Ensuring Your Power Metering and Energy Management Applications are Cyber Secure

Cybersecurity Risks in Power Metering and Energy Management

As cybersecurity concerns rise worldwide, the potential risk for utilities and commercial/ industrial energy metering increases significantly. The need for robust cybersecurity measures to protect energy management systems of all sizes cannot be ignored. US Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, signed by the U.S. President in 2017, acknowledged the need to strengthen cybersecurity in response to growing concerns.

As mentioned in Tucker Bailey's article from 2020, utilities especially are attractive targets of bad actors abroad, protestors against the energy sector, and cyber criminals looking for a big payout. There are multiple factors that cause utilities to be vulnerable to cyber attacks, including the critical nature of the industry, its "large attack surface" with many decentralized parts, and the interdependence between the physical and cyber infrastructure. These all render electrical utilities "vulnerable to exploitation, including billing fraud …, the commandeering of operational technology (OT) systems to stop multiple wind turbines, and even physical destruction."[1] And newer, renewable energy sources face the same kind of threats. In fact, in his article on this topic, Danny Palmer states "…the rapid transition towards renewable energy could lead to additional avenues for cyber criminals to exploit."[2]

Metering Cybersecurity Concerns

One access point to energy management data is through metering communication. To address this risk, among others, the North American Electric Reliability Corporation (NERC) designed the Critical Infrastructure Protection (CIP) guidelines. These have been updated by a newer NERC committee, the Reliability and Security Technical Committee (RSTC), which publishes guidelines for reliability and security for bulk power systems in North America. These guidelines provide means for companies to evaluate their level of security and protection against physical threats as well as tampering and hacking of critical data. The guidelines explain the types of encryption needed to secure bulk power systems' data. As NERC said in a recent statement "Security of the grid continues to be a key priority for NERC, the U.S. and Canadian governments and industry. "[3] Without appropriate encryption and other cybersecurity measures, there is no way to ensure the safety of bulk power systems' data.

---

[1] *The Energy Sector Threat: How to Address Cybersecurity Vulnerabilities,* Tucker Bailey, November 3, 2020; website link https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities

[2] Danny Palmer, website link https://www.zdnet.com/article/the-race-towards-renewable-energy-is-creating-new-cybersecurity-risks/

[3] *Statement in Response to Grid Vulnerability,* 2/28/2022, website link https://www.nerc.com/news/Pages/Statement-in-Response-to-Grid-Vulnerability-.aspx

Cyber Secure Metering

The basis of cyber secure metering is encryption. Encryption takes metering data, for example, usernames, passwords, or firmware files, and changes it into a string of characters that is no longer readable without the correct key. Encryption takes place with complicated algorithms that are transparent to the user of the system. The Advanced Encryption Standard (AES) is maintained by the National Institute of Standards and Technology (NIST). A study released by NIST in 2018 stressed the importance of implementing AES encryption, estimating that its usage produced a 1,976-1 benefit to cost ratio for the U.S. economy.[4]

Electro Industries (EIG) produces meters and energy management software with AES encryption-based advanced cybersecurity. One example of this is the Nexus® 1500+ Power Quality meter. The Nexus® 1500+ meter has EIG's latest Resilient Cyber Security™, which complies fully with utility security requirements. Details of the Nexus® 1500+ meter's cybersecurity include:

- AES 128-bit encrypted communication - It is estimated that it would take a supercomputer *billions* of years to crack a 128-bit encryption key.[5] The Nexus® 1500+ meter protects passwords, usernames, roles, and rights using AES 128-bit encryption.
- Role-based authorization - The Nexus® 1500+ meter offers multiple roles to restrict access to meter data and configuration. It has an admin level with full rights and up to ten configurable user levels.
    - Only the admin level can create user profiles and permissions, usernames, or passwords.
    - Only the admin level can enable or disable security for the meter.
    - The admin can program expiration dates for passwords to further secure data by periodically setting up new passwords.
- Password fail timeouts - To prevent brute force hacking, in which a system is inundated with multiple password entries in an attempt to identify the correct password, the meter has password fail timeouts. The timeouts will block password entry for a designated period (from one minute to 24 hours) after three consecutive incorrect passwords are entered. This breaks the chain of password hacking.
    - The admin level can view any authorized users that are in lockout due to failed password attempts.
- Digitally signed firmware - A digital signature is an encrypted value, or "key," attached to a file. Before the firmware can be uploaded to the meter, the file 's key is decrypted by the public key in the Nexus® 1500+ and 1450 meters. This ensures that the firmware file is authentic and valid, so that the meter cannot be hacked or infected with malware files.

[4] NIST's Encryption Standard Has Minimum $250 Billion Economic Benefit, According to New Study, September, 2018 ; website link https://www.nist.gov/news-events/news/2018/09/nists-encryption-standard-has-minimum-250-billion-economic-benefit

[5] What Is AES Encryption? [The Definitive Q&A Guide], Brett Daniel, March 31, 2021; website link https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered#:~:text=128-bit%20AES%20encryption%20refers,not%20top-secret%20government%20information

    - In addition to the signed firmware, EIG's CommunicatorPQA® meter configuration, polling, and data management software is digitally signed for a secure installation.
- Security lock - For applications with the most stringent security needs, the admin level user can implement a security lock. This will prevent the security from being disabled, even by the admin. The security lock is implemented in the meter's firmware and enabled via the meter's display.
- Sealing switch -The Nexus® 1500+ meter's sealing switch acts as a physical barrier, requiring a meter button to be pressed in addition to software password entry. This is an added level of security, since the button is located under an area that can be secured with a physical seal and which would indicate tampering if removed.
- Physical seals - The meter's seals prevent unauthorized access and indicate if tampering has been attempted.
- Anti-tampering System Events log - The System Events log records any actions in the meter, such as password entry, meter resets, log downloads, etc.

In addition to the Nexus® 1500+ and Nexus® 1450 meters and the CommunicatorPQA® software, EIG offers the following meters and applications with advanced cybersecurity:

- Shark® 250 power and energy meter.
- Shark® 270 socket and switchboard form revenue meter.
- EnergyPQA.com® AI based energy management system, which offers an Enterprise Cloud solution.
- HMIPQA+™ SCADA application.

The Future

To address geo-political concerns, power systems and critical infrastructure must be better protected, not only at the IT level, but at the equipment itself. Every day, there are new advances in cybersecurity threats. Most of the installed base of metering technology relies solely on password protection or there is no password protection at all. This lack of security is a very compelling reason to retire these older technologies and upgrade them to better face new threats as they arise.

Ensuring that the metering and recording equipment is cyber secure protects the power system infrastructure. It allows users to be confident that the data relied upon is correct and unhampered by malicious code, tampered user settings, and/or vulnerability due to security deficiencies. For this reason, EIG has set cybersecurity as a primary goal for each new product's release.