SAND03-1649C

COMMUNICATION VULNERABILITIES AND MITIGATIONS IN WIND POWER SCADA SYSTEMS

American Wind Energy Association WINDPOWER 2003 Conference
Austin, Texas
SESSION 3B – TECHNOLOGY PERFORMANCE PART 1
MAY 19, 2003, 2-3:20 PM

William F. Young, Jason E. Stamp and John D. Dillinger
Networked Systems Survivability and Assurance Department
Sandia National Laboratories
P.O. Box 5800, MS 0785
Albuquerque, New Mexico 87185-0785

Mark A. Rumsey
Wind Energy Technology Department
Sandia National Laboratories
P.O. Box 5800, MS 0708
Albuquerque, New Mexico 87185-0708
http://www.sandia.gov/
http://www.sandia.gov/iorta/
http://www.sandia.gov/wind/

Abstract

This paper focuses on securing wind power Supervisory Control And Data Acquisition (SCADA) systems that utilize commercial-off-the-shelf Information Technology (IT). The use of IT within SCADA systems provides the benefits of low implementation cost and ease of interoperability, but introduces the potential for new security vulnerabilities. To address these new vulnerabilities in wind power SCADA systems, we apply lessons learned from our SCADA assessment activities, design and implementation experience in secure communication systems, and knowledge of wind power operations. We present a SCADA security policy framework and provide two IT "best practices" examples. We also list several typical SCADA/IT vulnerabilities. To provide further reading into the many facets of securing SCADA/IT, an extensive list of references has been provided.