***Automation World* Features New White Paper on Wireless Security, Interviews Authors**

April 16, 2009

The April 2009 issue of *Automation World* magazine features the white paper *Wireless Systems Considerations When Implementing NERC Critical Infrastructure Protection Standards*. The paper addresses wireless protection issues arising from requirements of the Critical Infrastructure Protection (CIP) Standards for the electricity sector, developed by the North American Electric Reliability Corporation (NERC). The CIP standards require entities to monitor and control all electronic access to a company's electronic security perimeter, but this requirement becomes difficult to implement when it comes to wireless technologies. Cell phones, laptops, and any other wireless-enabled device can pose a security threat from either covert or unintentional access to the electronic security perimeter, the paper says.

The *Automation World* article includes an interview with three of the paper's seven authors: Tom Flowers (a member of the Energy Sector Control Systems Working Group), and Wayne Manges and Teja Kuruganti of Oak Ridge National Laboratory. The magazine is also offering a podcast of the interview on its website.

"The use of wireless in a secured, controlled arena is not like wired electronic access. It's still electronic access, but it's not the same, and you don't have the same tools and abilities," Flowers said in the *Automation World* interview. Lacking widely available and affordable security tools for emerging wireless technologies, the energy industry should implement a defense-in-depth approach to using wireless, the paper recommends.

The paper outlines such an "onion skin" approach, Manges said, which involves multiple layers of defense, including personnel controls, physical controls, wireless network controls, wired network controls, and containment measures. "Your level of protection goes up exponentially with the number of layers you have, versus just improving a single layer," Manges said in the interview.

To learn more:

- View the white paper
- Read the interview
- Listen to the podcast