Attack Graph Based Metrics for Identifying Critical Cyber Assets in Electric Grid Infrastructure

Arezoo Rajabi, Chen Huo, Panini Sai Patapanchala, Eduardo Cotilla-Sanchez, Rakesh B. Bobba

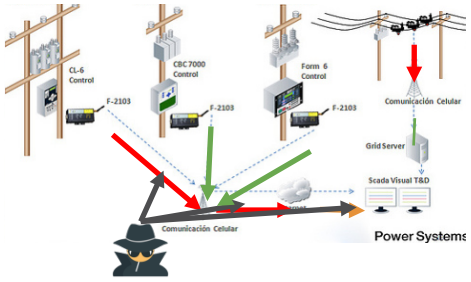
INTRODUCTION

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.

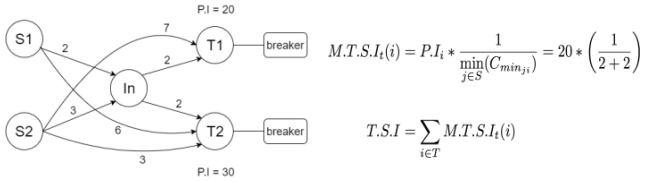


Figure 1. Attack Graph and Security Indexes Examples

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.

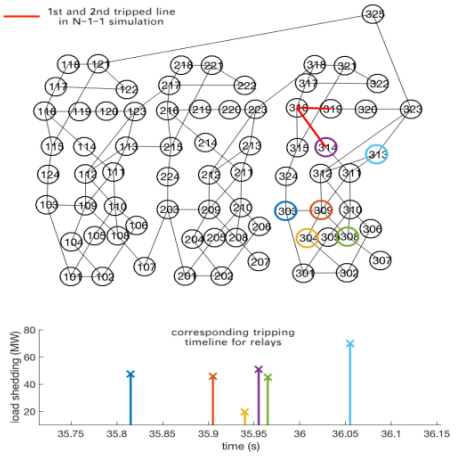


Figure 2. An example of N-1-1 simulation results fo RTS-96

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 1 generator and 1 load partitioned	0.8265	37.1925
Line fault 4	line 307-308	45MW LS 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.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY

Attack Graph Based Metrics for Identifying Critical Cyber Assets in Electric Grid Infrastructure

Arezoo Rajabi, Chen Huo, Panini Sai Patapanchala, Eduardo Cotilla-Sanchez, Rakesh B. Bobba

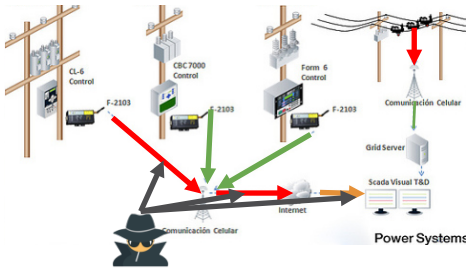
INTRODUCTION

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:

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

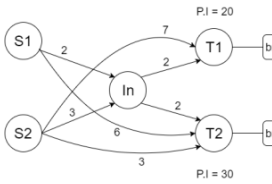


CHALLENGES

- **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.

DETERMINING VULNERABILITY FROM CYBER SYSTEM

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



$$M.T.S.I_t(i) = P.I_i * \frac{1}{\min_{j \in S}(C_{min_{ji}})} = 20 * \left(\frac{1}{2+2}\right)$$

$$T.S.I = \sum_{i \in T} M.T.S.I_t(i)$$

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.

Physical Impact *(PI)*: The amount of load shedding.

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

DETERMINING VULNERABILITY FROM PHYSICAL SYSTEM

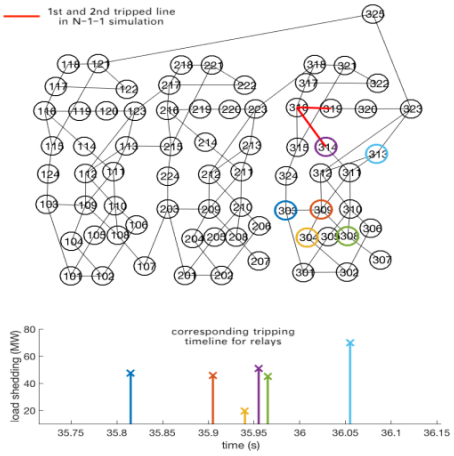


Figure 2. An example of N-1-1 simulation results fo RTS-96

1. tripped lines are N-1 secure
1. showing potential vulnerability for the physical system
1. automatic deployment for any size of cases
1. prioritizing critical assets based on resulted load shedding amount

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.
- Evaluating a portfolio of security configurations, controls, reliability of the operations in real-time

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.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY

Attack Graph Based Metrics for Identifying Critical Cyber Assets in Electric Grid Infrastructure

Arezoo Rajabi, Chen Huo, Panini Sai Patapanchala, Eduardo Cotilla-Sanchez, Rakesh B. Bobba

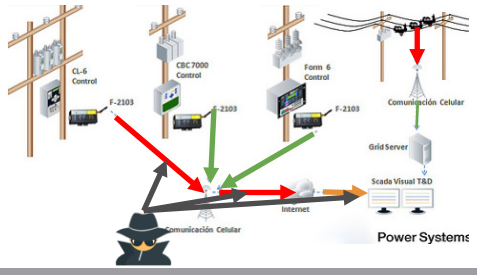
INTRODUCTION

Motivation:

- An attack on the US power grid has an estimated cost of $1 trillion to the US economy
- Cyber attack on Ukraine power grid left 225000 users without power

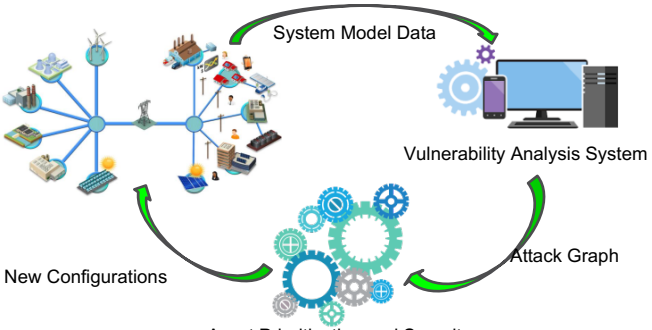
Goals of Security Metrics:

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.



RESEARCH VISION

RESEARCH ROADMAP



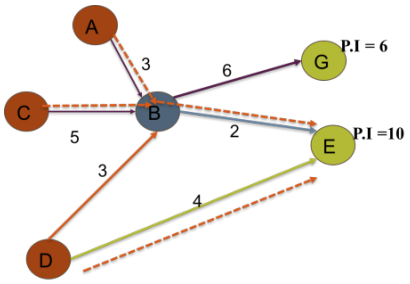


Figure 1. Attack Graph. Dashed lines show vulnerabilities series from source nodes to target node E.

We aim to detect series of vulnerabilities which can lead a system to be broken.

- We demonstrate vulnerabilities and their dependencies
- We utilize data from both cyber and physical data to have more accurate estimate of vulnerabilities
- We prioritize the actions for vulnerability mitigation

CYBER-PHYSICAL SECURITY METRICS

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

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.

Physical Impact *(PI)*: The amount of load shedding.

1. **Target Nodes/Assets Metrics**
2. **Stepping Stone Node Metrics**
3. **Source Node Metrics**
4. **Overall Security Metrics**

VULNERABILITY MEASUREMENTS ON SMALL SYSTEM

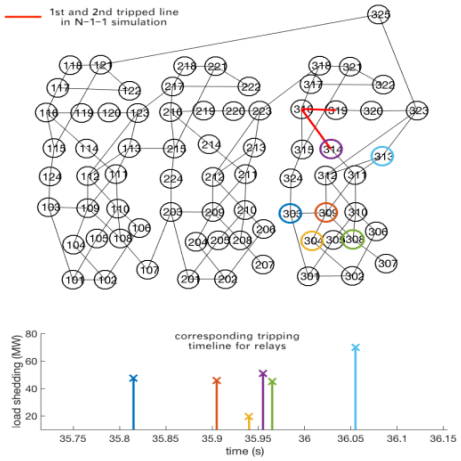


Figure 2. An example of N-1-1 simulation results fo RTS-96

1. tripped lines are N-1 secure
2. showing potential vulnerability for the physical system
3. automatic deployment for any size of cases
4. prioritizing critical assets based on resulted load shedding amount

POTENTIAL IMPACTS

System Security Benefits:

- Understanding systemic risks
- Prioritizing critical cyber assets and security investments
- Decision Support for security configuration and security control decisions

Business Benefits:

- Increasing attack cost by decreasing vulnerabilities in systems
- Reducing outage by detecting valuable assets and protecting them

COLLABORATION OPPORTUNITIES

Cooperation, support and guidance from industry partners in the following areas would benefit this research activity:

- **Datasets**: To evaluate our methods we need to have real dataset from current systems
- **Feedbacks**: Discussion about the critical assets, industry priorities in different situations can help us to improve our metrics
- Contact: rakesh.booba@oregonstate.edu, ecs@oregonstate.edu
- Activity webpage: https://cred-c.org/researchactivity/ ???

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY

Attack Graph Based Metrics for Identifying Critical Cyber Assets in Electric Grid Infrastructure

Arezoo Rajabi, Chen Huo, Panini Sai Patapanchala, Eduardo Cotilla-Sanchez, Rakesh B. Bobba

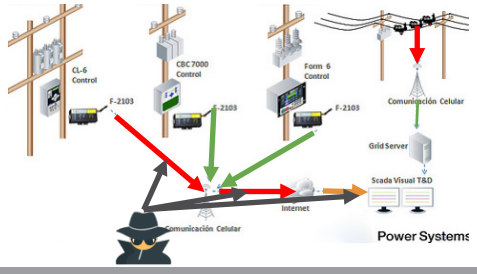
INTRODUCTION

Motivation:

- Attacks on energy delivery infrastructure have severe consequences
  - An attack on the US power grid could cost an estimated $1 trillion to the US economy
- Attacks on energy delivery infrastructure are real
  - Cyber attack on Ukraine distribution grids left 225000 users without power

Goals of Security Metrics:

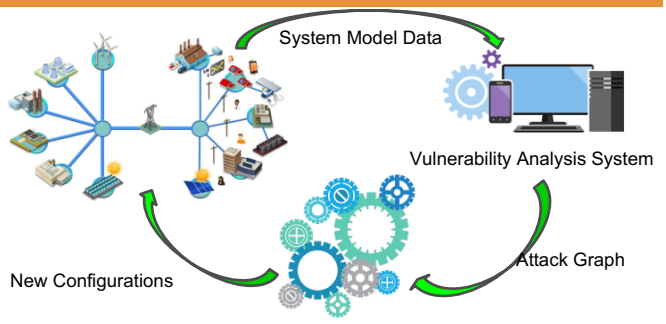
Security metrics for assessing reliability and monitoring the risk to the cyber-physical power grid infrastructure are necessary in order to ascertain the impact of cyber attacks and failures, as well as for identifying targeted cybersecurity investments.



RESEARCH VISION

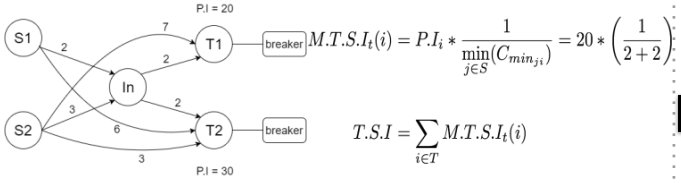
WE AIM TO DEVELOP ANALYSIS TECHNIQUES AND METRICS FOR IMPROVING CYBER-PHYSICAL SITUATIONAL AWARENESS IN EDS SYSTEMS AND FOR PROVIDE DECISION SUPPORT FOR CYBERSECURITY INVESTMENTS

RESEARCH ROADMAP



Asset Prioritization and Security Configuration

CYBER-PHYSICAL SECURITY METRICS



$$M.T.S.I_t(i) = P.I_i * \frac{1}{\min_{j \in S}(C_{min_{ji}})} = 20 * \left(\frac{1}{2+2}\right)$$

$$T.S.I = \sum_{i \in T} M.T.S.I_t(i)$$

Figure 1. Attack Graph and Security Indexes Examples

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

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.

Physical Impact *(PI)*: The amount of load shedding.

1. **Target Nodes/Assets Metrics**
2. **Stepping Stone Node Metrics**
3. **Source Node Metrics**
4. **Overall Security Metrics**

CASCADING FAULTS AS PHYSICAL IMPACT

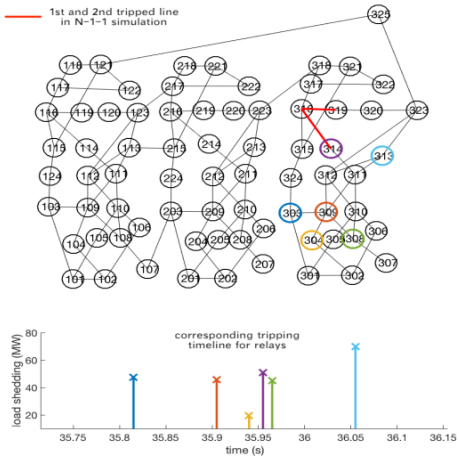
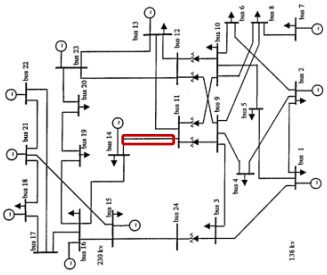


Figure 2. An example of N-1-1 simulation results fo RTS-96

1. Tripped lines are N-1 secure
2. Uncovers potential vulnerability of the physical system
3. Prioritizing critical cyber assets based on resulted load shedding amount



POTENTIAL IMPACTS

System Security Benefits:

- Understanding systemic risks
- Prioritizing critical cyber assets and security investments
- Decision support for security configuration and security control decisions

Business Benefits:

- Improved cyber risk profile and reduced cyber risk
- Improved system reliability

COLLABORATION OPPORTUNITIES

Cooperation, support and guidance from industry partners in the following areas would benefit this research activity:

- **Datasets**: To evaluate our methods we need to have real dataset from current systems
- **Feedbacks**: Discussion about the critical assets, industry priorities in different situations can help us to improve our metrics
- Contact: rakesh.booba@oregonstate.edu, ecs@oregonstate.edu
- Activity webpage: https://cred-c.org/researchactivity/rtsarisk

REFERENCES

- P. S. Patapanchala, Chen Huo, R. B. Bobba and E. Cotilla-Sanchez, "**Exploring security metrics for electric grid infrastructures leveraging attack graphs**," *2016 IEEE Conference on Technologies for Sustainability (SusTech)*, Phoenix, AZ, 2016..
- K. R. Davis, R. Berthier, S. A. Zonouz, G. Weaver, R. Bobba, E. Rogers, P. W. Sauer, and D. M. Nicol, "***Cyber-Physical Security Assessment (CyPSA) for Electric Power Systems,***"The Bridge, vol. 112, no. 2, May 2016
- Davis, K.R.; Davis, C.M.; Zonouz, S.; Bobba, R.B.; Berthier, R.; Garcia, L.; Sauer, P.W., "**A Cyber-Physical Modeling and Assessment Framework for Power Grid Infrastructures**," *Smart Grid, IEEE Transactions on* ,vol.6, no.5, Sept. 2015

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY