Electrical Infrastructure Vulnerabilities

The Electric Grid: Electricity, something that we all take for granted, is a critical component of modern life. It is delivered to our homes and businesses via an interconnected network that connects producers and consumers. This network consists of generating stations that produce the electricity, high voltage transmission lines that carry the power from distant sources to demand locations, and lower voltage distribution lines that connect to individual customers.

The generating stations, which are generally quite large, are often located away from heavily populated areas. In order to minimize transmission losses, high voltages are used to transmit power over long distances. Transformers allow the generated power to be stepped up to the required higher voltage in order to connect to the electric power transmission network. Transformers are then used at the local sub-station at the other end to reduce the high voltages back down to the 120V used by consumers. America utilizes approximately 2500 large transformers, some of which are almost 40 years old and have unique designs. Currently, only about 500 units can be built per year worldwide and typically it takes a year or more for delivery.

In North America, the power transmission grid is divided into regions. The two largest are the Western and Eastern Regions. There are three other regions—the Texas Interconnection, the Quebec Interconnection and the Alaska Interconnection. The five regions are not directly connected or synchronized to each other, but there are some High Voltage DC and Variable Frequency Transformers that allow for a controlled flow of energy between regions while maintaining isolation between regions.

Threats: Several threats to power distribution networks have been identified. These include a coronal mass ejection (CME) from the Sun; an electromagnetic pulse (EMP) event generated from a high altitude nuclear detonation, and cyberattacks.

CME: A CME is a giant cloud of charged particles blown away from the Sun during a solar flare event. The solar flare portion reaches the Earth in eight minutes, while the CME typically takes one to two days. While a solar flare can cause temporary communications outages, a CME, which interacts with the Earth's magnetic field to create a geomagnetic disturbance (GMD), could induce very large currents in transmission lines leading to damage or destruction of transformers and support equipment.

A major CME event could have very broad impact to the network leading to a downtime on the order of months. However, NASA now has a fleet of heliophysics observatories in space. Using data from these satellites, NASA can make forecasts on CME events and issue warnings to grid operators to allow them to isolate vulnerable equipment. Although the probability is generally considered low, a CME event of sufficient magnitude could potentially cripple the power distribution network if operators did not act to protect the network.

EMP: An optimized nuclear device detonated over the central U.S. at a high altitude (30-400 km above the earth) would generate an EMP event with line of sight damage, i.e. it could cover most of the continental United States and Canada. A high altitude EMP, also known as HEMP, event couples to and can damage electronic systems, but the main risk is to long-line networks such as the electrical power transmission lines and long-haul communication lines. The induced currents could damage or destroy the hard to replace transformers in the electric power transmission lines. Except for critical military assets, our critical national infrastructure remains largely unprotected. Former CIA director James Woolsey and other national security experts have said that an EMP attack is a real and credible threat for Texas and the country as a whole.

With regard to the Texas Interconnect, six members of the Texas state Senate, including members of both parties, are co-sponsoring legislation that—if passed—would begin the process of securing the state's electric power grid from an EMP attack. "The electric power grid is vulnerable to what legitimate experts classify as high impact threats," State Senator Bob Hall, a co-sponsor of Senate Bill 83, said while introducing the bill before the Senate Committee on Business and Commerce. The bill would

create a task force to assess vulnerabilities in the state's electric grid and make recommendations on how to secure the grid against attack by September 1, 2018. The bill stalled in the legislative session.

Because of the long lead times to replace the critical transformers and related equipment, the damage from a HEMP event centered over Nebraska could lead to the power infrastructure being off-line for an extended time lasting many months to possibly years. There is broad consensus that such an event would be catastrophic for the country. Unfortunately, that is where the consensus ends. The position of the privately owned electric companies is that the best answer lies in prevention of an attack as opposed to actually implanting hardening techniques.

Cyberattacks: As the world's infrastructure has become more interconnected the threat from increasingly sophisticated cyberattacks has increased significantly. Two attacks on the Ukrainian power grid in the last two years have highlighted the threat. The first attack occurred on December 23, 2015 with the result that approximately 230 thousand people were without power for 1-6 hours. The attack began by compromising the corporate network with malware. They then seized control of the supervisory control and data acquisition (SCADA) software and began switching substations off. Disabling and destroying IT infrastructure components and server data to prevent operators from regaining control followed this, while a denial of service attack prevented updates to consumers.

The next attack occurred in December of 2016. This attack moved up the circulatory system of Ukraine's power grid. The attack in the prior year had centered on substations. Now, the hackers went after a major transmission station, which handled a larger electric load than the 50-plus distribution stations in the 2015 attack combined. Analysis of the 2016 attack indicated that the malware was able to directly control grid equipment. This means that the software could be used to map out targets, and then launch an attack at a preset time without the hackers having direct Internet control. This was the first malware found in the wild since Stuxnet that is designed to independently sabotage physical infrastructure.

The impact of these attacks has been in terms of hours. However, the capabilities of the hackers are increasing. The attacks on the Ukrainian power infrastructure were used to develop and test new cyber-tools, which would give hostile actors the ability to damage and/or destroy critical infrastructure. In 2007, a team of researchers at Idaho National Lab demonstrated that it is possible to destroy power-generating equipment using nothing but digital commands. This indicates that with the right exploit, it could be possible to permanently disable power-generation equipment or even the massive, difficult-to-replace transformers that are required for power transmission. This could lead to an outage lasting months.

http://www.smithsonianmag.com/science-nature/what-damage-could-be-caused-by-a-massive-solar-storm-25627394/

https://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield

https://www.nasa.gov/content/goddard/the-difference-between-flares-and-cmes

https://en.wikipedia.org/wiki/Continental_U.S._power_transmission_grid

https://www.economist.com/news/world-if/21724908-huge-potential-impact-rich-countries-prolonged-loss-electricity-disaster?frsc=dg%7Ce

https://www.nasa.gov/content/goddard/the-difference-between-flares-and-cmes

http://www.eei.org/issuesandpolicy/cybersecurity/Documents/Electromagnetic%20Pulses%20%28EMPs%29%20-%20Myths%20vs.%20Facts.pdf

https://energy.gov/sites/prod/files/2017/01/f34/DOE%20EMP%20Resilience%20Action%20Plan%20January%202017.pdf

https://www.wired.com/story/russian-hackers-attack-ukraine/

https://energy.gov/oe/activities/cybersecurity-critical-energy-infrastructure

https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack