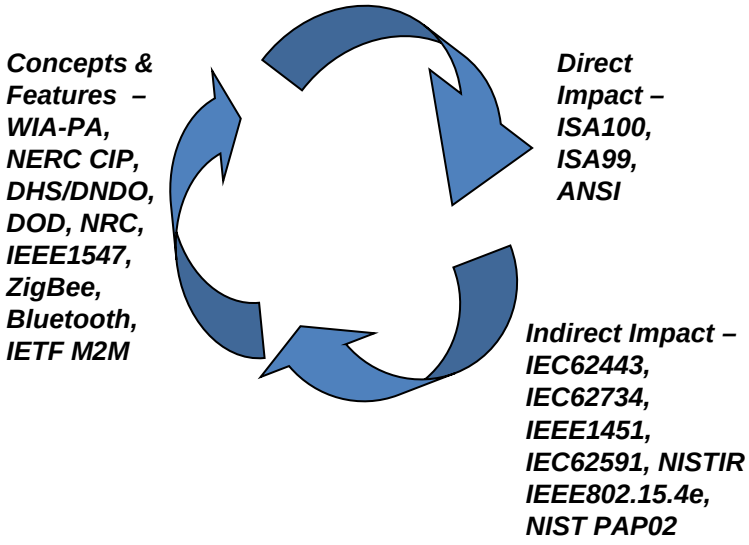
Wayne W. Manges
Oak Ridge
National Laboratory

Core and Frontier Capabilities - Summary

Cybersecurity for Energy Delivery Systems Peer Review
July 24-26, 2012

Summary: Trustworthy Wireless & ASAP-SG, Beholder (Detailed Example)

- **Objective**
  - Actionable, specific cybersecurity guidance for EDS (e.g. Substation Automation, cyber event detection)
  - Development of standards (ISA100, ISA99, TWWG) and guidelines (TWWG, ASAP-SG Profiles)
  - Influence development of related standards (IEC, IEEE, ISA, NIST)
- **Technical Approach**
  - Develop consensus through publications, presentations, F2F meetings, and conference calls
  - Produce documents and standards targeting acceptance by IEEE, IEC, NIST
  - Continue to increase EDS industry involvement



- **Schedule**
  - Reports on schedule
- **Performers:** ORNL
- **Partners:** ANL, ISA standards committee participants, Southern Co., SCE, NIST, EPRI, GE

Stacy Prowell

Oak Ridge
National Laboratory

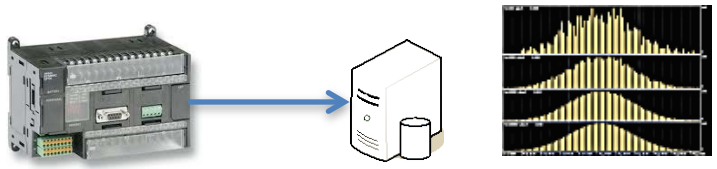
Beholder

Cybersecurity for Energy Delivery Systems Peer Review

July 24-26, 2012

Summary: Beholder

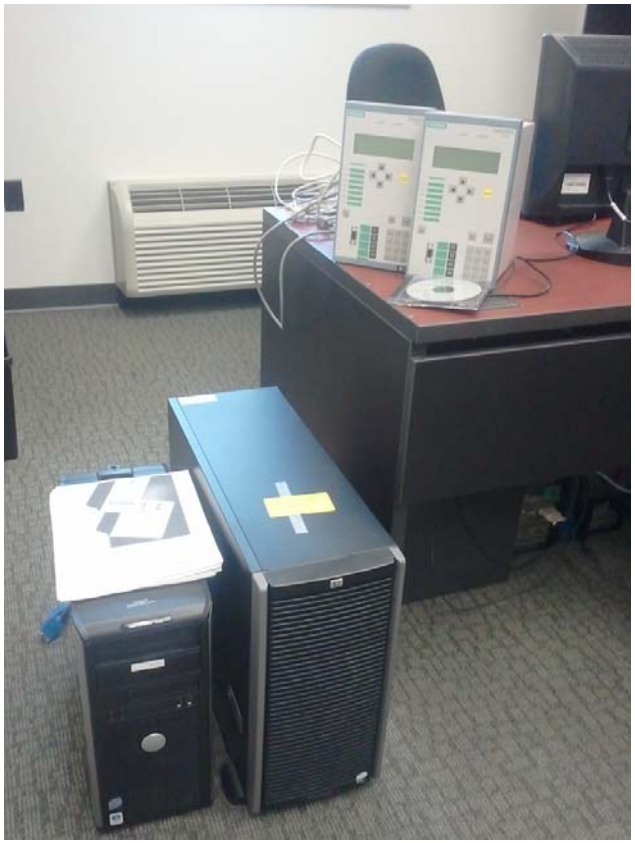
- **Objective**
  - Robust, remote (and real-time) cyber event detection
- **Technical Approach**
  - Monitor precise timing information for critical routines on a device and establish a device-specific baseline
  - Remotely detect deviations from the baseline due to device failure, intrusion, or tampering
  - Measure and detect the “extra work” required by malware or intrusion
  - Do not rely on a static database; establish each device’s unique fingerprint



- **Schedule**
  - Deliverables on schedule for 9/2012
- **Performers:** ORNL
- **Partners:** GE Digital Energy, GE Research

Technical Approach and Feasibility

- **Approach**
  - State of the Art: Static signatures Beholder uses dynamically-determined signatures that can be *device specific* and not known *a prior*.
  - Q1 Hardware survey and acquisition
  - Q2 Experimental design and execution
  - Q3 Initial feasibility demonstration
  - Improved cyber event detection using information not easily available to an adversary.



Technical Approach and Feasibility (Cont'd)

- **Challenges to Success**
  - Demonstrate feasibility of detection
    - Work with GE to use their labs to show detection **at scale**
    - Establish speed of detection and **false positive** and **negative** rates
  - Demonstrate no disruption of existing systems
    - Conduct repeatable tests to show the solution does not adversely impact the **availability** or **capacity** of targeted devices, relying on testing *in situ* by GE under typical work loads
  - Demonstrate applicability to legacy devices
    - GE interested in application to D20

Progress to Date

- **Major Accomplishments**
  - Acquired and configured hardware (RTU, relays, PLC, D400 VM)
  - Design of initial experiments in collaboration with GE
  - Major effort underway over summer (from one student running experiments to several students and staff)
- **Actual Progress**
  - Hardware acquisition, initial performance testing.
  - Several personnel have not been available until the summer due to other projects.

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Beholder can be (1) “baked in” to new devices, and (2) retrofitted to many older devices.
  - We have been working closely with GE digital energy with their D400 device as our initial target, and have approached EnerNex, a local company with a substation configuration using the D400
  - Planned integration with ORNL’s AMI testbed
  - We hope to gain industry acceptance by (1) demonstrating the technology at scale and in realistic settings and (2) gaining support from suppliers to license the technology and build it into their solutions
  - This solution *complements* existing approaches and can be deployed alongside them

Next Steps

- **Approach for the next year or end of project**
  - Development and single deployment in Year Two
  - Primary risk is **technical**: Must show that solution does not adversely impact availability and / or performance of existing devices
  - We have been very successful (so far) in gaining acceptance with suppliers, but feel solid demonstration is needed before we approach a utility
  - At scale demonstration in collaboration with a utility in Year Three
- **Future work**
  - The basic approach (measure additional work) can be applied to non-intrusive load monitoring of DC power
  - EnerNex is interested in collaboration on this work
  - Timeline: One Year (Separate Effort)

Wayne W. Manges

Oak Ridge
National Laboratory

Trustworthy Wireless for Critical Infrastructure

Cybersecurity for Energy Delivery Systems Peer Review

July 24-26, 2012

Summary: Trustworthy Wireless for Critical Infrastructure

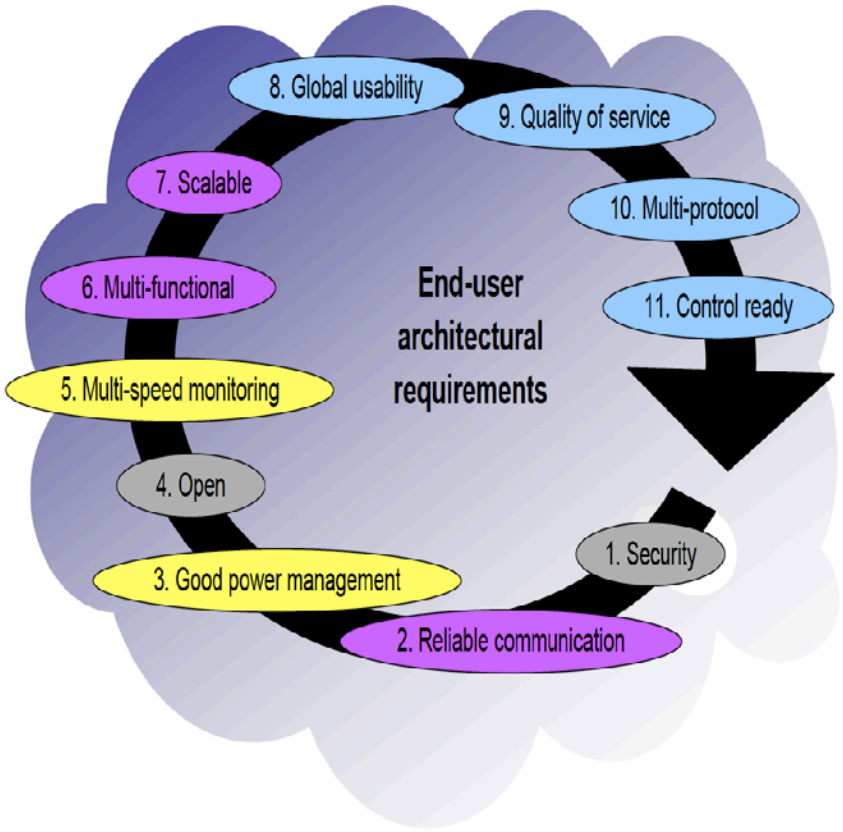
- **Objective**
  - Technical reports to provide basis for standards and testing around issues associated with Trustworthy Wireless (Security, Reliability, Resiliency)
  - Development of standards and guidelines
  - Influence development of related standards (IEC, IEEE, other ISA)
- **Technical Approach**
  - Develop consensus through publications, presentations, F2F meetings, and conference calls
  - Produce documents and standards targeting acceptance by IEEE, IEC, NIST
  - Continue to increase EDS industry involvement

http://trustworthywireless.ornl.gov/

- **Schedule**
  - Reports on schedule for 9/2012
- **Performers:** ORNL
- **Partners:** ANL, ISA participants, Southern Co., SCE, NIST

Technical Approach and Feasibility

- **Approach**
  - Collaborate with end users to document requirements and deficiencies in currently available wireless components using RFIs, meetings and calls to identify issues that need to be addressed
  - Document technical basis (input from end users, manufacturers, vendors, designers, implementers, operators) for development of standards and guidelines
  - Facilitate development of technical contributions from EDS end users, manufacturers, vendors, implementers, maintainers and operators
  - Publish co-authored reports, standards, and technical publications relevant to end user community and other standards bodies – IEC, IEEE, NIST

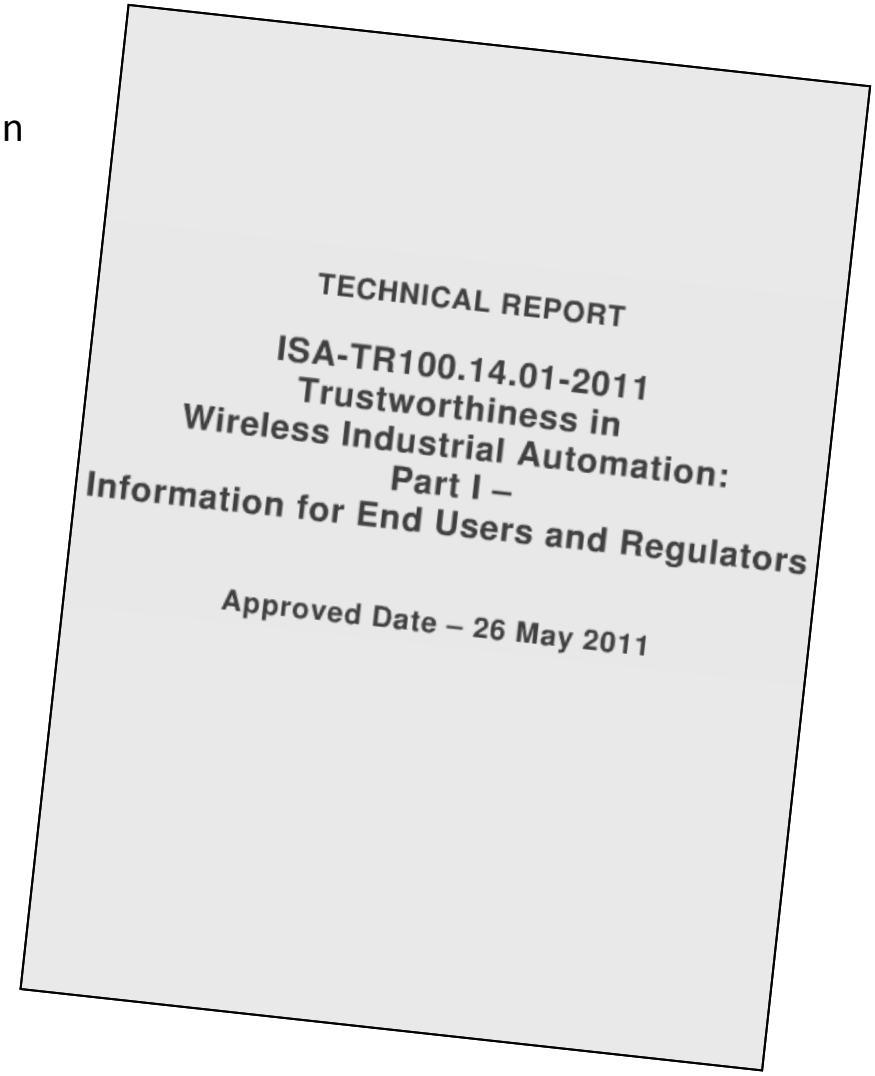


Technical Approach and Feasibility (Cont'd)

- **Challenges to Success**
  - Perception that ISA is closely aligned with the process control industry, not EDS
    - Increase collaboration with NIST, IEEE, IEC
  - EDS user and vendor acceptance slow
    - Use technical reports and published standards to help to develop protocols for compliance testing
  - EDS culture sometimes values compliance over performance
    - Continue work with NERC to develop appropriate guidance and solutions
  - Rapid pace of change with wireless technology and social acceptance
    - Maintain focus on fundamentals of the physics of radio
    - Continue to emphasize logical consequences of vulnerabilities
    - Maintain ISO open architecture model in standards development
  - Diverse Application Domains – M2M, I2G, Situation Awareness, SCADA, Asset Management, Closed-loop Control, Distributed Sensor Fusion, Energy Management
    - Continue outreach – invited training, papers, talks
    - Conference participation – diverse user applications and domains

Progress to Date

- **Major Accomplishments**
  - ISA-TR100.14.01-Part 1-2011. Trustworthiness in Wireless Industrial Automation: Part 1, Information for End Users and Regulators – on schedule and budget
  - ISA-dTR100.14.02-2011. Trustworthiness in Wireless Industrial Automation: Part 2 - Understanding the Issues Associated with Implementing a Trustworthy System (Draft ballot results: approve – 27, disapprove – 4, abstained – 1) – scheduled for public release in September 2012
  - IEEE 802.15.4e released in 2012 – based on ISA100.11a technology (MAC and PHY)
  - IEC 62734 based on ISA100.11a accepted in 2012 as "publicly available specification" for ballot
  - IEC 62443 released in 2012 based on ISA99



Collaboration/Technology Transfer

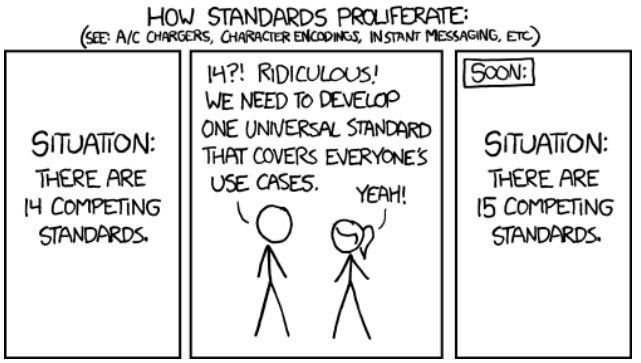
- **Plans to transfer technology/knowledge to end user**
  - Wireless Compliance Institute awaits publication of Part 2 report for use in preparing test plans and more definitive compliance criteria.
  - Extend efforts for a greater NIST PAP02 engagement (meetings, identify industry partners, document preparation).
  - Continue collaboration with Scott Mix at NERC - Trustworthy wireless is an area of increasing importance for CIP, especially for the aspects of security and resiliency.

Culture Issues – HELP!!

- **Legacy Culture – reminiscent of my home town – Pittsburgh!**
  - "We'll just work with our vendors and they will build what we need."
  - "I'll just wait for a clear choice to emerge."
  - "I'll vote with my wallet."
  - "Standards just document industry best practice."
  - "Everything we deploy must have 30 year life."
- **New Culture Emerging in Other Markets?**
  - "Reliability isn't as important as we thought it was." - GM
  - "The consumer will never accept the poor reliability offered by this technology." – GE
  - "If you're not ready to replace your entire mill in seven years, your competitors will put you out of business" – Danielli-Wean
  - "The only answer to cyber security is to make the asset owner fiscally libel for all intrusions" – S4 Conference

Next Steps

- **Approach for the next year**
  - Extend ISA100.14 Scope (needed to develop criteria/requirements)
    - Develop criteria for trustworthiness levels – requires extensive end-user interaction
    - Identify trustworthiness levels for required and achieved categories
    - Consequence analysis using zones and conduits
    - Appropriate metrics for trustworthiness levels required and achieved
  - Extend NIST PAP02 Engagement
    - Include reports, meetings, industry partners
  - Continue outreach to help overcome reluctance of manufacturers and vendors
    - More attention needs to be given to provisioning and configuration control practices
    - Protection of critical functions and operations against very sophisticated and determined attacks from worms like Stuxnet and Flame.
- **Describe potential follow-on work, if any**
  - FY2013 – Trustworthiness levels defined

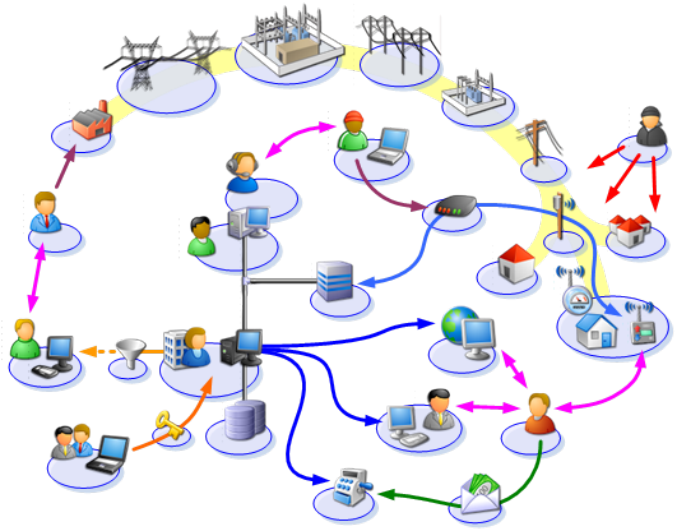


James Nutaro
Oak Ridge
National Laboratory

Advanced Security Acceleration Project for the Smart Grid (ASAP SG)

Summary: ASAP SG

- **Objective**
  - Provide actionable recommendations for securing cyber-assets used in specific smart grid applications.
- **Technical Approach**
  - Collaborate with utilities and information technology companies through the Open Smart Grid Subcommittee of the UCA International Users Group (OpenSG) to ensure the relevance of our products.
  - Use a team of industry and government experts to create and document recommended security practices targeted to ensure secure smart grid application deployment.



- **Schedule**
  - Complete security recommendations for substation automation in September 2012 – in progress
- **Performers:** Enernex, SEI, UtiliSec, ORNL
- **Partners:** Southern California Edison

Technical Approach and Feasibility

- **Approach**
  - Currently asset owners depend on their own resources to gather information to address the cyber security issues associated with the various roles that must be addressed in EDS implementations
  - Lack of standardization increases costs and decreases effectiveness of these alternatives
  - Critical steps include completion of the security profile for substation automation by the end of FY12
  - Publication of the profiles provides NIST, vendors, asset owners, and others implementation guidance for EDS

Technical Approach and Feasibility

- **Challenges to Success**
  - Maintaining relevance to industry
    - Stakeholder interviews
    - Review and approval of security profiles by OpenSG
  - Actionable cybersecurity guidance
    - Develop logical architecture for each profile
    - Usability analysis
    - Review from industry experts
  - Repeatability of process
    - Document process – security profile blueprint

Progress to Date

- **Major Accomplishments**
  - Industry adoption of security recommendations for AMI, 3rd party data access, distribution automation, and wide area protection and control

- **Actual Progress (technical, $, and Time) vs Planned Progress**
  - Completed security profiles on time and on budget
    - Advanced Metering Infrastructure
    - Third Party Data Access
    - Distribution Management
    - Wide Area Monitoring Protection and Control

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - NIST and other standards bodies will continue to use the ASAP-SG profiles for updating guidance documents
  - Journal/conference publications and presentations used to socialize concepts and proposed implementations
  - End user participation throughout the process incorporates issues associated with legacy systems

Next Steps

- **Approach for end of project**
  - Complete the security profile for substation automation
- **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  - Adoption of the security profiles by industry may create a need for new technologies to satisfy cost-effective recommendations given in the profiles
- **Describe potential follow-on work, if any**
  - Continue with next highest priority profile (1 year)

ORNL Proposed Strategy Integrates Activities Focused on User Needs

Major Focus Areas:

- User requirements specification and understanding
- Security guidance for users, regulators, and standards bodies
- Criteria for technology assessment and decision making — offline and real-time

Expertise

- Cybersecurity & Computer Science
- Power Systems
- Protection Engineering
- Control Systems
- Systems Engineering
- Reliability Engineering
- Modeling & Simulation