

Secure Smart Grids Need FIPS

A Technology Brief

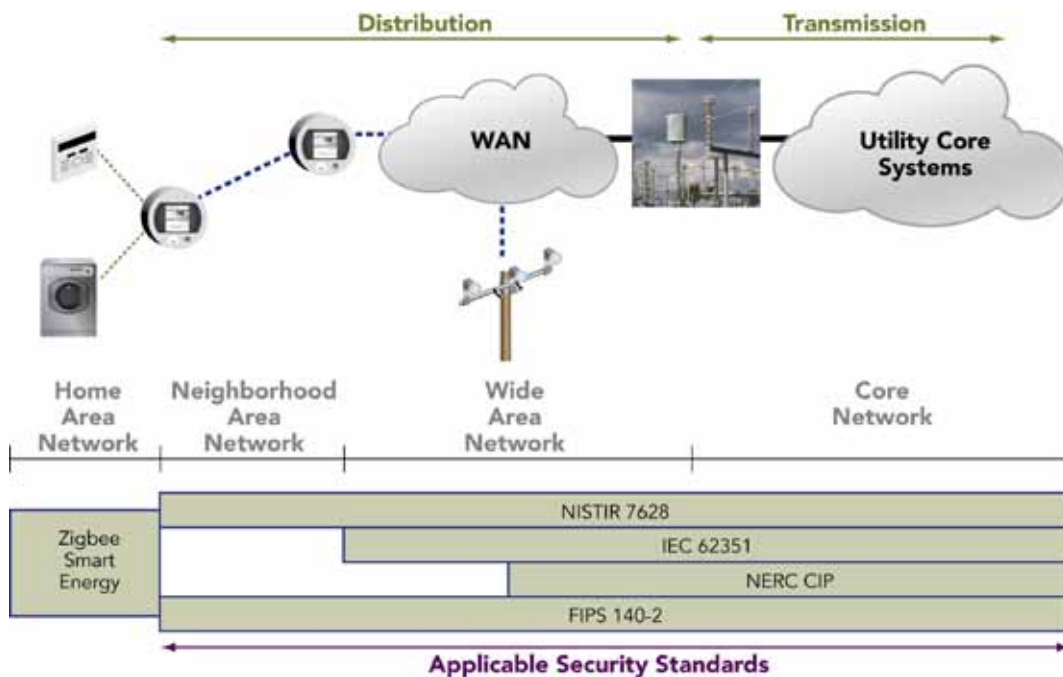
The Smart Grid is a system of systems with different security requirements at its various layers, from the home area network to utility core systems. Multiple security mechanisms operating at different layers of the protocol stacks comprise a defense-in-depth approach to security such that the impact of failure in any one mechanism is minimized and the likelihood of a successful attack is reduced.

At this time, there are several security standards being actively developed to address the security requirements corresponding to specific functional areas in the Smart Grid, including the NERC CIP standards for the bulk electric system and NISTIR7628 for comprehensive Smart Grid cyber security. Communications security standards play an especially important role in ensuring the overall security of the Smart Grid, since the network serves as the transport layer for a broad range of Smart Grid applications, including advanced metering, distribution automation and substation automation. In addition, there are several mature standards such as FIPS 140-2 for the implementation of secure computer and telecommunication systems that can (and should) be leveraged as a building block of Smart Grid security.

FIPS 140-2 is an established cyber security standard for the design and implementation of cryptographic systems (hardware as well as software) that is widely used by Federal organizations for the protection of sensitive or valuable data. While it has been applied to communications infrastructure equipment such as routers and wireless base stations, it is also applicable to any hardware or software systems that perform cryptographic functions, such as encryption, authentication, and key management. The FIPS 140-2 standard lays out specific requirements on the operating system environment, physical security protections, cryptographic services (e.g., encryption, authentication, access control and cryptographic key management), and software and firmware integrity tests for the secure design and implementation of cryptographic modules and systems.

Utility network architects can leverage FIP 140-2 certified network elements to obtain military grade security for their Smart Grid networks, ensuring independently verified security compliance from the encryption to the physical hardware.

The diagram below is an example of how a layered security strategy based upon industry standards can be effectively applied to protect Smart Grids.



555 Del Rey Avenue • Sunnyvale, CA 94085 • tel 408.331.6800 • fax 408.331.6801 • www.tropos.com • sales@tropos.com