




Utilities, Critical Infrastructure and Cyber Security

 Dr. Mani Vadari

May, 2015

Meet the Author:

An IEEE Fellow, electricity industry visionary, and leader, Dr. Mani Vadari delivers strategic services to a global set of utilities, vendors, and service providers seeking deep subject matter expertise in setting the business and technical direction to develop the next-generation electric/energy system. As a Business Architect, Dr. Vadari has been delivering solutions focusing on Transmission/ Distribution/ generation operations, Energy markets, and Smart Grid for over 35 years. In addition, he is an Adjunct Professor at Washington State University and an Affiliate Professor at the University of Washington. He has published two popular books, "[Smart Grid Redefined: Transformation of the Electric Utility](#)," and "[Electric System Operations – Evolving to the Modern Grid, 2nd Edition](#)", in addition to over a hundred industry papers, articles, and blogs. His books are serving as textbooks at several universities in the US and around the world

<https://www.moderngridsolutions.com/>

Is utility cyber security in dire straits and how should utility cyber security be addressed in this age of increasing digitalization, growing reliance on intelligent energy devices, and the rapid deployment of distributed energy resources?

Key terms – Energy security, critical infrastructure, impact on the US and global economy?

In 2003, the US National Academy of Engineering identified electrification as the top engineering achievement of the 20th century, meaning that this singular capability had the greatest impact on life during and following this period. The power grid is the core mechanism through which this ability is delivered to growing economies around the world. Places where the power grid does not exist – are noticeably behind in economic progress than others that do. Over time as the electric grid has grown primarily in developed economies and in other places, it has become somewhat indispensable to everything that is required to sustain the economy – so much so that life seems to come to a standstill when there is an outage.

For the longest period of time, cyber security was not an issue with the electric grid. This was because of three main factors:

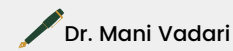
- *The core principles behind the flow of electricity from one point to the other are based on physics (Kirchoff's law, Maxwell's equations, and so on). And more importantly, the consumption of electric power at any point in time is exactly equal to the power generated at that instant of time.*
- *Most control systems such as SCADA, EMS, and other similar systems that monitored and controlled power flow were implemented and operated in isolation from the rest of the communications systems.*
- *The sensors and controls fed these centralized control systems communicated through proprietary (and closed to the internet) communication networks and proprietary protocols thereby making it very difficult for hackers to get in and do anything.*

However, while the law of physics is not changing, everything else is changing – with the Smart Grid, several changes have been happening.

- *Newer systems such as DMS, OMS, and DRMS are being implemented. These and some of the pre-existing systems identified above, are now becoming more connected and becoming less isolated from the internet.*
- *The sensors and controls (including Smart meters) that are being installed everywhere are being moved from proprietary mechanisms to IP-based mechanisms.*

These two changes identified above have brought incredible flexibility to the electric utility industry – because they have allowed greater change to come in at a much faster pace. However, they have also brought in the same vulnerabilities that have plagued the rest of the computer world – something we see in the news almost on a daily basis.

Utilities, Critical Infrastructure and Cyber Security



So – where is the cyber threat?

The core threat comes from the ability of a hacker to get into one or both the bullet items identified above and perform one or more of the following actions:

- *Opening or closing one or more (or all) remote-operated switches – thereby causing a combination of overloading, and loss of load – which could lead to fuses tripping and cascading outages*

The same action above also could cause an unsafe environment for utility crews working on various power equipment leading to either injury or death.

- *Interrupting communications on the utility network causes a lack of observability on the electric grid leading to faulty decisions by the system operator.*

And several other similar issues

So – How serious is this threat?

This is a very serious threat and unlike cyber hacking of financial networks can lead to the ultimate end result of causing people to die. So, Yes this is very serious and must be taken as such. To combat this threat, it is important to re-assess the grid from the bottom-up from a security perspective and plug all possible areas from where a hacker can get into the network and set the standards to ensure that it is safe.

Now – for something innovative-

There is a lot of work being done on intrusion detection from a communication network perspective. The idea here is to monitor the communications network to check for hackers who may have entered the network through some form of a back door and then shut them out.

New research being conducted is looking at electrical networks and searching for anomalies in the behavior to see if there is evidence or a pattern of external interference. We believe that this research has the potential to make cyber threats more benign because when successful, it can eliminate the threat even before it can cause harm.