India needs to boost efforts to protect power grids against hackers

ANIL THOMAS

India has begun its journey to protect power grids against malware and hackers, but needs to pick up the pace to head off the rising cyber security risk that will come with smart grids and smart meters. Closing the gap between security and threats requires political will, asking the right questions, and requiring best-practice.

The country cannot afford to be lulled into a false sense of security by the fact that the grid – divided into five regions–is not yet widely automated and connected to external sources of potential cyber threats (e.g. smart meters) via the Internet of Things (IoT).

The clock is ticking. The National Smart Grid Mission (NSGM) started operating in January 2016 under the aegis of the Ministry of Power to plan and monitor implementation of policies and programmes related to smart grids. The ultimate vision, Smart Grid, will involve generators, service providers, and millions of consumers. The target is to achieve full rollout by 2025, including connections to renewable power sources, microgrids, electric vehicle charging infrastructure, and smart meters. Smart meters will add real-time, two-way communication to Smart Grid, thus introducing susceptibility to cyber attack.

The longer-term trend will add further automation and connectivity as a growing number of renewable power sources connect to the grid, and home and business/industry users participate in demand side response (DSR). One example of DSR will be electric vehicle owners programming smart equipment to charge their vehicles when electricity is cheapest.

The potential emergence of cross-border super grids with neighbouring nations will also increase cyber security challenges. India is already connected to Bangladesh, Bhutan, Myanmar, and Nepal; and the country's Ministry of New and Renewable Energy has proposed a globally connected power grid known as OSOWOG ('one sun, one world, one grid').

These trends indicate the need not only to design and implement fit-for-purpose cyber security measures in the short to medium term, but also to base them around standards that will allow them to be updated and upgraded to deal with whatever threats emerge longer term.

These are not abstract concepts, as recent history shows. In December 2015, Ukraine experienced the first known incidence globally of a cyber attack on a power grid, which halted electricity supply. In early 2019, hackers exploited firewall vulnerabilities to cause blind spots in monitoring at a grid control centre and some small generation sites in the US for several hours, though without disrupting electricity supply.

India has itself had a foretaste of the potential for cyber attacks on the power system to lead to major

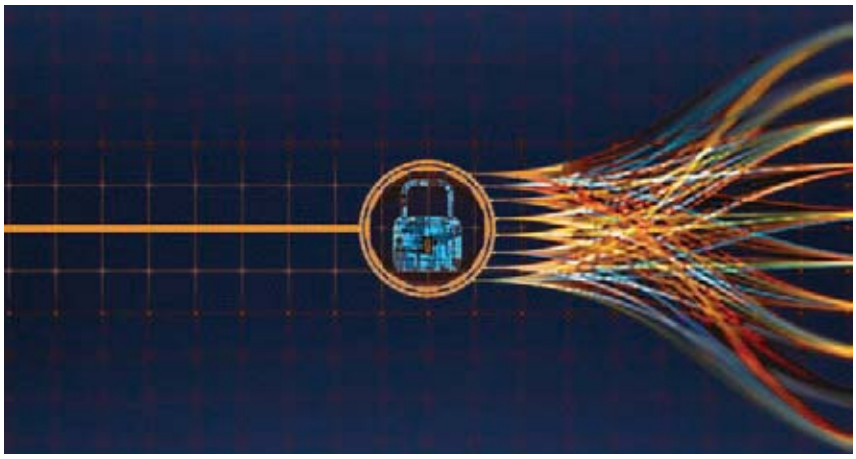
incidents that could threaten health, safety, and the environment. The confirmed malware attack on Kudankulam Nuclear Power Plant in Tamil Nadu in 2019 was a sharp reminder of vulnerabilities even though government investigations found it had been confined to a personal computer connected to the administrative network's internet server but not to operational technology systems.

Evidence has thus been accumulating worldwide to suggest that the financial costs of cyber attacks on energy systems could be huge. It is not unrealistic to envisage incidents that would leave energy companies having to spend billions of dollars to replace or repair equipment, or entire plants, if they were damaged in the future as a result of such attacks, and to settle any legal claims. This is quite apart from any reputational costs from power supplied being disrupted and, in the worst-case scenarios, fatalities and damage to health and/or the environment.

India has not sat on its hands as the threats have become more transparent and defined. In March 2017, the Ministry of Power constituted a Committee to look into cyber security. It will soon be four years since the country's Central Electricity Authority (CEA) warned that urgent measures should be adopted immediately to protect India's electricity networks.

The Government of India' Computer Emergency Response Team (CERT-In) is tasked with advising on policies needed to ensure cyber-secure power generation, transmission and distribution, load dispatch, equipment manufacturing, smart grids and microgrids.

CERT-In established a commission



that recommended grid operators should at the very least have firewalls in place. This was a first step in the right direction. The challenge now is to ramp up the pace or risk having to play catch-up as grids become smarter. To look at it another way, inadequate grid cyber security could slow the energy transition towards electricity in general, and renewables in particular. It could also delay domestic and business consumers being able to enjoy the benefits of greater control over when and how much energy they use.

The 'recipe' exists to bake cyber security into the grid as it becomes smarter and more connected. For example, India could seize the opportunity to implement best practice solutions based on tried and tested international standards such as ISO/IEC 27001. It can tailor such solutions for its own needs and priorities.

DNV GL can attest to this potential through the global perspective it has from assisting critical infrastructure operators such as electricity and gas transmission system operators. We have developed rigorous cyber security health testing to bring cyber security validation for energy IT systems, smart meters, and smart grid components. Through this, we are assisting utilities to assess the susceptibility of their control systems to hard-to-detect security breaches, and to better understand appropriate levels of cyber security for each system.

To develop detailed test cases, we have translated international security standards into specific technical requirements for each component type. Knowing how a device will be applied in a system enables out experts to perform exploit and robustness tests tailored to energy IT and smart meter protocols. It means we can verify how secure a device is to all globally known vulnerabilities.

With these insights from real industry experience, we see how growing understanding of ththreats, potential consequences, and preventative solutions are enabling knowledge sharing to better analyse gaps between cyber security and risks. We are confident that India, if it has the will and draws on in-depth industry experience, can adapt such insights to proactively limit cyber risk in Smart Grid in time to benefit from the increasing automation and connectivity that is looming along the chain from generator to end user. ■

(Anil Thomas is Head of Section, Energy Advisory, DNV GL – Energy)