Cyber attack impact on power system blackout

The Transportation Department said on Friday that U.S.-based airlines must provide affected passengers compensation for flight disruptions set off by the global software outage that had roiled air ...

Publicly available information on significant cybersecurity incidents is limited due to under-reporting and lack of detection. However, there is increasing evidence that cyberattacks on utilities have been growing rapidly since 2018, reaching alarmingly high levels in 2022 following Russia"s invasion of Ukraine.

Emerging Risk Report - 2015 Innovation Series SOCIETY & SECURITY Business Blackout The insurance implications of a cyber attack on the US power grid About Lloyd"s Lloyd"s is the world"s only specialist insurance and reinsurance market that offers a unique concentration of expertise and talent, backed by strong financial ratings and international licences.

Power companies have long been aware of growing cyber risk, and were one of the first industries to respond, with requirements to implement cybersecurity controls through the North American Electric Reliability Corporation"s Critical Infrastructure Protection (NERC-CIP) standards, initiated in 2007.

Blackouts in a power system can occur in several ways. How to prevent a blackout is an important issue in power systems. The reasons to cause blackouts can be the overloading of transmission lines ...

"The cyber incident exacerbates the impact of the physical attack," says John Hultquist, Mandiant"s head of threat intelligence, who has tracked Sandworm for nearly a decade and named the group in ...

The aggregated impact of a cyber attack on the U.S. power grid could cause huge economic losses and upheaval. ... The controllers used in Iran are the same as those used in U.S. military systems, power plants, water ...

1 School of Electrical Engineering, Yanshan University, Qinhuangdao, Hebei, China; 2 Smart Distribution Center of State Grid Jibei Electric Power Limited Company, Qinhuangdao, Hebei, China; Improving the accuracy of the vulnerability assessment of the power cyber-physical system has important practical value for protecting the vulnerable links of the ...

Coordinated cyber attacks against the protection system in digital substations may cause generation and line disconnections, triggering cascading failures in the power grid. This may ...

The U.S. power system has evolved into a highly complex enterprise: 3,300 utilities that work together to deliver power through 200,000 miles of high-voltage transmission lines; 55,000 substations ...

Cyber attack impact on power system blackout

Russian hackers targeted the Ukrainian power grid and attempted to cause a blackout that would have hit 2 million people, according to Ukrainian government officials and the Slovakian ...

Power system automation and communication standards are spearheading the power system transition towards a smart grid. IEC 61850 is one such standard, which is widely used for substation automation and protection. It enables real-time communication and data exchange between critical substation automation and protection devices within digital substations. ...

Future power system blackout studies and risk assessments shall take this into account as well. ... Increased failure rate of a cyber-attack on the CPP system impacts the CPP system considerably however, value of impact varies with various power system components. Fig. 16 and Fig. 17 show the base case and scenario D load shed and EENS ...

The looming threat of cyberattacks on power grids, however, may result in unprecedented large-scale cascading failures, leading to a blackout. Therefore, new analysis methods are needed to study ...

The cyber-security company Information Systems Security Partners (ISSP) has linked the incident to a hack and blackout in 2015 that affected 225,000. It also said a series of other recent attacks ...

The aggregated impact of a cyber attack on the U.S. power grid could cause huge economic losses and upheaval. ... The controllers used in Iran are the same as those used in U.S. military systems, power plants, water systems, transportation, manufacturing and other commercial and industrial enterprises, said cyber security expert Joe Weiss ...

The statement also added that actions were taken to prevent any damage to the power systems. "There is no impact on any of the functionalities carried out by Power System Operation Corporation (POSOCO) due to the referred threat. No data breach/ data loss has been detected due to these incidents," it read.

The power outages at the distribution system level lasted for several hours and affected 225,000 customers in the Ivano-Frankivsk region. As similar cyber attacks occurred again in Ukraine one year later, it is important to analyze the impact of the 2015 cyber attacks on power systems dynamics and assess how they can lead to a complete blackout.

2016 [7]. These are the first and only known cyber attacks to directly result in power outages. cascading failure analysis, 2) cyber FIGURE 2. Timeline of power system related cyber security incidents

This is exactly what happened in the 2003 Northeastern blackout, ... Cyber attacks on power system state estimation through topology errors, in IEEE Power and Energy Society ... A.G. Phadke, S. Horowitz, Hidden failures in protection systems and its impact on power system wide-area disturbances, in Proceeding of IEEE Power Engineering ...

Cyber attack impact on power system blackout

In addition to lower rates of job postings, power utilities have difficulties recruiting and retaining cybersecurity employees due to three main reasons: A worldwide shortage of cybersecurity workers across all sectors, estimated at 3.4 million people in 2022.

The cyber-physical power system achieves the controllability and observability of the power system through ubiquitous sensing technology, advanced measurement technology, and powerful ...

The operational impacts of cyber-attacks on power system security, as well as the economic impact on deregulated energy markets, have been extensively explored. In addition, the robustness of security features and cryptographic methods against various cyber-attacks is investigated to suggest unexplored cyber-attacks for future scope.

However, the measurements need to be transmitted to the control center over communication links, and, therefore, power systems face potential cyber-attacks because of the vulnerability of communication technologies. For example, a malicious agent may inject false data to induce the operators to make the wrong decision on the system status.

Unknown. Most likely, the hackers intended to test a remote cyber operation directed against Ukraine"s critical energy infrastructure. Result The attack resulted in power outages for nearly 225,000 consumers in Western Ukraine. The malware disconnected electrical substations, causing the blackout.

In recent years, cyber attacks have garnered attention from scholars as emerging security threats [6].Due to the reliance of CPPS on network subsystem monitoring and control [7], such attacks can be highly destructive [8], [9].The 2015 blackout in Ukraine stands as a stark illustration of how malware can propagate through communication networks, leading to widespread assaults on ...

This review article thoroughly investigated possible ways to address cyber security challenges such as smart meter security, end-users privacy, electricity theft cyber-attacks ...

With the rapid development of the smart grid and increasingly integrated communication networks, power grids are facing serious cyber-security problems. This paper ...