

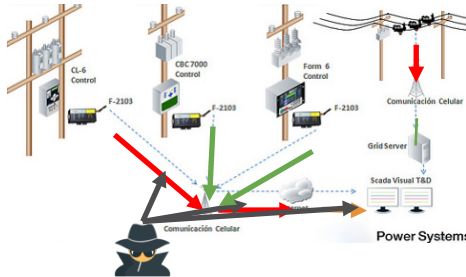
INTRODUCTION

Motivation:

Security metrics for assessing reliability and monitoring the risk to the cyber-physical power grid infrastructure are necessary in order to ascertain the impact of events such as cascading failures as well as identifying investments.

Goals of Security Metrics:

- Evaluating a portfolio of security configurations, controls, reliability of the operations in real-time
- Prioritizing critical assets
- Prioritizing efforts to secure critical assets
- Describing potential cyber-physical vulnerability



CHALLENGES

- Data Availability:** Lack of the interconnections information between cyber and electrical topologies (control devices e.g., relays).
- Scalability:** gathering and analyzing data in real-time.
- Prioritization:** Considering all threat factors and prioritizing operations for risk mitigation.

PROPOSED METRICS

An attack graph is a graph representation that captures potential attack paths leading to specific threats to a given system.

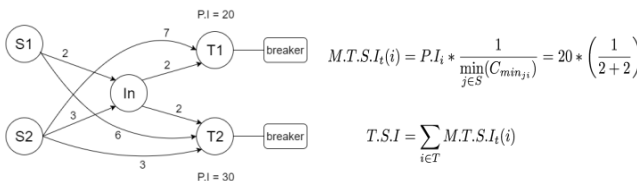


Figure 1. Attack Graph and Security Indexes Examples

Attack Cost (C): Cost of exploitations of series of vulnerability from source node to a desired target node. This measure evaluates the chance of a potential threat.

Attack Impacts: The physical impact (PI) of a cyber attack on the electrical network.

1. Target Nodes/Assets Metrics:

- M1: Min-Cost Target Node Security Index
- M2: Target Node Security Index

2. Stepping Stone Node Metrics:

- M3: Intermediate Node Min-Cost Betweenness Security Index
- M4: Intermediate Node Betweenness Security Index

3. Source Node Metrics:

- M5: Min-Cost Source Node Security Index
- M6: Source Node Security Index

4. Overall Security Metrics:

- M7: Total Security Index

ILLUSTRATION of CYBER-PHYSICAL VULNERABILITY

Q1: How do we determine critical assets from PHYSICAL perspective?

A1: N-1-1 simulations.

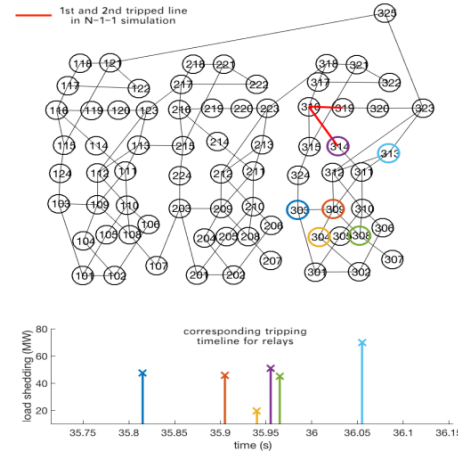


Figure 2. An example of N-1-1 simulation results for RTS-96

Q2: How we determine critical assets from CYBER perspective?

A2: Proposed Security Metrics.

| Description | Contingency | Load shed | Reach-ability Index | T.S.I |
|--------------|---|---|---------------------|---------|
| Line fault 1 | line 103-124 | 47.25MW load shedding (LS) | 0.8265 | 39.0521 |
| Line fault 2 | line 303-324 | 47.25MW LS | 0.7624 | 36.0234 |
| Line fault 3 | line 207-208 | 45MW LS | 0.8265 | 37.1925 |
| Line fault 4 | line 307-308 | 1 generator and 1 load partitioned | 0.8265 | 37.1925 |
| Line combo 1 | line 119-120, 120-123, 118-121 | 0 | 1.5688 | 0 |
| Line combo 2 | line 108-110, 207-208, 307-308, 115-121, 215-221, 315-321 | 90MW LS; 2 generators and 2 loads partitioned | 4.2357 | 381.213 |

Table 1. Prioritization of contingencies by applying security metrics for RTS-96

LIMITATIONS

- We currently have access to synthetic data. Real datasets are not available or frequently do not include all possible cyber-physical attack side-effect information.
- The security indexes values themselves do not have inherent meaning and just help us to prioritize cyber-security tasks in a specific system.

FUTURE WORKS

- Create an automatic approach to implementing the cyber-physical model for a larger utility case.
- Quantify the security metrics.
- Find an industry partner to validate the metrics against realistic scenarios.

REFERENCES

- Patapanchala, P., Huo, C., Bobba, R., Cotilla-Sanchez, E. (2016). Exploring Security Metrics for Electric Grid Infrastructures Leveraging Attack Graphs. IEEE Conference on Technologies for Sustainability (SusTech 2016).
- Weaver, G. A., Davis, K., Davis, M., Rogers, E. J., Bobba, R. B., Zonouz, S. A., Berthier, R., Sauer, P. W., Nicol, D. M. (2016). Cyber-Physical Models for Power Grid Security Analysis: 8-Substation Case. IEEE International Conference on Smart Grid Communications (SmartGridComm), Sydney, Australia, 2016, pp. 140-146.
- Kate R. Davis, Charles M. Davis, Saman A. Zonouz, Rakesh B. Bobba, Robin Berthier, Luis Garcia, and Pete W. Sauer, "A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures," IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2464-2475, Sep. 2015.