Cyber Resilience Metrics for Bulk Power Systems

Sachin Shetty (Old Dominion University), Bheshaj Krishnappa (ReliabilityFirst) and David Nicol (University of Illinois)

Introduction

The North American Bulk Power System is a complex technological network, and its cyber-physical interconnectivity allows for long-distance power transmission but presents a "surface" for cyber-attacks. The BPS is comprised of substations, control centers, energy management systems, multiple communication technologies, supervisory control, etc. The critical operation of BPS is to provide monitoring, protection and control based on information gathered from field units and decision making and control at multiple control centers. The components in the BPS that are vulnerable to cyber-attacks include, substations, control centers, communication links and networks. The cyber-attacks can manifest as, spear phishing, denial of service, man-in-the middle, timing, replay, integrity. There is a need to develop cyber resilience metrics for BPS to provide quantitative insights into ability of security controls to ensure operational resilience and development of cost-effective mitigation plan.

The availability of cyber resilience metrics will facilitate effective risk management decision making in BPS. Specifically, asset owners will be able to prioritize corrective actions through identification of resilient topologies/configurations, identification of critical vulnerabilities which need to be mitigated, cost-effective security controls, etc. In addition, the availability of cyber resilience metrics will motivate operators to continually assess their response to cyber threats. However, existing cyber resilient metrics to achieve these desired objectives for BPS are inadequate. This brief describes the need for cyber resilience metrics for BPS and techniques to develop the metrics.

Motivation

There have been efforts on developing models for power grid structural resilience in the presence of cascading failures. According to the Energy Sector Cybersecurity Capability Maturity Model [1], there is a need to develop techniques to reduce risks and to increase operational grid resilience, commensurate with the risk to critical infrastructure and organizational objectives. However, resilience metrics for BPS substation networks in the presence of cyber threats do not exist.

Efforts on understanding and quantifying resilience in the power grid primarily focus on local and cascading failures which are caused due to physical faults [2-5]. Specifically, researchers have analyzed the power grid's structural resilience to deliberate physical attacks to substations, control centers, substation/transmission lines, and communication systems. The physical attacks caused due to vandalism or theft result in faults or failures in the generators and/or transmission lines and any cascading effects can be traced back to the original fault reliably. Physical attacks in contrast to cyber-attacks are deterministic in nature because attackers are usually aware of the system units to target. Due to the selective nature of the physical attacks, the impact felt on the immediate victims or potential of cascading events are not similar to cyber-attacks. The physical attacks are also characterized by temporal selectivity. The timing of physical attack is chosen to maximize the impacts. In contrast, the timing of cyber-attacks cannot be always guaranteed to be precise. The restoration process after a successful physical attack versus cyber-attack may have different timelines.

Resilience metrics have been developed for critical infrastructures. [6-10]. Tierney et al. [6], proposed a R4 framework for disaster resilience. The R4 framework comprises of Robustness (Ability of systems to function under degraded performance), Redundancy (identification of substitute elements that satisfy functional requirements in event of significant performance degradation), Resourcefulness (initiate solutions by identifying resources based on prioritization of problems), and Rapidity (ability to restore functionality in timely fashion). However, these models have not focused on cyber resilience of bulk power systems.

Approach

The Cyber Resilient Energy Delivery Consortium (CREDC) funded by the U.S. Department of Energy is advancing security and resiliency in the cyber support infrastructure as a key enabler of Energy Delivery System (EDS) resiliency [11]. The objectives are achieved through collaborative research activities between universities and industry. The cyber resilience metrics for BPS is a research activity under the theme of cyber monitoring and metrics.

A framework for developing cyber resilience metrics for BPS should not build on top of models for physical attacks, but differentiate from these by considering the additional complexity introduced by the cyber aspects of modern BPS. The availability of resilience metrics will aid in identifying the most vulnerable devices and the impact on operation of the power grid and security controls which are cost-effective and provide appreciable tradeoff between protection and performance

Weighted graph models have been developed for quantifying resilience of physical attacks. The modeling of exploitability and impact of cyber-attacks needs to be integrated in the weighted graph model. The model should be also integrated with varying degrees of exploitability and impact of cyber-attacks, diversity of network topology, configuration and vendor products and study influence of critical nodes, attack timing, stepping stones, pivot points, and attack launch location. The cyber resilience metrics should be based on the four elements (robustness, rapidity, resourcefulness and redundancy) of the R4 framework. The models for each of the aforementioned properties for the networks interconnecting sub stations and control center should be developed. A multi-level directed acyclic graph is a good model to use as it incorporates security domains, security policies and protocols. Fig. 1 illustrates a security architecture schema proposed by NIST for industrial control systems. This architecture is applicable to SCADA systems in general and BPS infrastructures in particular due to the similarities in inter-connectivity between corporate, control system and substation networks. Fig.2 illustrates the multi-layered Directed Acyclic Graph (DAG) to model interactions between the devices in the cyber infrastructure depicted in Fig. 1. In addition, the graph model also incorporates channel vulnerability paths to assess the exploitability of cyber-attack and the impact on operational resilience. Network and system configuration parameters, such as firewall rules, network paths, node recovery time, backup resources available, etc., will impact the computation of robustness, redundancy, resourcefulness and rapidity properties. There is need to provide relationship between the network/system configuration parameters and resilience which will be benefit the BPS stakeholders.

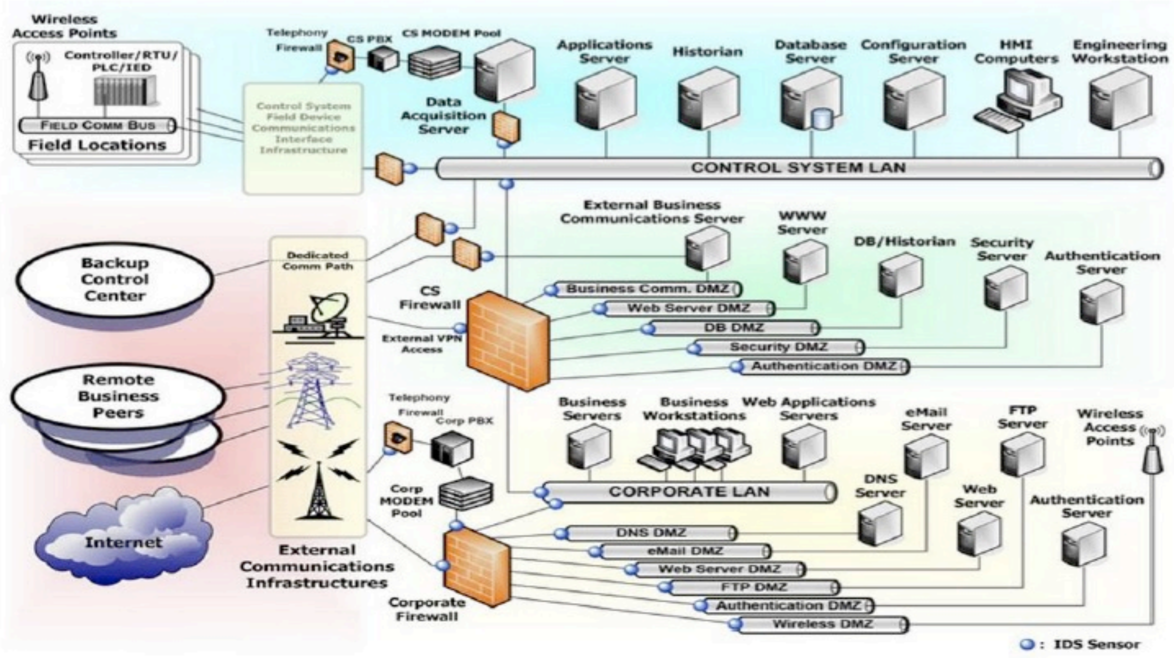

Fig. 1. CSSP Recommended Defense-in-Depth Architecture [12]

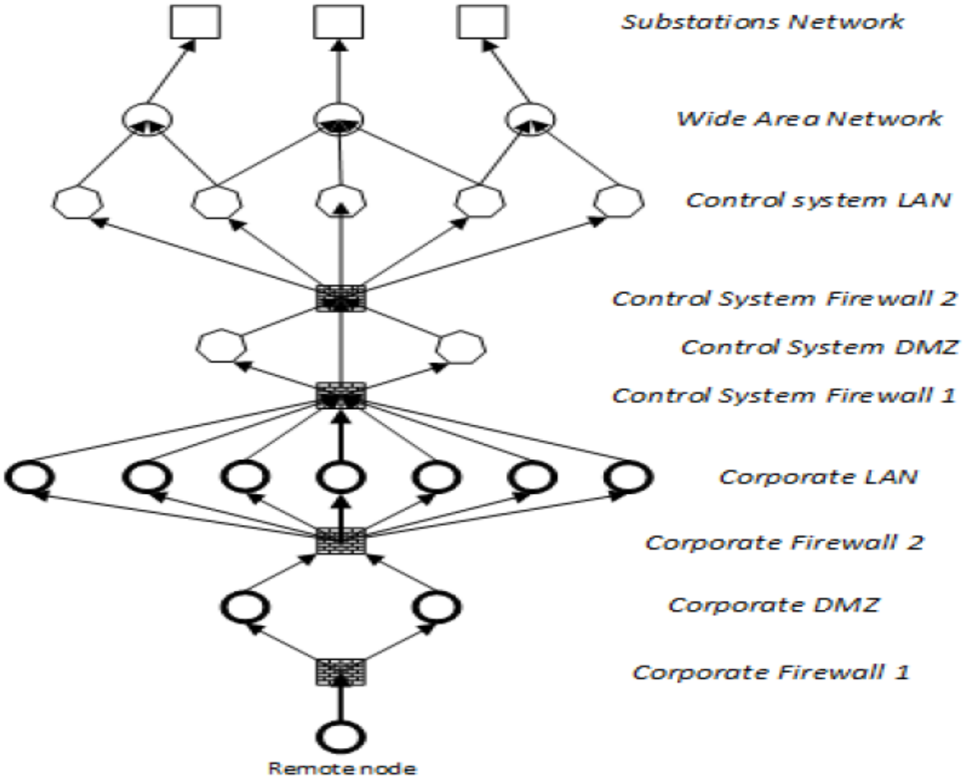

Fig. 2. Bulk Power Systems infrastructure modeled as multi-layered DAG

Bibliography:

1. Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), https://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf
2. Modeling cascading failures in the North American power grid, R. Kinney, P. Crucitti, R. Albert, and V. Latora, Eur. Phys. B, 2005
3. Y. Zhu, J. Yan, Y. Tang, Y. L. Sun and H. He, "Resilience Analysis of Power Grids Under the Sequential Attack," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2340-2354, Dec. 2014.
4. Y. Zhu, J. Yan, Y. Sun and H. He, "Revealing Cascading Failure Vulnerability in Power Grids Using Risk-Graph," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3274-3284, Dec. 2014.
5. J. Yan, Y. Tang, Bo Tang, H. He and Y. Sun, "Power grid resilience against false data injection attacks," *2016 IEEE Power and Energy Society General Meeting (PESGM)*, Boston, MA, USA, 2016, pp. 1-5.
6. Tierney, Kathleen, and Michel Bruneau, 2007, "Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction," TR News, May, 2007, pp. 14 – 17
7. Ganin, A.A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J.M., Kott, A., Mangoubi, R. & Linkov, I. (2016). Operational Resilience: Concepts, Design and Analysis. Scientific Reports, 6: 19540
8. I. Linkov et al., "Resilience Metrics for Cyber Systems," Environment Systems & Decisions, vol. 33, no. 4, 2013
9. Thorisson, H., Lambert, J., Cardenas, J., and Linkov, I. (2016). "Resilience Analytics with Application to Power Grid of a Developing Region." Risk Analysis,
10. P.E. Roege, Z.A. Collier, J. Mancillas, J.A. McDonagh, I. Linkov, Metrics for energy resilience, Energy Policy., 72 (2014) 249-56
11. NIST 800-82, Guide to Industrial Control System Security.
12. Cyber Resilient Energy Delivery Consortium, https://cred-c.org/

Sachin Shetty is an Associate Professor in the Virginia Modeling, Analysis and Simulation Center at Old Dominion University (ODU). His research interests lie at the intersection of computer networking, network security and machine learning. He has authored and coauthored over 125 research articles in journals and conference proceedings and two books. Email-sshetty@odu.edu

Bheshaj Krishnappa is a Principal in the Risk Analysis and Mitigation department at ReliabilityFirst, a regional regulator overseeing electric service reliability across 13 U.S. States and Washington D.C. Previously, he worked as Critical Infrastructure Protection Compliance Auditor. He was instrumental in leading several small to large scale IT and security projects that have enabled businesses to transform and be resilient in delivering their mission.

David M. Nicol is the Franklin W. Woeltge Professor of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign, and Director of the Information Trust Institute (iti.illinois.edu). He is PI for two recently awarded national centers for infrastructure resilience: the DHS-funded Critical Infrastructure Reliance Institute (ciri.illinois.edu), and the DoE funded Cyber Resilient Energy Delivery Consortium (cred-c.org); he is also PI for the Boeing Trusted

Software Center, and the NSA-funded Science of Security lablet. His research interests include trust analysis of networks and software, analytic modeling, and parallelized discrete-event simulation, research which has led to the founding of startup company Network Perception, and election as Fellow of the IEEE and Fellow of the ACM.

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.