Smart security for smart grid

The challenges and risks with implementing effective security and controls for smart grid

Smart grid is a highly cohesive integration of mechanical and electric components supported by Information Technology (IT) aiming to enable intelligence within the grid and allowing two-way traffic of power where electricity can be both consumed and generated and sent back into the grid by the end consumer. In order to realize the economic value of a fully deployed smart grid, select power companies are taking the necessary steps to implement smart grid networks, taking the leading edge within their industry.

In order to realize the economic value of a fully deployed smart grid, select power companies are taking the necessary steps to implement smart grid networks, taking the leading edge within their industry

In order to fully realize the benefits of smart grid, power companies must address the challenges associated with such implementations; one of the major challenges being the application of effective security and controls across the grid components. Physical security, such as guarding the perimeters of electric components, is and will always continue to be a requirement. Nevertheless, there are several challenges smart grid implementations must address in order to carry out effective security and controls for the mechanical and electric components involved. These challenges include ensuring effective controls are implemented within the smart grid architecture, safeguarding the data generated through smart grid components, and the risks of intrusion present within the different smart grid components on both the Operational Technology (OT) and IT components of the system.

Smart grid implementations are evident

Smart grid implementations are becoming evident primarily due to the benefits they identify for both power companies and their consumers. Several Middle Eastern governments recently introduced initiatives and set up channels to finance energy sector reformation. Local providers, software companies, and governments are partnering with worldwide smart grid manufacturers and early investors as a result of these policy measures.

Within the UAE, Dubai Electricity and Water Authority (DEWA) is aiming to employ a smart grid and smart meter foundation with investments totaling US$1.9 billion.

At the Mohammed bin Rashid Al Maktoum Solar Park, the world's biggest solar park in the world, DEWA has developed two pilot projects for energy storage technologies, one of the first in the Middle East. By 2030, it is expected to have an industrial capacity of 5,000 MW. This will save approximately 6.5 million tons of carbon emissions per year once completed .

Business cases for smart grid implementation identify a number of benefits which include enabling Load Management and Time of Use (TOU) billing to meet peak demand times, reducing meter reading costs for power companies, distributing generation (which in addition to integrating multiple sources of power generation, also allows for consumers to actively participate in power generation), and enabling intelligence by allowing two-way grid communication between power companies and their consumers.

These benefits propose smart grid implementations to be the smart choice in reducing carbon footprint and modernizing the grid network.

Contrary to implementing a smart grid, the business case of not implementing smart grid solutions for power companies is becoming a challenge. These challenges include maintaining status-quo and potentially increasing costs to consumers given economic inflation and increasing demand for power, risks associated with not practicing load management, lost opportunity to track data and power consumption at the individual component-levels of the grid, and lost opportunity to participate in carbon reduction/green initiatives.

Controls within the smart grid architecture

As power companies look into smart grid operations, a common smart grid architecture is becoming evident. At a high level, from the distribution perspective, the architecture includes smart meters at consumer locations (homes, offices, factories, etc.) communicating with a power region access point that transmits data back to the power companies' master data management centers where processing takes place. This is commonly supported by

Contrary to implementing a smart grid, the business case of not implementing smart grid solutions for power companies is becoming a challenge

an Advanced Metering Infrastructure (AMI), GeoSpatial Information System (GIS), and Distributed Management System (DMS).

Although a common architecture helps enforce standardization, industry acknowledged consortium reviews, and a best practiced framework for power companies, it is not evident if effective controls are in place to ensure secure and reliable two-way communication between grid components. Controls help implement preventive and detective measures, and not being able to identify and implement controls within the smart grid architecture can pose a number of threats to power companies and their consumers. These threats can include data theft, alteration, and power theft for intruders looking to collect data or steal power.

The availability of mobile computing and external storage devices can provide the tools for intruders looking to access data if they can gain access to the smart grid network through the most vulnerable points (such as smart meters, power region access points, and databases at data management centres) or obtain the correct credentials and parameters to connect to the network. Access to individual components requires controls to ensure the components collecting, processing, and storing confidential data are secure.

Controls also help mitigate risks, create audit trails, utilize logs, and enable segregation of duties. It is estimated that the 2005 blackout in Dubai could have cost residents a loss of an estimated US$73 million due to the loss of power and the interruption in telecom services if it had lasted the entire day. A cascading power outage like this could be caused by lack of controls at any point in the power grid which smart grid implementations can address.

Data generation

One of the key components of a smart grid is a smart meter. The smart meter replaces the current analog meters and increases functionality to collect data on electricity consumption during different times of the day. It is estimated that a residential smart meter collecting data and forwarding to the master data management center will require approximately 170 Megabytes (MB) of data storage per meter per year if data is collected twice a day. According to the Advanced Electronics Company (AEC), Saudi Arabia is one of a small set of countries working on big plans to shift from traditional electrical grids to smart grids. One of the Kingdom's key efforts is reflected in the aspirational 'Vision 2030' plan. By the end of the next decade, it is expected that the KSA will have established itself as a global hub for smart energy technology. This initiative will spread the smart meters to a huge margin; thus, data collection and reports will be updated frequently.

By collecting vast amounts of data, power companies have an increased responsibility to secure their data collection and storage techniques. Securing the data generated through smart meters will assist power companies in building customer trust, which is essential as it provides assurance that the organization is meeting legal 'protection of consumer privacy acts' and fulfilling its communicated commitments. Losing consumer trust can lead to legal actions against power companies resulting in unnecessary costs. Similarly, unsecured customer data can also be subject to theft, which can result in failure to comply with 'protection of consumer privacy acts' as well.

One of the key components of a smart grid is a smart meter. The smart meter replaces the current analog meters and increases functionality to collect data on electricity consumption during different times of the day.

Risks of intrusion

There are multiple points of intrusion within a smart grid that must be monitored, safeguarded, and controlled to ensure effective security measures and controls have been implemented. Network entry points, such as smart meters at each consumer end point with a connection back to the power company over wireless transmission, carry an inherent risk of intruders being able to gain access to the network to gather information and potentially alter the information being transmitted back to the master data management center. This risk creates integrity concerns on the data being collected, which can result in mislead decision-making by processes and systems relying on the data.

Safeguarding the grid against intrusion under defined security standards can support benefits associated with the 'smart-security for smart-grid' concept. Smart security measures can protect grid wide intrusion points, such as residential and industrial meters and other smart grid components located within the power company perimeter. These protection configurations can address both data protection and failover scenarios for the different components integrated within the grid.

Smart security

The threats and vulnerabilities identified drive the need to enforce smart security standards and ensure measures taken to implement 'security-in-depth' are regulated and applied for smart grid implementations. Effective application of security and controls across grid components can ensure the data generated is accurate, stored, and analyzed in a manner where confidence in the integrity of data can be maintained. It can also allow power companies to engage in 'risk-intelligent' approaches by allowing them to balance the risks such as security, privacy, and business continuity to the costs associated in delivering the true value of smart grid implementation.

Smart security can also support a flexible, manageable, and consistent configuration among the smart grid architecture which can allow scaled protection from as low as 500 access points (power company offices, substations, and generation stations) to over 1,000,000 (residential, consumer, and industrial smart meters) access points. Smart security can also allow staff, contractors, and auditors to do their jobs effectively by implementing preventive, detective, and corrective measures while ensuring responsible resources are assigned least privileged access.

In the end, security is everyone's responsibility. The challenges presented for smart grid implementation can be approached in a positive and effective way by utilizing a structured 'risk-intelligent' method. The tools and technology can be made available; however, it is how we decide to use them that will prove to be successful after all.

By **Ali Khan**, Partner, Cyber Detect & Respond Leader, and **Tamer Charife**, Partner, Energy, Resources & Industrials Cyber Leader, Risk Advisory, Deloitte Middle East

Endnotes

1. Smart Grid Report. https://www.dewa.gov.ae/~/media/Files/About%20DEWA/Smart%20Grid%20Report%20EN.ashx?la=en
2. Blackout cost Dh11m an hour | Business – Gulf News. https://gulfnews.com/business/blackout-cost-dh11m-an-hour-1.290410

Effective application of security and controls across grid components can ensure the data generated is accurate, stored, and analyzed in a manner where confidence in the integrity of data can be maintained