Intermediate Device for Interactive Remote Access
2. Encryption for all Interactive Remote Sessions
3. Multi-□factor authentication
4. Logging and monitoring
5. Up-□to-□date anti-□malware software on user devices
6. Up-□to-□date patch levels on user devices

The most important mistake to avoid when implementing an Interactive Remote Access solution is for a Utility organization to take a minimalist approach that is focused on simply meeting the stated requirements of CIP005. While a properly designed strategy ca n
deliver advanced security without negatively affecting performance (probably improve it) a
less considered approach could have significant, negative consequences.

The best practice guidance for implementing an Intermediate Device solution is to look at the problem holistically. Utility organizations should recognize upfront that performance penalties are not a tradeoff they must make, but that due diligence will likely be required on their part to ensure that performance degradation does not become part of the outcome of the Interactive Remote Access Management practice.

*Bill Johnson, Founder and CEO – TDi Technologies*

1:30 pm
**Analysis of the Capabilities of Cybersecurity Defenses…..58**

Over the past several years of the IT/OT convergence challenge, IT security programs were held up as the gold standard for industrial control system/OT cyber-security programs, but that thinking is changing. While the hardware and software on IT and OT networks are becoming very similar, other characteristics of the two networks differ sharply.

The essential difference between control systems and IT systems is, not surprisingly, control. OT networks control the physical world, whereas IT systems manage data.

The cyberthreats to our critical infrastructure continue to evolve to take advantage of IT security weak points. As new cyberattacks are created and discovered, it is incumbent upon us to evaluate the capabilities of our defensive strategies and technologies against these new offensives. This session will investigate and report on how the modern, targeted online and removable media threats to industrial cybersecurity fare against the most popular IT security protections deployed to protect critical infrastructure, including: whitelisting, intrusion detection, next-gen firewalls, and risk management practices. Finally, we will present Operations cybersecurity technologies and strategies that are effective in the protection of our physical processes as a comparison.

*Michael H. Firstenberg, (GICSP, CISSP, GCIH) Director of Industrial Security - Waterfall Security Solutions*

2:00 pm

**IP Video: Innovating on the Edge…..68**

IP video was invented nearly 20 years ago and had limited capabilities. Today, network cameras have evolved into miniature computers with lenses and sensors. This presentation will illustrate how the transition from simple devices to intelligent edge functionality Continues to evolve. Improvements in processing enables surveillance systems to move from reactive to proactive, as network cameras are now able to analyze, manage and act on events in real-time.

The evolution to intelligent in-camera operations translates to significant savings of time and money:

- Lower bandwidth consumption—only pre-processed video is being sent across the network rather than massive amounts of constantly streaming footage that must be analyzed on the server side.
- Lower storage requirements—only content-rich video is being streamed to the video storage array rather than every frame that was captured by the camera.
- Lower operating costs—in-camera processing is less expensive than monopolizing CPU cycles on the server.

From a physical security perspective, relevant advances will include onboard storage capabilities in IP video cameras; the ability to upload resident programs for video analytics; advance event triggers and traps; and optimization agents, such as video over

Wi-Fi, that can identify itself to the network infrastructure and allow for automated quality of service settings for the camera output.

*Anthony Incorvati, Business Development Manager of critical infrastructure and transportation - Axis Communications*

2:30 pm

**A New Layer of Security to Protect Critical Infrastructure from Advanced Cyber Attacks…..88**

Critical infrastructure attacks have risen 43% in the past year. Perimeter defenses have been rendered useless by sophisticated attacks, which is why the majority of these attacks easily make it to the inside of the network. Protection against these advanced threats requires a new layer of security that limits hacker movement once they inevitably breach perimeter defenses.

A recent report revealed that between 80-100 percent of all serious security incidents featured the "signature" of exploited privileged accounts. In this session, CyberArk's Adam Bosnian will review the challenges and proposed solutions for energy utilities in dealing with management of their privileged administrator accounts across their ICS/SCADA and smart-grid networks. Bosnian will also discuss the NERC requirements on the security of remote access and will offer tips on how to go beyond those regulations to further secure access into the ICS/OT network.

*Alex Leemon, Sr. Manager - CyberArk*

3:00 pm – Networking Break in Exhibit Hall

3:30 pm

**Remote Monitoring and Predictive Diagnostics of Remote Power Systems…..98**

Off-grid PV-Battery based power solutions are an increasingly integral part of many industries, such as Telecom, Oil & Gas, Security, Waste Water Management, Transportation, and Environmental Monitoring. Having adequate monitoring and control of these systems can provide not only increased system reliability, but increased cost savings as well.

This presentation will cover the basics and best-practices of monitoring and control of remote PV-Battery based systems. In this presentation you'll learn about wireless transmission options & hardware (cellular, satellite, radio) and accessories (Charge Controllers, MSC, RSC-1, Serial/Ethernet), how to wire & network components (RJ-11, RS-232, EAI-485, Ethernet), differences between local & remote connections, monitoring & control requirements of single device systems vs multi-device systems, examples of most commonly used networking configurations, overview of MODBUS compatibility requirements, examples and overview of Relay Driver use, and a quick demonstration of the MSView software that's used to remotely access the power system from your PC.

*Aerel Rankin – SunWize  Power & Battery*

4:00 pm

**Hybrid Fuel Cell / Solar Systems for Reliable Long Duration Remote Power…..119**

Solar power is being deployed extensively to power remote monitoring and control, telecom relay, and weather monitoring equipment in highly inaccessible areas across the globe. However, as deployment areas move further and further from the equator, the solar arrays needed to support uninterrupted operation become prohibitively large, cumbersome, and expensive.

Protonex, in partnership with Sirius Integrators, has transitioned its hybrid fuel cell / solar technology from its military roots to a lightweight, robust, reliable triple-hybrid (battery, solar, fuel cell) system that for many applications permits drastically easier and less costly installation, increased reliability, and significantly decreased operational costs. This presentation explores the system, as well as the results of the trial deployments already underway in the US and Canada.

*Phil Robinson, VP Defense Power Systems – Protonex*

4:30 pm

**Closed Cycle Vapor Turbogenerators (CCVT) for Reliable Remote Applications…..129**

The objectives for high reliability in telecommunications, cathodic protection and SCADA systems in strategic projects have become very demanding, and the problems faced in areas not serviced by commercial power are very stringent, since power generators must operate continuously on a 24-hour-per-day, 365-day-per-year basis with high reliability, long life (over 20 years) and low maintenance.

Closed Cycle Vapor Turbogenerators (CCVT) powered numerous applications in the oil and gas industry along pipelines and on offshore platforms. They provide DC power for telecommunications networks, telemetry and SCADA systems, pipeline cathodic protection, motorized valve controls, navigational aids and remote emergency lighting. CCVTs power also telecommunication applications, including repeater stations, telecommunications links and fiber optics sites in Antarctica, North America, South America (Andes Mountains and Patagonia), Siberia, Far East of Russia and Kazakhstan. Reliability and availability of power supply in remote stations are paramount factors for pipeline operation and its revenues. Selection of the most reliable power units and adequate redundancy are also extremely important factors. With over 45 years of field experience, CCVT technology is proven to be highly reliable in the most adverse of environments.

*Jean Gropper, Director of Business Development - Ormat*

5:00 pm – Cocktail Reception

**Friday, Nov. 6th 2015**

7:30 am – Registration Opens/Continental Breakfast

8:15 am – Day 2 Keynote

**Surviving the In-House Solution Stack Hack…..138**

Sometimes, you can't find an off-the-shelf solution for a problem. You're stuck. Then, you have a bright idea. With commodity parts, a bit of expertise and determined effort, you cobble something together. You write a new script. You make a custom cable. You think you've saved the day. But soon, your "In-House Solution Stack Hack" backfires.

What goes wrong? Other divisions hear about your solution and want their own. You can't scale the solution stack because you don't have design control. A component gets discontinued. New models replace older ones. Nothing is compatible anymore. Your technician who makes the custom cables quits. No vendor understands your design, so there's no tech support. Your bright idea has become a nightmare. Who cares whether you're the technician that built it or the manager that authorized it? No one's happy.

You have too many sites and discerning customers to tolerate an uncontrolled solution stack hack in your enterprise network. You can mitigate problems by preparing in advance. Secure inventory. Write documentation. Create FAQ lists. Establish a release process. How do you bring these skill sets into your company and manage the roll out of an In-House Solution Stack Hack? I'll teach you.

*Marshall DenHartog, President – DPS Telecom*

9:00 am -

**Case Study: Microgrid Platform Security…..161**

Industrial Control Systems (ICS) are a necessary part of oil and gas environments. Regardless of mid-, up-, or downstream, there is always an ICS controlling, monitoring, and collecting data from various sensors in any given facility. With a limited number of trusted personnel in the ICS environment, it should be extremely easy to secure, right? Well, no.

Enter your business LAN. Connectivity between IT and OT systems is a reality we can't ignore. Many companies have hundreds, and even thousands, of workstations in their organizations. Every workstation is a potential entry point for malware, viruses, or harmful cyber attacks. If the operational technology systems are connected to the IT environment within an organization, thousands of USB ports, CD/DVD drives, mobile phones, and internet connections could provide an attack vector into the ICS.

With the risk of access to corporate information, or even worse control access to a plant, refinery, or pipeline, adequate just isn't enough. You need to take security to the next level.

In this presentation, Tresys will describe a secure, effective architecture for sharing information from the OT environment to the IT environment.

*Charles Zaloom, Director, VP of Critical Infrastructure - Tresys Technology*

9:45 am – Networking Break in Exhibit Hall

10:30 am
**Smart Grid Automation in a Cyber-Physical Context…..172**
Smart Grid Automation in a cyber-physical context is introducing very complex interdependencies between Information Technology Computer Systems and Networks (IT) on one side and distributed Industrial Control Systems (OT) on the other side while making the energy delivery systems vulnerable and susceptible to cyber-attacks in the process of modernization.

Cyber security solutions for the utility segment show similar requirements compared to Trusted Networking solutions for Security and Defense forces. A "Trusted Network Platform (TNP)" was developed in partnership with Southern California Edison, who recognized the parallel and wanted to draw on the vast experience in this field to apply it to Grid Automation security.

The presentation provides detailed information on the principles applied to provide secure networking for utilities tying communications and networking solutions together. Broadband applications for physical security and remote video surveillance such as substations can be established very affordably using today's High Capacity Satellite service offerings and are combinable with the best practices in military grade networking.

*Stefan Jucken, Strategic Business Development – ViaSat*

11:00 am
**Proximity Based Contextual Mobility for SCADA…..180**
Proximity based services enabled by micro-geolocation with indoor positioning technology, is a significant improvement and enables new capabilities for remote access to SCADA systems by mobile workers. The indoor location technology market alone is estimated to reach $5 billion in revenues by 2017 and will represent over 200,000 installations of infrastructure equipment, including Wi-Fi hotspots, Bluetooth antennas, and more than 800 million branded applications downloads.

Remote access to SCADA systems has long been accomplished using internet browsers on laptops. The rise of mobile devices such as tablets and smartphones, it is more and more common to use technology such as Microsoft Remote Desktop Services (RDS) for this purpose. Navigating a SCADA interface using a mobile device with RDS can be difficult given the small screen size and mechanism for managing the mouse.

Micro-geolocation integrated with SCADA enables the presentation of SCADA mimics and alarms in the context of the mobile workers location without the need to manually navigate to the equipment view; presenting a dynamic view appropriate to the role and location of the mobile device user. It is invaluable when it is important to know what level a facility the mobile user is located. For example, in a plant even if GPS can

provide the geographical location, micro-geolocation provides the floor the worker is on and enables the SCADA view to be presented in that context. It is a much more pro-active approach that improves the efficiency of mobile workers during commissioning, operation and maintenance of the system.

*Edward Nugent, COO – PcVue Inc.*

11:30 am

**Data Driven Approach for Early Prediction in Real-Time Oil & Gas Production…..194**

Oil and gas production process is highly complex and capital intensive process. Often times, there are several production issues that reduce barrel production. Traditional methods applied to tackle the production issues are reactive in nature, resulting in monetary and time loss.

The business requirement from field personnel is to be equipped with a methodology and tool for predicting the production issues in near real-time. At Cyient-Insights, we believe that effectively leveraging data and advanced analytics answers many, if not all, challenges business face today. Our expertise lie in understanding complex M2M data, and applying advanced analytics approaches to generate actionable insights.

In this paper, we consider SCADA data, and mud logs from an oil production major based in US for a period of two years. We demonstrate a data-driven prediction approach that aids in early prediction of well loading and choke issues encountered in production. Our approach is a hybrid of principal component analysis and machine learning. In particular, we could predict a well loading issue 60 days in advance, while choking issues are detected 30 days in advance. The results are encouraging and being evaluated on the field by an Oil major.

*Sean Otto, Data Scientist – Cyient Insights*

12:00 pm – Networking Lunch

1:00 pm

**Future Proofing your M2M Technology…..203**

M2M is growing and changing constantly. How does one overcome the many challenging aspects of choosing the correct M2M device to meet not only current needs but future needs as well? Customers must consider market demands, business impacts, carrier networks and device management before their purchase.

M2M is increasingly becoming a necessity and it is essential that these products withstand the evolving environment of machine-to-machine technology. NetComm Wireless has considered all of these impacts in order to make the decision process easier for the customer. Future proofing your device is essential to the success of your business and the presenter will walk you through choosing the best solution for your current and future needs with all requirements in mind.

*Terra Bastolich, M2M/IOT technology Advocate - Netcomm Wireless*

1:30 pm

**Effects of Lower Crude Oil Prices on the Automation Sector…..214**

This presentation will address the return on investment scenarios and analysis of benefits for implementation of new and improved technologies such as upgrading to wireless monitoring, control and automation, adoption of new internal operational strategies and integration of existing and new solutions based on the effects of lower crude oil prices on the automation and communications sector for Upstream Production and Downstream Refining and Petrochemical Industries.

The impact of lower crude pricing presents owner/operators with opportunities and challenges on both sides of the industry; upstream (onshore) and downstream. On the upstream side the threat to the business is that the rig count will go down drastically and the new well count will be substantially reduced. This will have a negative on all the panel shops and system integrators that support this industry with well pad control and automation systems. On the downstream side low feedstock pricing is creating a profitable refinery and petrochemical industry sector which will spawn new projects, expansions and modernizations; including DCS revamps which are long overdue.

*Fred Czubba, Senior Business Development  Oil & Gas - Phoenix Contact*

2:00 pm – Conference Conclusion