Mobile Devices for SCADA Integration and Beyond: Considerations, Security and Applications

Speakers:
Pavol Segedy and Brandon Erndt

2012 ISA Automation Week
September 24-27, 2012 – Orlando, Florida, USA
Presenter

• Pavol Segedy
  – Over 8 years of experience in the design and implementation of electrical and control systems for water, wastewater and pump station facilities.
  – Expert in design, specification and startup of plant instrumentation
  – Provides support and troubleshooting services to resolve issues in established plants and/or systems.
  – Programming Leader for Mid-Atlantic region.

• Brandon Erndt, PE
  – 17 years of experience as a controls engineer, project manager, and programming department manager
  – Programmable logic controller (PLC) programmer and Human-Machine Interfaces (HMI) software developer.
  – Responsible for developing several vendor software programs.
Presentation Outline

• Overview of SCADA (Industrial Control Networks)
  – New Role of SCADA in Water/Wastewater Industry – Data Hub

• Introduction to communications options
  – Technologies
  – Configurations
  – Security

• Introduction to Mobile Solutions – different applications for different client needs

• Live Demos
  – Remote Desktop – Visualizing the SCADA system
  – Real Time access to Control System
  – Mobile Reporting
Background – Industrial Control Systems

- Proprietary networks
- Hard to interface between networks
- Closed communication networks
- Challenging to integrate with other systems
Current Configuration – ICS

• Last 10 years – migration to open communications (i.e. Ethernet)

• Physical connection to Control Systems for Ethernet is the same as your PC even if the protocol is slightly different (Ethernet IP, Modbus TCP/IP, etc)
SCADA Role as Data Hub

- Collaborative environment between control systems and IT
- “Getting on the same page”

SCADA System

Financial  CMMS

GIS  Energy Management

LIMS  Equipment Monitoring & Control

Process Monitoring
communication_solution = How far do you want to go?

- What is happening?
- How many, how often?
- How can I change system operation?
- How efficient, how effective?
- How does performance vary?
- What’s the best that can happen?

degree_of_SCADA_communications

degree_of_utility_optimization

system_monitoring

system_reporting

system_control

system_performance_analysis

system_trend_analysis

system_predictive_modeling

improved_operation_performance

2012 Isa Automation Week
Sept 24-27, 2012 – Orlando, Florida, USA
Security Considerations
Traditional Responses - ICS

Traditional responses to SCADA security
(and why they no longer work in the age of Mobility)
Security Considerations

• Most Common – VPN (Virtual Private Network)
  – Work with your IT staff but understand the difference between City WAN and Industrial Control Network

• Local Wi-Fi
  – Dedicated Security for the Local Wi-Fi network
    – Change Defaults – includes changing SSID and passwords
    – Disable SSID (Service Set Identifier) Broadcast
      – Does not offer protection against determined intruders
    – MAC Access Control – MAC filtering
    – Activate Encryption - built in Wireless encryption
      – WEP (Wired Equivalent Privacy) 64- or 128-bit encryption
      – WPA-PSK [TKIP] (Wi-Fi Protected Access with Pre-Shared Key with TKIP (Temporal Key Integrity Protocol) encryption type (IEEE 802.11i)
      – WPA-PSK [AES] (Wi-Fi Protected Access with Pre-Shared Key version 2 with AES (Advanced Encryption Standard) encryption type
      – WPA-PSK [TKIP] + WPA-PSK[AES] allow both encryption types
Expanding the SCADA wirelessly

- Communications Options
  - Cellular (3G, 4G)
  - Local Wi-Fi
Example of SCADA Architecture
Mobility Options – Consider Your User

- Operator
- I&C Technician/Programmer
- Supervisor/Manager
Live Demo and Questions

Pavol Segedy 919-233-9178  psegedy@brwncaI.com