Pacific Northwest NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

Wireless Communications for the Electric Power System

The Wireless Communications for the Electric Power System project developed a white paper that includes a survey and concise summary of the technical underpinnings of the following wireless technologies:

- IEEE 802.16 d and e (WiMAX)
- IEEE 802.11 (Wi-Fi) family of a, b, g, n, and s
- Wireless sensor protocols that use parts of the IEEE 802.15.4 specification: WirelessHART, International Society of Automation (ISA) 100.11a, and Zigbee
- The 2, 3, and 4 generation (G) cellular technologies of GPRS/EDGE/1xRTT, HSPA/EVDO, and Long-Term Evolution (LTE)/HSPA+UMTS.

The text shown here is the executive summary of a larger white paper. The full paper can be found at ***http://pnl.gov/nationalsecurity/technical/secure_cyber_systems/critical_infra_assess_pro.stm.***

A key mission of the U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) is to enhance the security and reliability of the nation's energy infrastructure. Improving the security of control systems, which enable the automated control of our energy production and distribution, is critical for protecting the energy infrastructure and the integral function that it serves in our lives. The DOE-OE Control Systems Security Program provides research and development to help the energy industry actively pursue advanced security solutions for control systems.

The focus of this report is analyzing how, where, and what type of wireless communications are suitable for deployment in the electric power system and to inform implementers of their options in wireless technologies. The discussions in this report are applicable to enhancing both the communications infrastructure of the current electric power system and new smart system deployments.

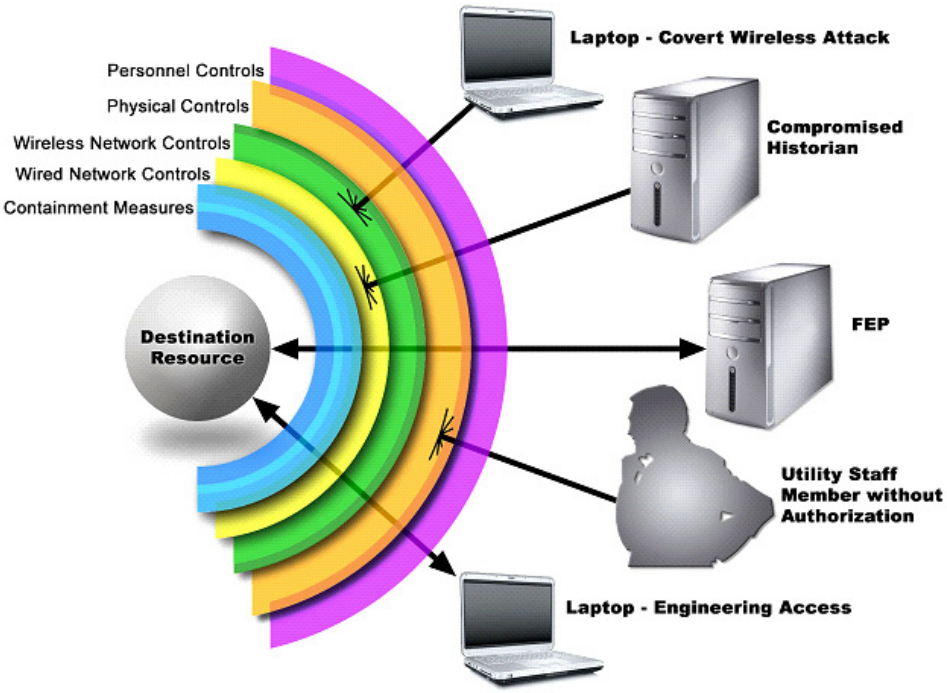
In this document, we provide a concise summary of the technical underpinnings of each wireless technology. We also outline the feature set and the strengths and weaknesses of each technology. Our intent is to provide enough detail to our readers such that when considering wireless for a particular application, they will know enough to ask the right questions to get the features and capabilities desired.

For obtaining data communications coverage quickly and inexpensively over a large geographic area, both WiMAX and 3G/4G cellular technologies should be considered. WiMAX at the present holds a bandwidth and latency advantage

U.S. DEPARTMENT OF ENERGY

over 3G cellular communications; however, with the imminent LTE deployment from multiple carriers, we believe this advantage will be short-lived. Unlike WiMAX deployments, LTE will mostly reuse existing cellular networks and should be a straightforward evolution of the 3G cellular networks. Both of these technologies operate over licensed spectrum and therefore should be protected against unintended interference. In terms of scalability, we know that the cellular networks are capable of accommodating hundreds of millions of subscribers while providing both voice and data communications. WiMAX networks have been deployed to provide wireless local loop service successfully. However, presently, WiMAX networks only support a small fraction of users compared to 3G cellular networks. Whether using WiMAX or 3G/4G cellular, we recommend a combination of application-level security and virtual private networking (VPN) for transporting electric power system information over these public networks.

For creating a wireless sensor network for both data gathering and command/control applications, there are three alternatives, all based on the IEEE 802.15.4 protocol stack: ZigBee, WirelessHART, and ISA100.11a. We expect ZigBee to be a common choice for electric power system networking within the home.



While there are legitimate concerns for the security properties of ZigBee as we will discuss in this report, these concerns can be addressed and should be acceptable for use in the home environment. For transporting data from a customer premise back to an operations center, we expect 3G/4G cellular and WiMAX to be the dominant choices. For wireless sensor network applications elsewhere in the electric power system, such as a substation or a generation plant, we recommend WirelessHART or ISA100.11a. These two standards are very similar in functionality, and either standard is suitable for deployment. Wi-Fi, while being used in many municipal deployments to provide data communications service, is in our opinion not suitable for deployment in the electric power system other than inside a residence as a replacement for ZigBee. Wi-Fi does not provide the reliable wide-area coverage and predictable latencies that are expected for an electric power system application. While offering improved security with the 802.11-2007 specification, the operation in the unlicensed bands would be unacceptable for transporting electric power system data over a wide area.

For more information, contact:

Sam Clements

Pacific Northwest National Laboratory

Samuel.Clements@pnl.gov

NSTB
National SCADA Test Bed

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*