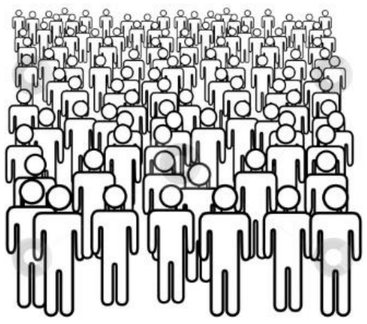
Smart Grid Cyber Security: Research & Challenges

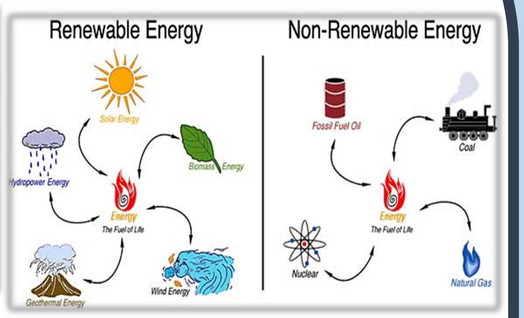
University of Victoria

PANDA Parallel, Networking and Distributed Applications

Maryam Tanha (tanha@uvic.ca)

Introduction





Key Challenges of the Legacy Power Grid [1]

- ❑ Population explosion & increase in demand for energy use
- ❑ Green house effect & climate change
- ❑ Legacy power grid has become larger & more complex

What Is Smart Grid?

Information & Communication Technology (ICT) + Conventional Power Grid

Virtues of Smart Grid [1]

- Ease of management & control
- Bidirectional information flow & active participation of consumers (Demand Response)
- Distributed electricity generation – (Integrating Distributed Energy Resources)
- Self-healing & self-reconfiguration (in case of power outage)
- Economical benefits & high overall efficiency
- Environmental-friendly

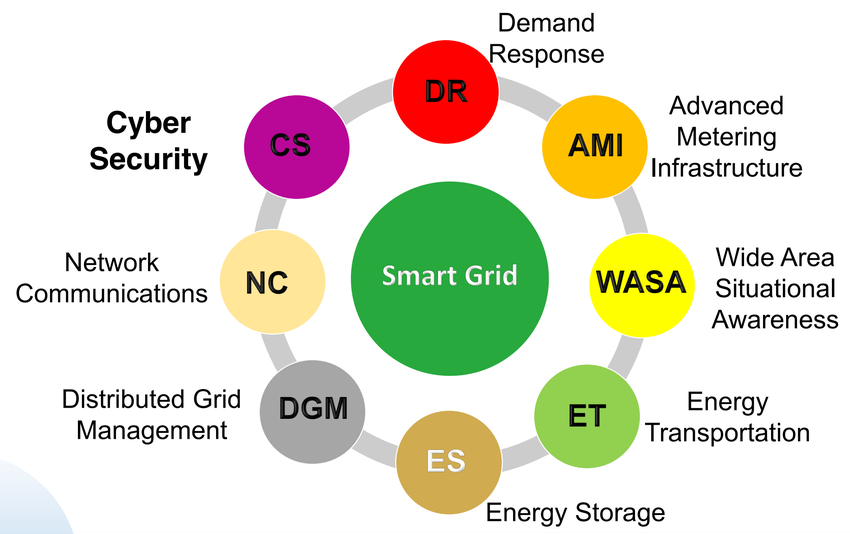
Well-known Guides Standards for Smart Grid:

- **NIST** (National Institute of Standard and Technology)
- **IEEE Std 2030**

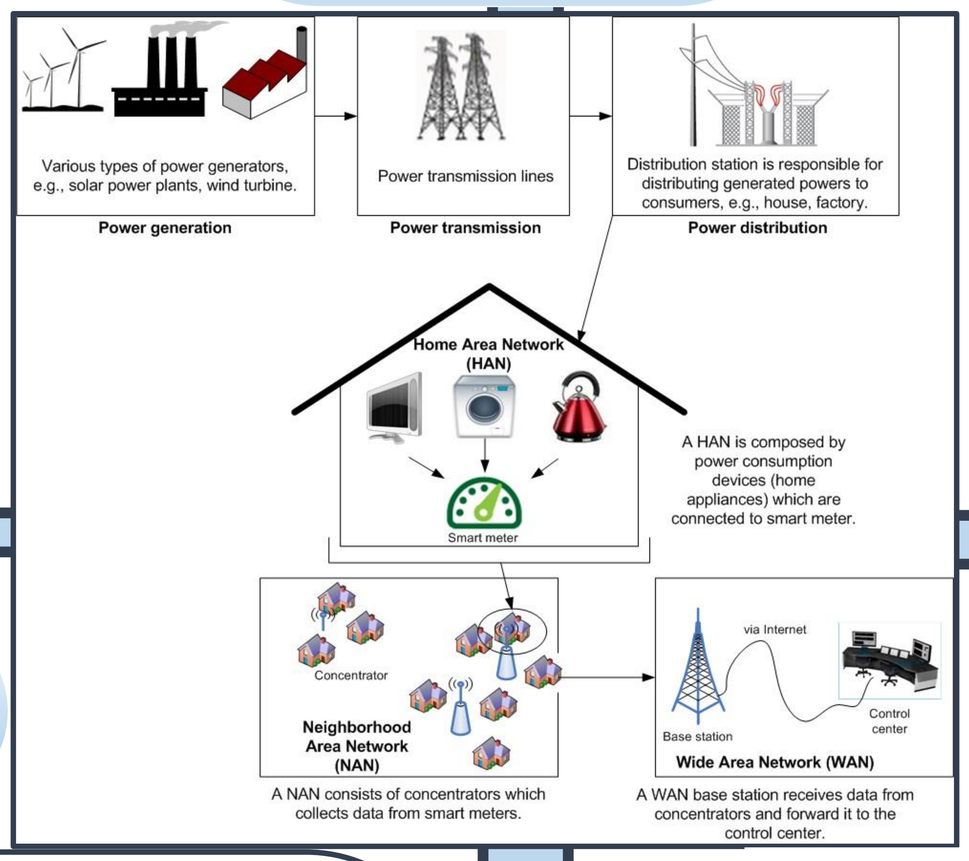
Smart Grid Cyber Security

Importance of Cyber Security for Smart Grid

Security is one of the eight priority areas & features identified in **NIST** roadmap for Smart Grid [2].



Smart Grid Communication Infrastructure



Security Challenges of Smart Grid

- Large-scale operation
- Heterogeneity
- Complexity
- Two-way Communication between utilities & consumers
- Widespread social & economic impacts

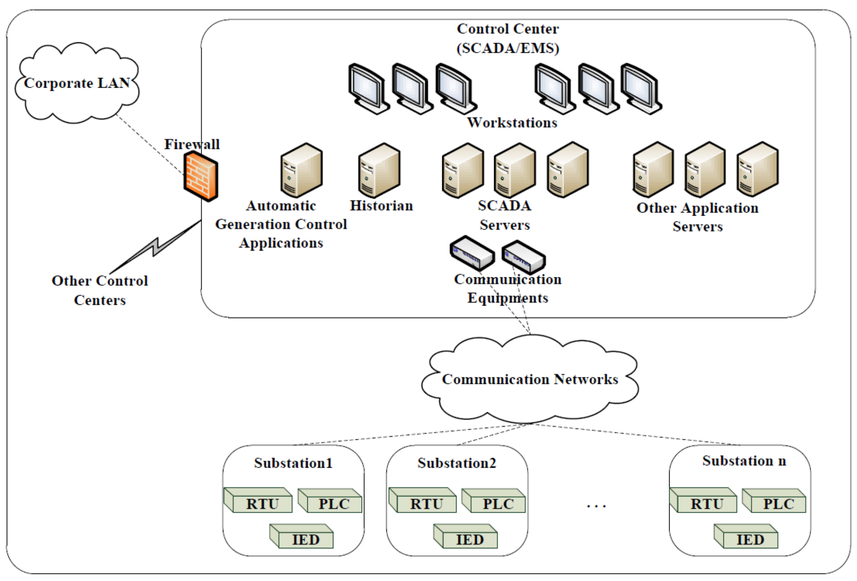
Security Objectives of Smart Grid in Order of Importance [3]

1. Availability & continuity of service
2. Integrity
3. Confidentiality

Security of Smart Grid Control Centers

Control Centers in Smart Grid

- **Control centers are considered as the brain of Smart Grid** (data analysis & decision making). SCADA systems are the main component of control centers. Malfunction or failure of these systems may result in widespread and devastating effects (e.g., power outage, cascading blackouts) on industry, economy and people's daily life.
- The main issue is **ensuring a high level of availability**.

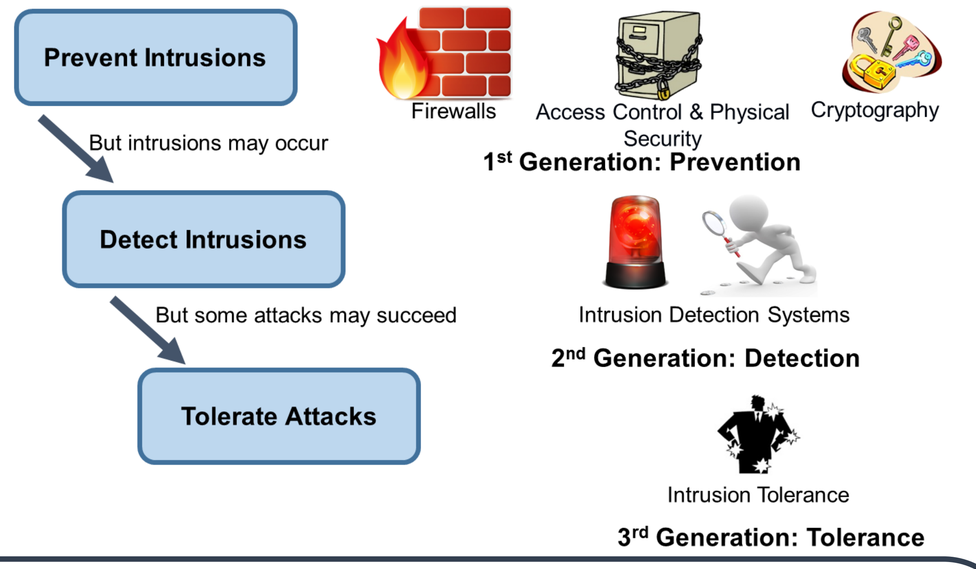


Other Cyber Security Concerns in Smart Grid

- **Integrity of transmitted messages and data**: Modification or manipulation of the control commands sent from SCADA to substations may result in safety issues or widespread power outage. Violating integrity of meter data may result in financial loss for utilities (may lead to generating incorrect bills).
- **Privacy& Confidentiality**: Smart meter readings may reveal the lifestyle and habits of the specific household. Disclosure of such information may lead to misuse by house robbers or advertisers of certain products.

A Promising Solution

Intrusion Tolerance for Smart Grid [4]



Summary

Smart grid cyber security is a hot research area due to the fact that smart grid is a critical infrastructure which is tightly coupled with ICT. The security incidents in cyber domain may affect the physical world and may subsequently lead to **nationwide and disastrous consequences such as cascaded failures and massive blackouts**.

Significance of using **intrusion tolerance** as a security approach to enhance the cyber security of smart grid control centers has been highlighted. Intrusion tolerance serves as a promising security approach to compensate for the shortcomings of classical security mechanisms as well as it ensures availability as the main security property in smart grid.

References

1. C.-H. Lo and N. Ansari, "The Progressive Smart Grid System from Both Power and Communications Aspects," IEEE *Commun. Surv. Tutorials*, vol. 14, no. 3, pp. 799–821, 2012.
2. "NIST Framework and Roadmap for Smart Grid Interoperability Standards , Release 2.0," 2012.
3. J. Liu, Y. Xiao, S. Member, S. Li, W. Liang, and C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," *IEEE Commun. Surv. Tutorials*, no. 99, pp. 1–17, 2012.
4. S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-Physical System Security for the Electric Power Grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, 2012.