Mobile Devices for SCADA integration and beyond: Considerations, Security and Applications

Pavol Segedy[1]* and Brandon Erndt[1]

[1]Brown and Caldwell, 5430 Wade Park Boulevard, Suite 200, Raleigh, North Carolina, USA, 27607
(*correspondence: psegedy@brwncald.com)

FORMAT: 30 minute PowerPoint presentation

KEYWORDS

SCADA, Mobile Device, Ethernet, Remote Connectivity, Wi-Fi, 802.11, Wireless, Integration

ABSTRACT

The use of mobile technology offers plant managers; instrumentation techs and operators secure access to critical process data from anywhere using smart phones or tablets. Mobile devices provide convenience and simplicity by bringing meaningful real-time data that can help both operators and executives make decisions and improve system operation.

Supervisory Control and Data Acquisition (SCADA) systems collect data from treatment plants and remote facilities. Historically, SCADA was designed to be connected in a private, hardwired network utilizing line communication. With the arrival of Internet Protocol (IP) in the industrial space, Ethernet and Wi-Fi use in SCADA communications has rapidly increased. This type of communication provides more access to real-time data, alarming, reporting, and trending from remote equipment. SCADA is conventionally setup in a private network not connected to the internet to isolating confidential information as well as the control to the system itself. As the scope of SCADA platforms become larger and mobile applications move from the consumer to industrial markets, mobile devices for SCADA integrations are becoming practical.

This presentation focuses on the primary considerations for implementing wireless solutions, security methodologies and provides a demonstration of some of the more popular SCADA applications currently being used in industry.

Topics include:

- Value proposition and information technology requirements for mobile applications
- Wireless infrastructure options
- Implementation options with real world successes and failures examples including security of Wi-Fi and 3G/4G required to support mobile applications. Wi-Fi technology is built on IEEE 802.11 radio standards, the WPA and WPA2 security standards and the EAP authentication standard. As of 2009, Wi-Fi technology has spread widely within business and industrial sites
- Applications deployed for SCADA such as iView, Ignition SCADA mobile module, mySCADA, ScadaMobile, C-more, PLCLink and more

Mobile devices have matured, making them suitable for many industrial applications. They provide many benefits for operations, such as replacing numerous costly industrial operator interface terminals (OITs)

with a few mobile devices and capturing information from multiple systems; such as SCADA, online electronic O&M manuals, CAD drawings and Key Performance Indicators, all in one location that can go wherever plant staff needs to be. Finally, safely connecting these devices to an already secure network is a critical, yet achievable, task that must be investigated whenever considering wireless access to industrial control systems.

About the Authors:

Pavol Segedy is a Senior Automation Engineer at Brown and Caldwell. Typical projects include design, specification, SCADA development, on-site startup, construction support and inspections. He also provides project management, consulting services, support for completed projects as well as troubleshooting services to resolve issues in established plants. He is a member of ISA, AWWA and IEEE, and serves as a membership chair at ISA Tarheel Capital Section and Section-Division liaison at ISA Water Wastewater Industry Division.

Brandon. Erndt is an Electrical I&C department manager, controls engineer, project manager with 16 years of experience. He is also a PLC programmer and SCADA/Human-Manchine Interface software developer. Mr. Erndt is registered Professional Engineer in control systems engineering in the State of Arizona. He is also trained in cyber security for industrial control systems by the Department of Homeland Security.