Education on Cybersecurity Issues with Smart Power Grid

Dr. Mohd. Hasan Ali

Associate Professor

Electrical and Computer Engineering

The University of Memphis, USA

June 10, 2022

Smart Power Grid Concept

Motivation:

 # Much more renewable energy sources are going to be integrated into the existing power grid systems, which will make the network more complex. Fault current level will be increased; consequently circuit breakers need to be upgraded.

 # Maintaining stability, reliability, quality, and security of the power network will be major issues.

Smart Grid Aims:

 # The aim of the smart grid is to improve the efficiency, reliability, economics, and sustainability of the production and distribution of electrical power.

 # Two-way digital communication and computer-based remote control and automation are the keys to a smart grid system.

What is Smart Power Grid?

Smart Grid: Communication-enabled intelligence for the electric power grid.

Three Main Components of Smart Grid:

1) Electric power system
2) Communication and networking
3) Embedded and distributed intelligence

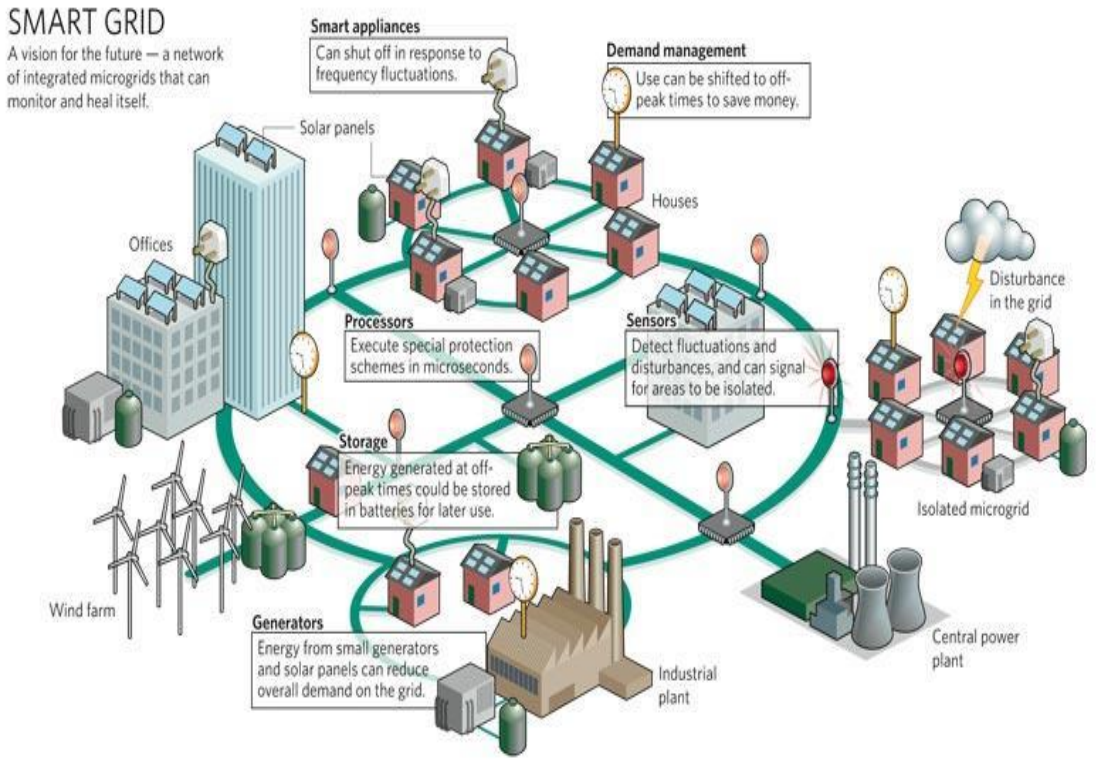

Fig. 1. Smart grid layout.

Distributed Energy Resources (DERs)

 # Distributed energy resources (DERs) are small-scale units of local power generation connected to the power grid at the distribution level.

 # DERs can include behind-the-meter renewable and non-renewable generation such as rooftop solar photovoltaic (PV) units, natural gas turbines, microturbines, wind turbines, fuel cells, battery energy storage, electric vehicles (EV) and EV chargers, controllable loads, and demand response applications.

 # DERs may provide reliability during outages resulting from adverse events, manage energy expenditures, meet customer desires to reduce their environmental footprint and/or support new evolving technologies.

 # One of the major challenges is cyber vulnerabilities in DERs and associated control and resulting large scale impact on the power grid.

 # One of the important DERs is the solar PV system which is connected to the grid through the smart inverter (which converts DC power generated from PV modules to AC power).

Investment in "Smart Grid" electricity infrastructure will be needed….

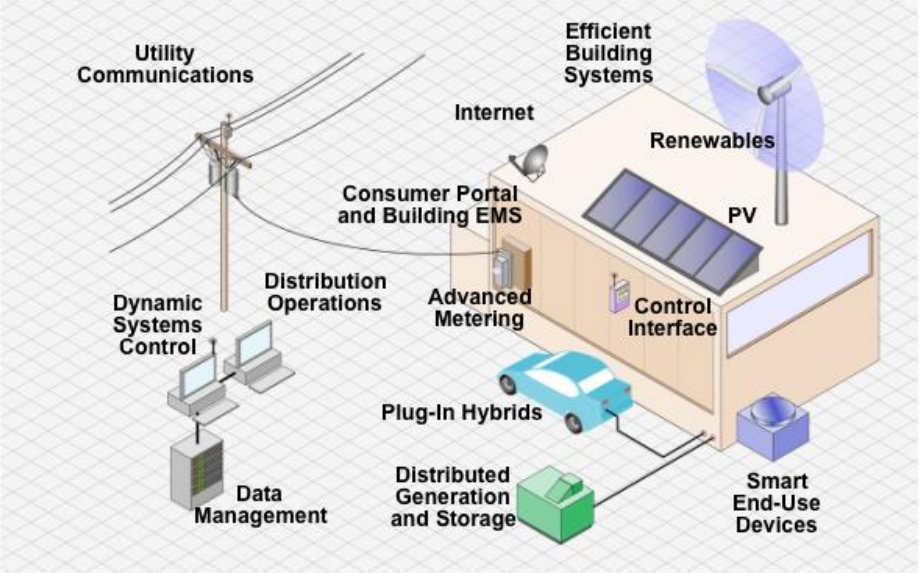

Fig. 2. Smart grid home owner layout showing DERs.

How Cyber-Attack Occurs in DERs/Smart Power Grid?

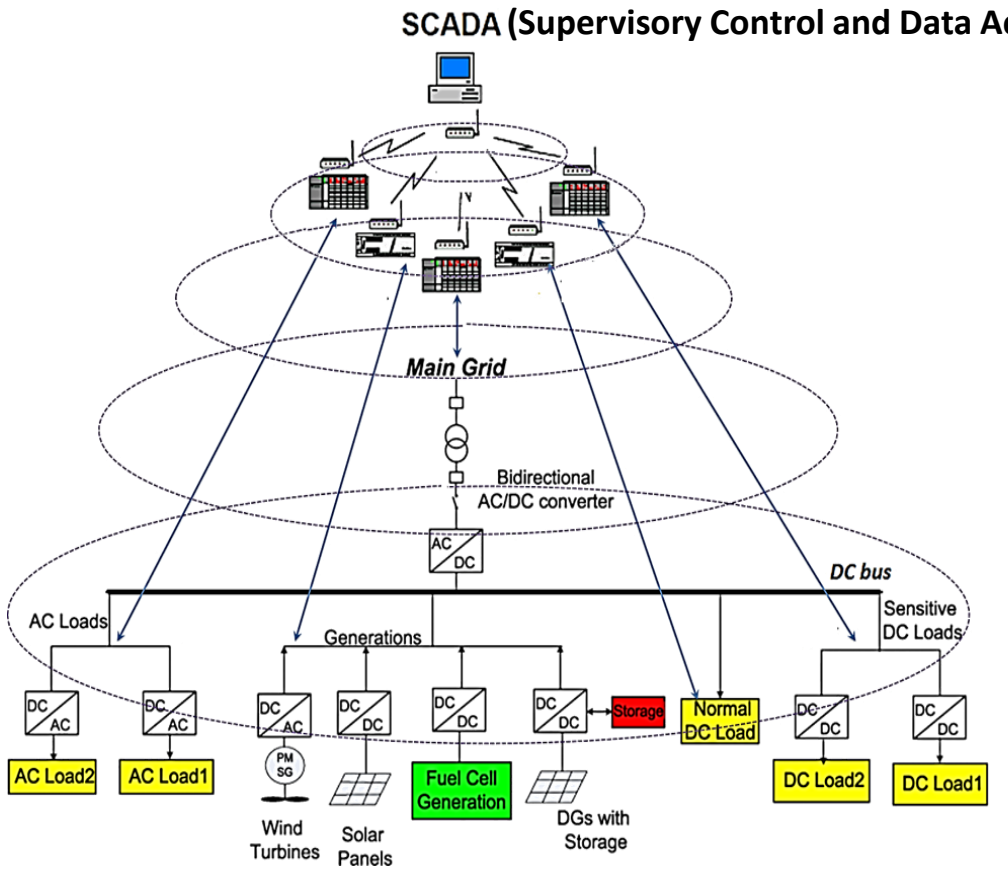

Fig. 3. DC microgrid system incorporated with the SCADA system.

What Consequences Cyber-Attacks Have on Power Grid?

Cyber-Attack incidents:

- Stuxnet (2010)
  - Targeted SCADA system and programmable logic controllers (PLCs)
  - Caused Damage to the Iran's Nuclear system
- Night Dragon Attack (2011)
  - Targeted SCADA system
  - Affected 71 organizations in China
- Ransomware Attack (June 2017)
  - Targeted many organizations including Ukraine's Electricity Company
  - 73 MWh of electricity was not supplied

- Aurora Attack: An Aurora attack is a type of malicious command injection attack which opens and closes critical circuit breakers without authorization.

- Crash Override Attack: This attack can malfunction circuit breakers and ultimately destroys the power grid.

"Stuxnet worm hits Iran nuclear plant staff computers". BBC News. 26 September 2010.
"'Night Dragon' Attacks From China Strike Energy Companies". *PCWorld*. 10-02-2016.
Kim Zetter (03-03-2018). "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid". Wired.

National Security Agency (NSA) Funded Project

Project title: Cybersecurity Education for Critical Infrastructure Protection (in Community Development) Through Regional Coalition.

PI: Dr. Dipankar Dasgupta.

Smart Grid Security Workshop-Part of NSA Project

 # A workshop on smart grid security was held at the FedEx Institute of Technology building of the University of Memphis on March 25, 2022. There were total 84 registrants (38 in-person and 46 virtual) at the workshop.

 # Three external/invited and two local speakers lectured on various topics of the smart grid security at the workshop. The details about the speakers and their talks are given below.

 # External/Invited Speakers:

1) Dr. Stacy Prowell, Distinguished Researcher, Oak Ridge National Laboratory.
Title of the talk: Cautious Optimism.

2) Mr. Chip Harris-Cybersecurity Administrator at DMI.INC.
Title of the talk: Cyber Security for Smart Grid Technology for I.T and O.T.

3) Dr. Sandip Roy, Program Director, Computer and Network Systems, National Science Foundation (NSF).
Title of the talk: Implications-Focused Cybersecurity Research for Power and Transportation Systems.

Local Speakers:

1) **Dr. Mohd Hasan Ali, Associate Professor, Electrical & Computer Engineering.**

Title of the Talk: Cyber-Security Issues and Solutions to Distributed Energy Resources.

2) **Mr. Nathan Farrar, Undergraduate Student, Electrical & Computer Engineering.**

Title of the Talk: Impact Assessment of Cyberattacks on Inverter-Based Microgrids.

 # The workshop was a great success. We hope to organize another workshop around October, 2022.