

# DNP Security Development, Evaluation and Testing Project Opportunity



With the NERC Critical Infrastructure Protection (CIP) standards in place in North America, utilities can no longer rely on “security through obscurity” to protect their automation systems from electronic attack. The use of wide-area and local-area networks and integration with corporate networks has created a need to provide cyber security solutions for all parts of the utility automation network.

Over 75% of electric utilities in North America use the Distributed Network Protocol (DNP3) to control their power systems. EPRI is helping the DNP Users Group to develop a standard that could provide security for all these networks.

The DNP specification has been nearly completed by the DNP Users Group, primarily a volunteer organization with limited resources. EPRI’s and a participant’s involvement will work to complete important parts of the specification in a timely manner. A utility’s interests will also be served through the proper evaluation and testing of the specification before deployment.

## This project will:

- Accelerate the development of an open standard for cryptographically securing the utility data communications protocol in North America.
- Have recognized security experts evaluate the new standard before deployment.
- Support the widespread adoption of the standard among utilities.
- Lay groundwork for interoperability and conformance testing in 2009.

## Value

**EPRI research will help provide the DNP protocol standards to the industry.** The specification will also be valuable to utilities for a number of reasons:

- Providing an open, standardized method for a master station, remote terminal unit, sensor or intelligent electronic device (IED) to verify that any given message was transmitted by an authorized device.
- Establishing control system security to utilities that are currently using DNP3 over serial links and are migrating to deploy it over LANs and WANs using Internet protocols (IP).
- Providing the flexibility to work well on serial links, IP-based networks, or combinations of the two built with terminal servers or IP radios.
- Improving the migration path for utilities considering the IEC 61850 data communications standard.
- Establishing a collaborative environment where utilities can freely dialog and share security concerns with other participants and vendors.

## Drivers and Trends

NERC CIP-005 states: "Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible."

DNP Secure Authentication also provides a mechanism that will help utilities meet the logging and auditing requirements of the CIPs by tracking the actions of individual users.

## Challenges

The DNP Secure Authentication specification lacks the capability to change the cryptographic keys used by remote devices over the DNP link. Requiring site visits to change keys could be costly. This project will develop and evaluate this missing portion of the specification.

Finding vendors willing to take a chance on implementing a new specification is difficult. EPRI support demonstrates that utilities are interested in this technology and are willing to buy devices that implement the specification.

There is a danger of "competing" security standards being developed, which could divide resources available to vendors and utilities. The DNP Secure Authentication specification is being developed simultaneously with, and based on, the IEC 62351-5 international standard.

## Project Summary

This project will:

1. Provide resources to help complete the existing DNP Secure Authentication specification in a timely manner.
2. Create an addition to the specification that can update cryptographic keys remotely so site visits are not necessary.
3. Arrange to have the specification evaluated by cryptographic experts, develop a report on the evaluation and have the specification modified according to its recommendations if necessary.
4. Arrange to have PC-based implementations of the specification tested by recognized security experts, develop a report on the testing, and have the specification modified according to the results of the testing if necessary.

5. Present papers at major industry conferences encouraging the use of the standard.
6. Develop the corresponding IEC specifications so that utilities worldwide can make use of the same technology.
7. Develop recommended wording to be included in RFPs by utilities wishing to specify the security mechanism.

## Deliverables

- The DNP Secure Authentication Specification
- Specification modifications for remotely changing cryptographic keys.
- Report evaluating the specification.
- Report on the simulation testing.
- The IEC 62351-5 and IEC 60870-5 specifications mirroring the DNP specification.
- Recommended RFP wording.

## Price [or Cost] of Project

The price to participate in the Project is \$25,000. This project qualifies for EPRI's Tailored Collaboration funding

## Project Status and Schedule

The duration of this project is 6 months and will commence in June 2008.

## Who Should Join [or Who Can Participate]

This opportunity is open to all electric utilities interested in proper, timely and cost-effective implementation of security and interested in a strategy for moving forward. Utilities using DNP over serial with plans to upgrade to TCP/IP should be particularly interested.

## Contact Information

For more information, contact the EPRI Customer Assistance Center at 800.313.3774 ([askepri@epri.com](mailto:askepri@epri.com)).

## Technical Contact

For more information, contact Madhava Sushilendra, EPRI Project Manager, 865.218.8150 ([msushilendra@epri.com](mailto:msushilendra@epri.com)).

### Electric Power Research Institute

3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA  
800.313.3774 • 650.855.2121 • [askepri@epri.com](mailto:askepri@epri.com) • [www.epri.com](http://www.epri.com)