SAND2012-5759P

Sandia National Laboratories

Energy, Climate & Infrastructure Security

# Cyber-Based Vulnerability Assessments

The nuclear power industry in the United States is reliant on digital Instrument and Control (I&C). I&C systems monitor the safe, reliable and secure generation and delivery of electricity but many plant owners are unaware of their potential cyber vulnerabilities.

## Nuclear Cyber Vulnerability

Sandia National Laboratories has conducted cyber-based vulnerability assessment on multiple commercial digital I&C platforms being deployed in the nuclear industry for the purpose of identifying vulnerabilities and improving the design and implementation of these systems. The assessment methodology has been developed at Sandia and is used to determine the risk associated with the design, configuration and operation of cyber-based products.

## Threat Characterization

While modern information technology provides valuable capabilities in today's control systems, its widespread availability and commonality has also made the modern control system inherently vulnerable to many more threats, especially in the cyber domain.

Since there are a large variety of threats, it is important to quantify these threats in a way that allows an analyst to anticipate their impact. By identifying important characteristics of the threats it can be possible to determine the capabilities of adversaries. This allows for the simplification of the continuous threat space to be captured in a more discrete way thus allowing for a more objective analysis. Sandia has identified methods that can be used by threat analysts to identify and quantify threats against cyber-based systems of interest. More information on the Information Design and Red Team (IDART) methodology can be found on the IDART website at idart.sandia.gov along with some accompanying publications listed below.

## Cyber Vulnerability Publications

Duggan, D. P., & Michalski, J. T. (2007). Threat Analysis Framework. Sandia National Laboratories. SAND2007-5792.

Duggan, D. P., Thomas, S. R., Veitch, C. K. K., & Woodard, L. (2007). Categorizing Threat: Building and Using a Generic Threat Matrix. Sandia National Laboratories. SAND2007-5791.

## Risk Informed Product Acquisition

Additional risk imposed on any critical infrastructure industry, such as electrical power production, is the risk to the subversion of products and servers associated with the global commercial supply chain. Industry is dependent on an uncompromising supply chain in the manufactory, purchasing, and delivery of its critical components. Sandia is developing a supply chain risk management methodology that can be used to help the purchasing agent quantify product subversion risk associated with the acquisition of products and services associated with any industry.

For more information please contact:

John Michalski
E-mail: jtmicha@sandia.gov
Phone: (505) 844-3122
idart.sandia.gov

Jennifer Depoy
E-mail: jdepoy@sandia.gov
Phone: (505) 844-0891
idart.sandia.gov

U.S. DEPARTMENT OF ENERGY

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND 2012-####P