

Get smart, get secure

The electric power grid is the beating heart of our modern economy, and securing the grid must be a top priority. Today's aging electromechanical grid provides only modest security, largely reliant on weak physical barriers and limited networked control. Tomorrow's digital smart grid introduces a ubiquitous network infrastructure that improves efficiency, raises reliability, lowers costs, and fosters sustainability... but at the same time it also increases the risk of cyberattack. Fortunately, proven security solutions can take grid security well beyond its current state. Done right, a smart grid is a secure grid.

Technologies exist for network security

Thanks to experience gained from the deployment of networks in information technology, broadband internet, telecommunications, and other sectors, the foundation for securing the smart grid already exists. Rather than reinventing the wheel for security, utilities can build upon the work of others who have successfully developed secure network technologies. For perspective, if we trust the Internet to buy billions of dollars of goods online, to move trillions of dollars of financial transactions regularly, and even to transmit highly sensitive corporate data for today's mobile workforce, we have clearly laid the technological foundation for a secure smart grid that we can trust.

Robust security from open standards

Against intuition, we must recognize that security through obscurity inevitably fails. Using proprietary protocols and burying flaws offer only limited buffers against indefatigable hackers. Instead, adopting the most proven networking platforms – and none is more universal than IP (Internet Protocol) – leverages billions of dollars of collective R&D, which has resulted in such robust security standards as [IPSec](#) (is there a better link?), which is widely used in the corporate world for Virtual Private Networks (VPNs), and [elliptic curve cryptography](#), which is utilized to protect sensitive information by the National Security Agency. Additionally, the long operational lifespans of smart grid hardware requires appropriately complex algorithms (e.g., no electronic key should be hackable during the field life of hardware) and associated physical security (e.g., unique “birth certificates” for all network gear). Finally, the massive size of smart grid networks call for security architectures that can scale effectively to encompass millions of networked devices.

Bottom line

The smart grid can improve the security of our electricity system. Indeed, smart grid networks *must* be secured against cyberattack, in order for their compelling benefits to outweigh the risks of potential compromise. Fortunately, security for the smart grid can build upon lessons learned from network experiences in other sectors. Open standards, especially Internet Protocol, serve as the critical foundation for the most robust, efficient, and scalable security solutions for securing the smart grid.