ENERGY

CYBER SECURITY HEALTH TEST

Comprehensive, cost-effective cyber security testing for energy IT systems and smart grids
Smarter electricity grids require more complex energy IT systems, making cyber security more important and more challenging. Rigorous testing is essential to ensure your critical infrastructure is secure. DNV GL's cyber security health test offers the most comprehensive and cost-effective cyber security validation for energy IT systems, smart meters and smart grid components.

Recent years have shown rapid growth in the scale and complexity of energy IT systems. Off-the-shelf devices and open IT platforms have replaced dedicated systems, and there are far more data and access points on each system. All this makes cyber security a vast and evolving challenge. The U.S. National Institute of Standards and Technology (NIST) has identified around 60,000 cyber vulnerabilities. And new threats are discovered every day.

So how do you ensure the cyber security of your IT system and/or smart grid? Thorough testing can pinpoint any vulnerabilities, allowing you to close them down before they can be exploited.

The DNV GL's cyber security health test takes a fresh look at cyber security testing to help you identify and address more threats to cyber security than ever before. Using the proven white-box testing approach, it exploits knowledge of your system to pinpoint vulnerabilities that black-box or penetration testing could miss. It also provides detailed and testable system and procurement cyber security requirements.

By testing the device and its application within the overall system, the cyber security health test provides asset owners and suppliers with recommendations for implementing security requirements. This frees asset owners from worrying about the

technical details of cyber security, and provides a common baseline for future risk assessments.

Comprehensive testing as standard

The DNV GL cyber security health test is based on a superset of internationally accepted smart grids security standards such as IEC62351, NERC-CIP and IEEE 1686. By translating these standards into specific technical requirements for each component type, we have developed a set of detailed test cases.

Using the well-known Common Criteria-based methodology, our analysts identify which test cases are relevant to your device. Then, using knowledge of how the device is applied in your system, they perform a series of exploit and robustness tests that are tailored to energy IT and smart meter protocols. These tests are performed using state-of-the-art security tools such as Metasploit, robustness test tools that are integrated according to the IEC62443 robustness test specification and our own proprietary tools for protocol testing. Each device is tested against a global vulnerability database that is updated daily to ensure the device is resilient to all known threats.

The results of these tests verify how secure the device is to all globally known vulnerabilities. Once testing is complete, you receive a detailed report back of all our findings, highlighting potential threats and outlining possible mitigation measures. We can also provide advice on improving the device to enhance its cyber security level. This could form the basis of discussions with your own management or the device supplier.

OPERATIONAL BENEFITS

- Assesses cyber security at the deepest level
- Directly addresses vulnerabilities attackers use to gain access
- Provides data on the need for investments to improve security
- Helps management make the right decisions on measures to improve high-level security
- Provides a clear overview of the risks associated with new equipment

PROCUREMENT BENEFITS

- **Vendor engagement**
  Provides unambiguous guidelines to help vendors improve their equipment
- **Vendor requirements**
  Enables verified technical requirements for procurement
- **Vendor comparison**
  Creates a clear framework for comparing security levels between vendors

Using this white-box approach to testing, the DNV GL cyber security health test goes beyond simple robustness testing and can highlight more potential vulnerabilities than black-box or penetration testing. Moreover, in situ testing guarantees all tests are directly relevant to the device's operation environment. Hence testing does not go unnecessarily deep, ensuring a cost-effective service.

A proven cyber security partner

Unlike most other cyber security service providers, DNV GL combines traditional IT security expertise with a deep understanding of the electricity transmission and distribution industry. Our team of local and international experts draw on extensive knowledge and experience in a number of relevant areas including the energy value chain and risk management. This helps ensure all testing and the suggested mitigation measures are tailored to the specific needs of the energy industry as well as your own particular circumstances. Moreover, the cyber security health test is a part of our holistic cyber security approach and has been extensively proven in pilot projects and real-life case studies with energy utilities and component manufactures around the world.

DNV GL

Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. Operating in more than 100 countries, our 16,000 professionals are dedicated to helping our customers in the maritime, oil & gas, energy and other industries to make the world safer, smarter and greener.

In the Energy industry

DNV GL delivers world-renowned testing and advisory services to the energy value chain including renewables and energy efficiency. Our expertise spans onshore and offshore wind power, solar, conventional generation, transmission and distribution, smart grids, and sustainable energy use, as well as energy markets and regulations.
Our 3000 energy experts support clients around the globe in delivering a safe, reliable, efficient, and sustainable energy supply.