APU INSIGHTS

Product of APU Commercial Information Services LLC

Smart Grid Revolution

How AI-enabled power distribution systems ensure maximum savings, efficiency & consumer satisfaction

SMART IDEA & PRACTICE

SMART PAPERS

INDEX

Introduction

Section 1
Four key factors impacting power distribution

Section 2
Five AI techniques and their four-step launch process

Section 3
Seven key advantages of using AI in power grids and top use cases with their lessons

Conclusion

WATCH DIGITAL FUTURES VIDEO

DIGITAL FUTURES

DIGITAL FUTURES is an online content publication platform catering for technology business leaders, decision makers and users, by sourcing and sharing valuable information and best practices in connection to the latest emerging technologies trends and market developments that leverage capabilities and contribute towards enhanced enterprise-wide performance.

WATCH VIDEO

LEARN MORE ›

Introduction

Today's buzz around mobile phones, streaming, the Internet of Things, cryptocurrency, reflect the new digital technology trends, but recent advances in power supply rarely appear on literature for the reason it is taken for granted despite its fundamental impact on society. With the world becoming more connected every day, having a continuous and uninterrupted flow of electricity is out of question. The increasing demand for renewable resources, either for industrial or personal use, and the emergence of autonomous vehicles have transformed energy solutions, triggering massive adoption.

The other side of the coin, though, reveals cybersecurity threats against existing power systems. The growing threat of hacking has become a costly, increasing trend, due to the fact that smart meters and automated control account for 10 percent of global grid investments, worth USD 30 billion per year.

Power loss can be attributed to various factors, such as the installation of smart meters at consumer premises without meeting security standards, automated operations with no proper protection plan, and extreme weather conditions. Furthermore, non-technical reasons are also precarious, which concern fraudulent activity, such as tampering meters and stealing power by direct hooking. All the aforementioned threats have created further volatility in the distribution system, compromising the grid's reliability.

Cybersecurity attacks in power grids can cost ***USD 30 billion*** ***annually.***

Artificial intelligence can solve such complicated problems by improving the efficiency of electricity networks and decreasing errors through advanced digital capabilities and instant decision-making. Both elements minimize the risk of manipulation and corruption. But more importantly, AI has the potential to ensure significant savings in energy, accelerating the deployment of clean and green power systems, like smart grids that allow two-way communication between infrastructure and consumers. This new approach enables real-time measurement and data alignment from multiple remote points across the network, facilitating better grid management, particularly during urgent conditions.

Several countries have taken serious action to implement smart grids, including Brazil, China, Gulf Cooperation Council countries, South Africa, and others, but the rest of the globe has fallen behind due to sluggish economic development. In the business world, DeepMind, a Google subsidiary, has applied machine learning algorithms to 700 megawatts of wind power in the central US to predict power output 36 hours ahead of actual generation. This is feasible through neural networks trained on weather forecasts and historical wind turbine data. Below are some top applications of AI, described with more details on the next section, targeted to restore the grid's dependability:

- ***Identifying deceitful activities in the network, such as meter tampering and hooking to the lines***
- ***Estimating equipment failure to support the maintenance of the device before actual failure and subsequent blackout scenarios***
- ***Forecasting of renewable energy production to accurately project consumer demand, enabling quick committing and flexible load generators***
- ***Optimizing resources for enhanced grid stability and reliability*** [1]

[1] Makala, B., Bakovic, T. (2020, April). Artificial intelligence in the power sector. IFC.

SECTION 1

Four key factors impacting power distribution

1. Soaring cybersecurity threats

Energy is considered one of the fundamental building blocks of modern society. According to the European Union Agency for Cybersecurity (ENISA), it is one of the only two most critical segments across 18 European states because of the direct and indirect humongous impact it has on the rest industries and day-to-day activities. On the other hand, power production is the most affected by cyber crime, thus being the most costly in all affected sectors.
A number of cyberattacks incidents have occurred across the length of the energy supply chain including generation, transmission, and distribution stations and networks. With respect to the primary source, attackers have targeted oil and gas industries and at times, even nuclear power plants. One of the most worrying aspects concerning cybersecurity is that a lot of intrusions have been kept undisclosed to the general public or not discovered at all.

Studies have shown that the detection of the existence of an intruder in the network if at all discovered, takes for an organization between 12 days. This demonstrates its complexity and the extent of harm they can create in the systems. Although identifying an incoming threat has recently reduced, it is still unacceptably high.

Smart grids are the most trickly structures to monitor. According to the head of information security at Enel, Italy, the company had huge background noise on a daily basis, in its search for cyber security threats with over 100,000 events noticed by their global IT security team. The idea here is that this noise is a strong indication that there are skilled attackers that can hide their traces behind those noises, making it extremely difficult for the enterprises to identify intrusive elements in their infrastructure.

Sophisticated malware and toolkits have been developed to compromise the health of power systems with some of the most popular assaults illustrated below:

Stuxnet was designed in 2010 to reduce the maximum spin speed of nuclear centrifuges. This resulted in the destruction of about one-fifth of the Iranian nuclear centrifuges. While the main target of this malware was that particular facility, it was much later identified in other energy plants.

Shammon attacked Saudi Aramco and RasGas systems in 2012, making thousands of workstations redundant with sever operational implications. Its updated version n 2016 targeted more companies in Saudi Arabia and later in Italy in 2018.

Dragonfly/Havex – Havex is a Remote Access Trojan (RAT) malware that can control a system through a remote network connection. Dragonfly leveraged Havex to collect information targeting different industry sectors, impacting 2,000 sites, mostly in Europe and the US.

BlackEnergy – Starting from a web-based distributed DDoS platform, this malware evolved into a plugin architecture. It infected the SCADA systems of a regional Ukrainian electricity facility in 2015. As a result, several substations were disconnected for about 3 hours, leaving more than 200,000 customers without power during a cold winter day.

SMART PAPERS

APU INSIGHTS

Product of APU Commercial Information Services LLC

SMART IDEA & PRACTICE

Designed and produced by APU Insights Creative Studio

FOLLOW OUR THINKING :