Module 6

Grid Security

How did the yesterday's definition differ from tomorrow's?

Chee-Wooi Ten

Arizona State University

Module 6.3

Redefined security

Let’s revisiting the root cause of problem and formulate cyber-physical system security.

Arizona State University

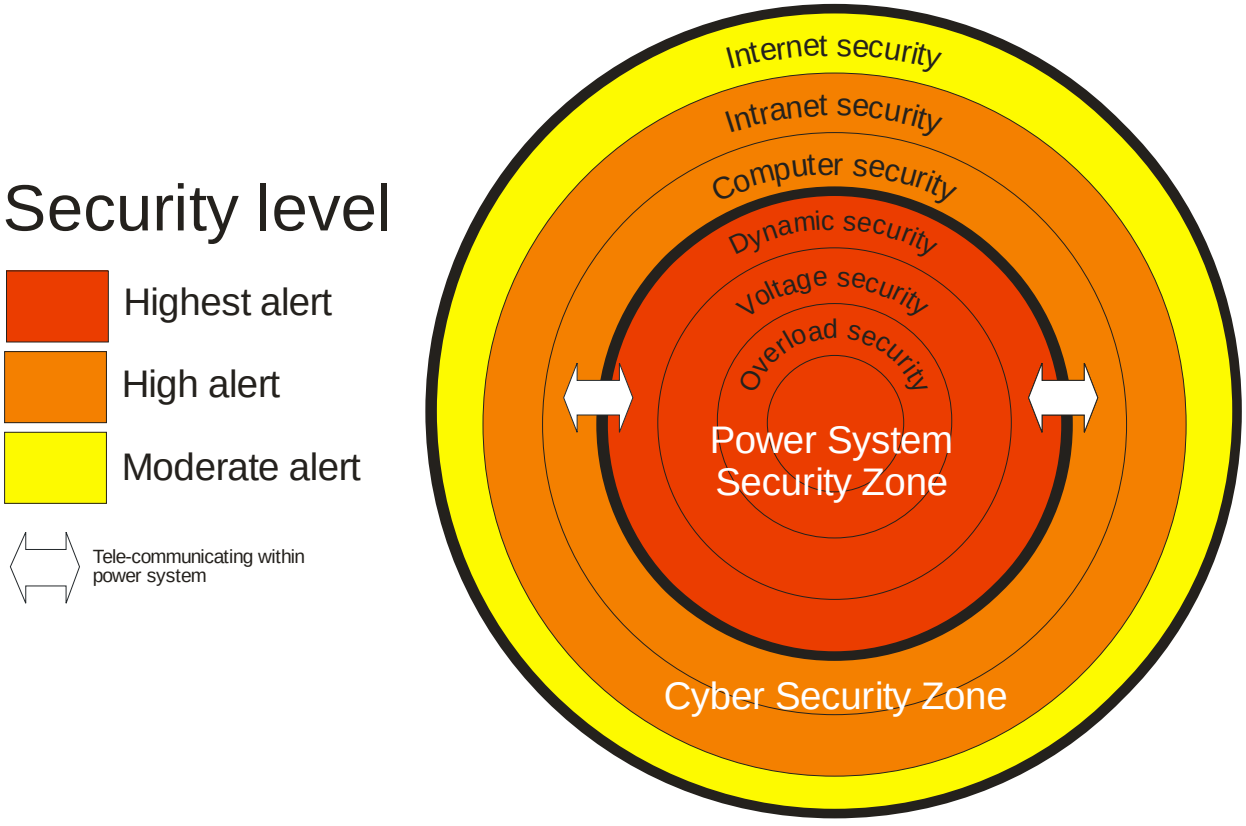
Redefined Security

1. Anticipating the extreme scenarios
2. Emerging cyberthreats and electronic intrusion path
3. S-1 contingency
4. M-k contingency and anomaly detection expansion
5. Sum S-k contingencies (without incurring overlead)
6. Sum S-k contingencies (with incurring overload)

IP-Based Distributed SCADA

- Current trend in the development of distributed control centers
- Do not depend on fixed dedicated communication from RTUs to Control Center
- Standard protocol enables the use of heterogeneous components
- Speed vs. Cybersecurity

Onion of multiple securities…



Comparisons of Security Standards

	BS7799	ISO/IEC 17799	ISA TR 99.00.02	AGA12	21 Steps	NERC 1200
Security Definition	Ref. ISO 17799	Own	Own	Own?	Cyber	Cyber
Confidentiality		Yes	Yes	Yes	Yes	Yes
Integrity		Yes	Partly	Partly	Partly	Partly
Availability		Yes	Partly	Partly	Partly	Partly
Scope						
Type of Organization	Any	Any	Any	Any	Any	Power Entity
Type of System to Protect	General IT	General IT	SCADA Communications	SCADA	SCADA	Critical Cyber Systems
Risk Assessment	Important	Important	Important	Important	Important	Important
Methodology Guidance	No	No	Some	Some	No	No
Security Policies						
Guidelines	No	Yes	Yes	Yes	No	No
Examples	No	Yes	Yes	Yes	No	No
Security Management						
System Guidance	Yes	No	Yes	Yes	No	No

A. Torkilseng, and G. Ericsson, “Some guidelines for developing a framework for managing cybersecurity for an electric power utility,” no. 228, October 2006, ELECTRA.

Escalating Cybersecurity Factors

1. Adoption with standardized technologies with known vulnerabilities
2. Connectivity of control systems to other networks
3. Constraints on the use of existing security technologies and practices
4. Insecure remote connections
5. Widespread availability of technical information about control systems

The Age of Information Technology

- Low cost of computer peripherals expand the computer communication systems into an Internet

- Evolution of communications
  - System performance
  - Interoperability
  - Reliability

- Drawback of the improvements
  - Security flaw may develop

- Significant efforts to identify and isolate from online system

Two Approaches of Cybersecurity Investments

1. NERC CIP Incentives Approach
2. NIST Framework Approach

Commission staff suggested that the 2 aforementioned approaches could be used independently or in combination.

NERC CIP Reliability Standards

1. CIP-002: BEES Cyber System Categorization
2. CIP-003-8: Security Management Control
3. CIP-004-6: Personnel and Training
4. CIP-005-6: Electronic Security Perimeter(s)
5. CIP-006-6: Physical Security of BES Cyber Systems
6. CIP-007-6: System Security Management
7. CIP-008-5: Incidence Reporting and Response Planning
8. CIP-009-6: Recovery Plans for BES Cyber Systems
9. CIP-010-3: Configuration Change Management and Vulnerability Assessments
10. CIP-011-2: Information Protection
11. CIP-012-1: Communication Between Control Centers
12. CIP-013-1: Supply Chain Risk Management

CIP Reliability Standards are objective-based **within a utility organization** and allow entities to choose compliance approaches best tailored to their systems

NIST Framework

1. The Cybersecurity Enhancement Act of 2014 updated the role of NIST
2. **Identify** and **develop** risk frameworks (risk assessment and management) for voluntary use by asset owners or operators
3. Must identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls
4. Voluntary consensus standards and industry best practices
5. Consist of 3 parts: (1) **Framework core**, (2) **Implementation tiers**, and (3) **Framework profiles**

NIST Framework (continued)

1. The **Framework Core** consists of 5 concurrent and continuous functions: (1) identify, (2) protect, (3) detect, (4) respond, and (5) recover. It is a set of cybersecurity activates.
2. **Implementation tiers** provides a mechanism for an organization to view and understand the characteristics of its approach to managing cybersecurity risk, which is designed to help in prioritizing and achieving cybersecurity objectives.
3. Elements of the Framework Core provide detailed guidance for developing individual **Framework Profiles**. This will help align and prioritize business requirements, risk tolerance, and resources.

NIST Framework Approach

1. **Automated and continuous monitoring**
2. Access control
3. Data protection
4. Incident response
5. Physical security of cyber systems

Emphasize on vulnerability assessment and mitigation!

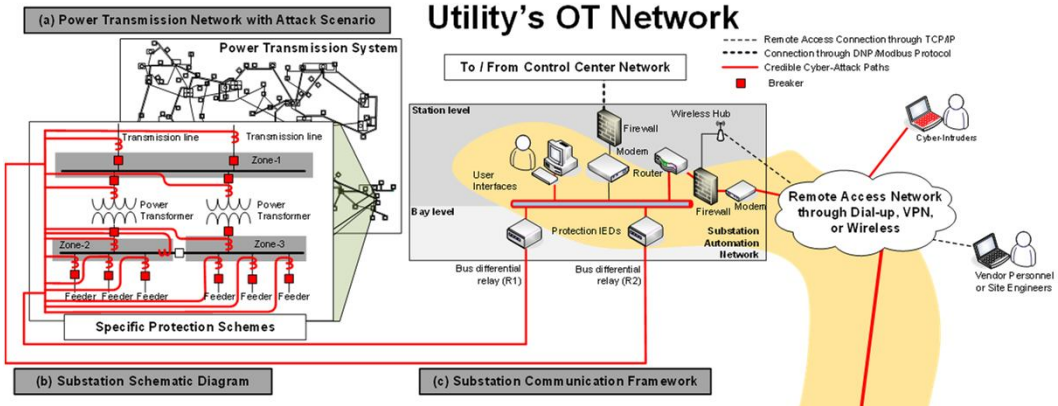
Warrant an incentive could include on item (1) for public utility to install a dynamic asset management program to improve its ability to quickly detect and address new or previously unknown equipment (threats to IT/OT networks) on its network.

Implementations (1) to dynamic file analysis program (sandbox), (2) of a process to scan inventory of hardware and software across IT/OT networks (identify, block, log, and report unauthorized access)

Need for Reform on **Supply Chain Security**

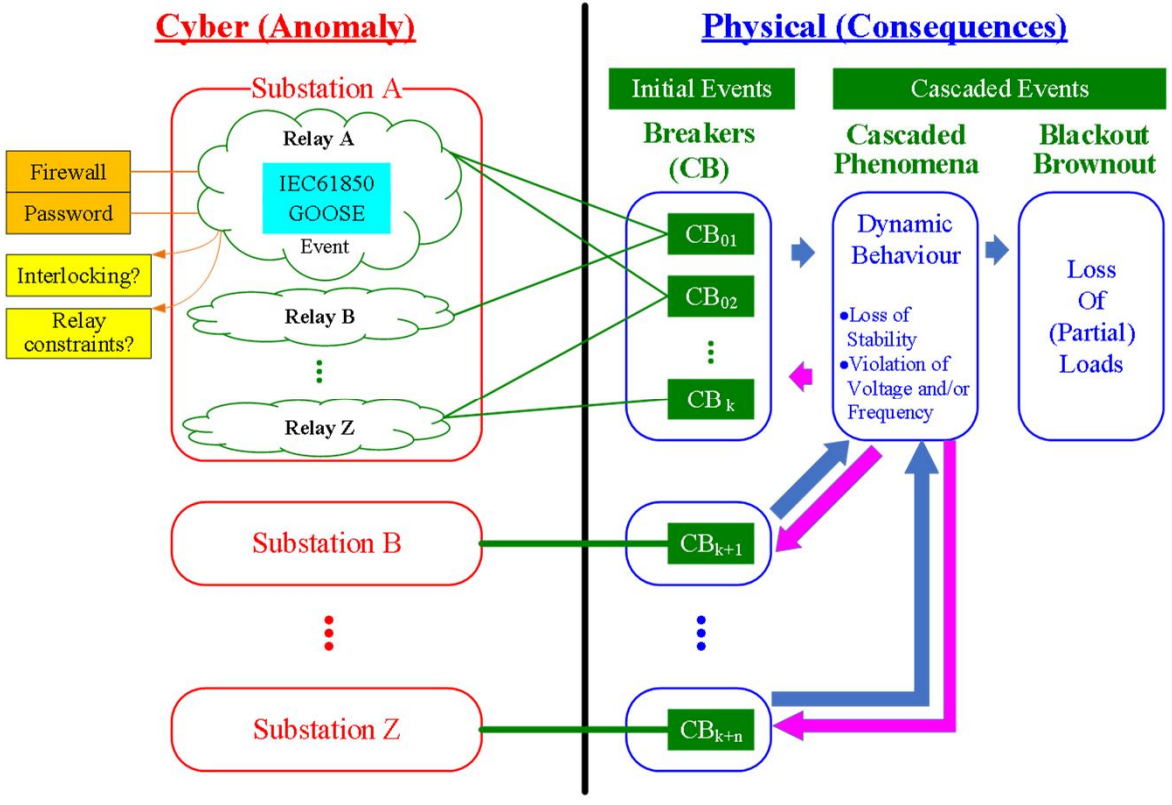
1. “Commission has previously explained, the global supply chain affords **significant benefits** to customers, including low cost, interoperability, rapid innovation, and a variety of product features. Despite these benefits, the global supply chain creates **opportunities for adversaries** to directly or indirectly **affect the management or operation of companies** with potential risks to end users that could **introduce new unintended threats** to the system and **necessitate rapid mitigating actions**.”

OT & IT Interconnectivity

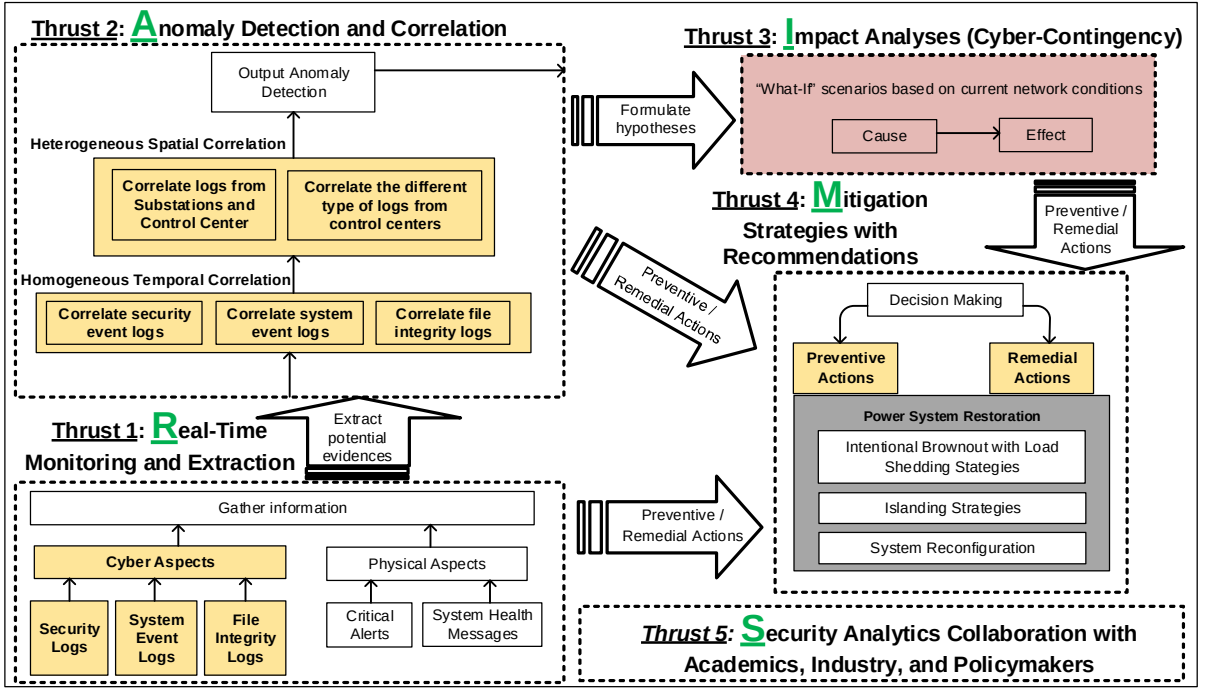


Most OT attacks start from IT networks

Components of Cyber-Physical Relationship



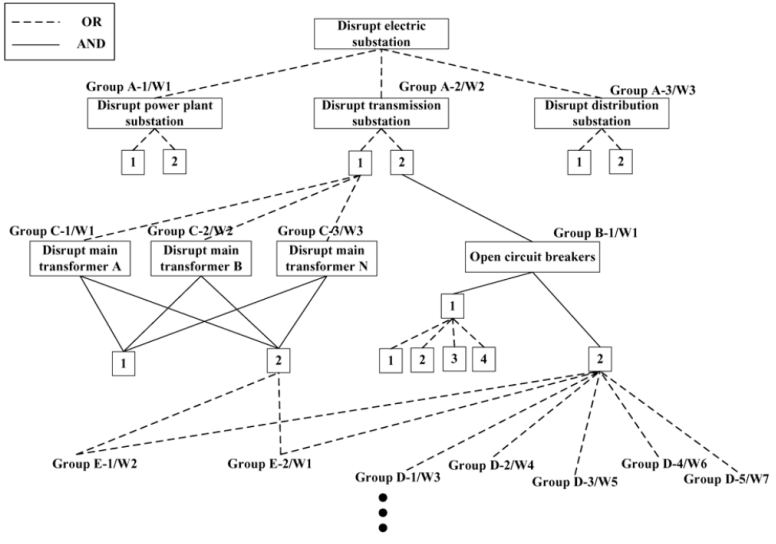
Online RAIMS Framework for Cyber-Related Decision Support Tools for SCADA Security Analytics



Chee-Wooi Ten, Manimaran Govindarasu, and Chen-Ching Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Trans. Syst., Man, Cybernetics, Part A*, vol. 40, no. 4, pp. 853—865, Nov. 2010.

Threat Modeling and Vulnerability Assessment

Attack Tree

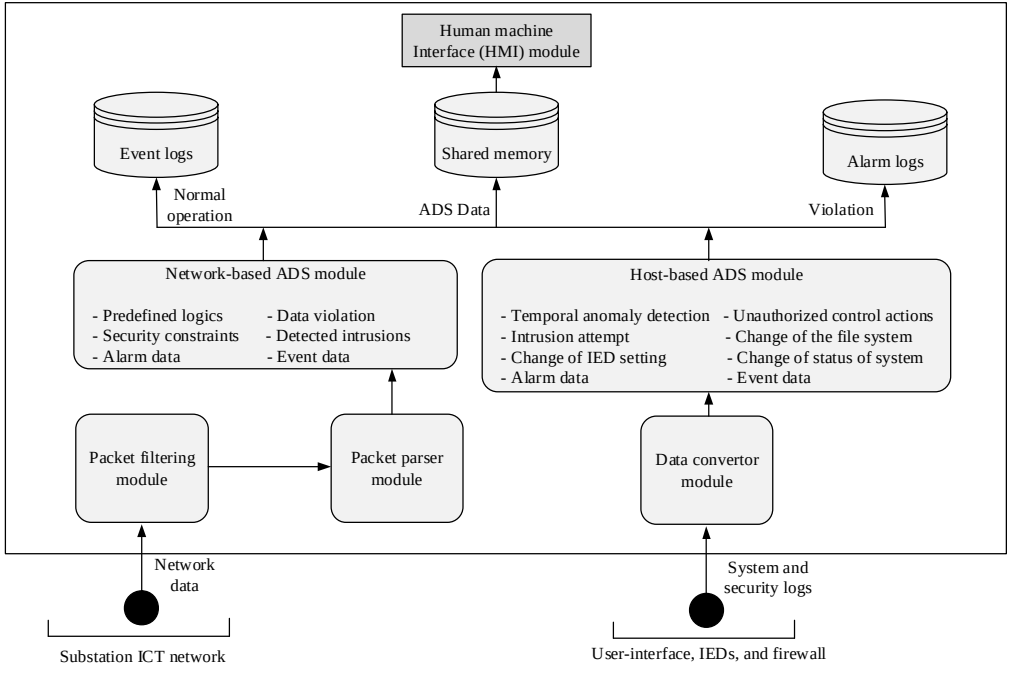


STRIDE Model

- ❑ **S**poofing
- ❑ **T**ampering
- ❑ **R**epudiation
- ❑ **I**nformation disclosure (privacy breach or data leak)
- ❑ **D**enial of service
- ❑ **E**levation of privilege

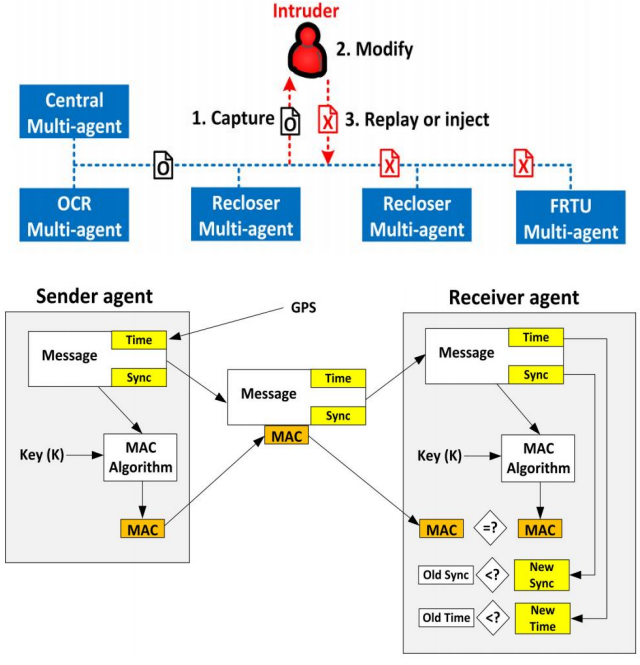
Junho Hong, Chen-Ching Liu, and Manimaran Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations." IEEE Transactions on Smart Grid, Vol. 5, No. 4, pp. 1643-1653, July 2014

Integrated Anomaly Detection System (SCADA + Cyber Alarms)



Junho Hong, Chen-Ching Liu, and Manimaran Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations." IEEE Transactions on Smart Grid, Vol. 5, No. 4, pp. 1643-1653, July 2014

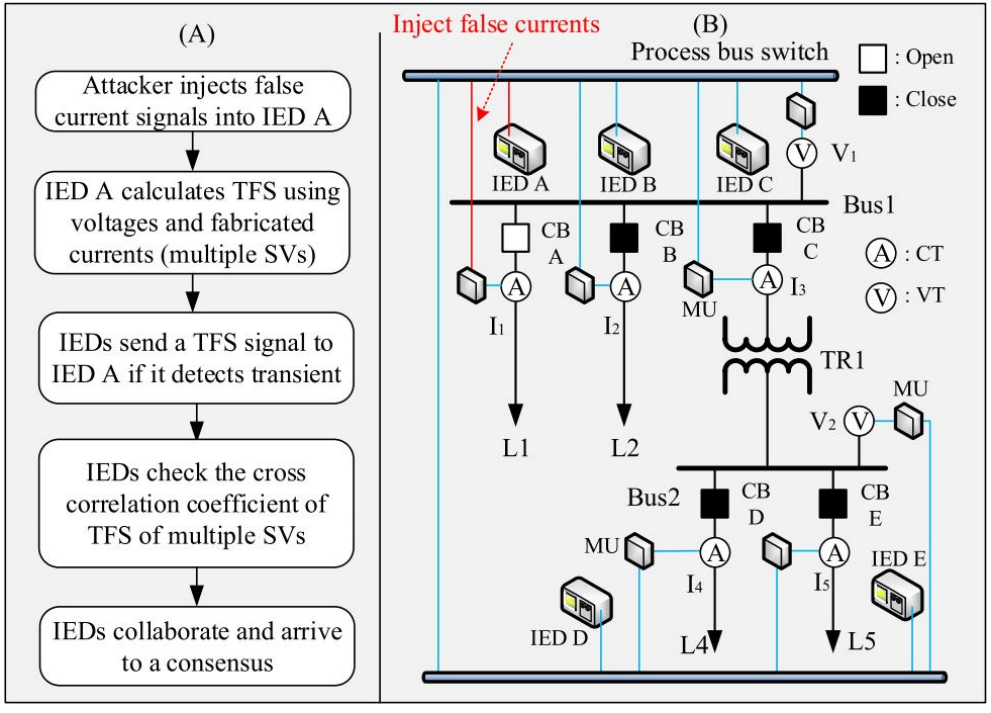
Message Authentication Code (MAC)



- False data injection attack (man-in-the-middle)
- MAC based message authentication
- Galois Message Authentication Code (GMAC) or Hash Message Authentication Code(HMAC)
- Key distribution algorithm

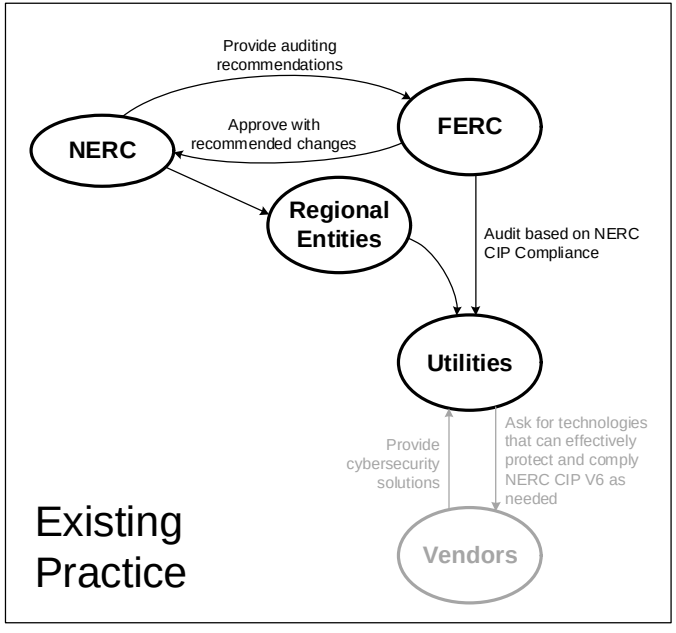
In-Sun Choi, Junho Hong, and Tae-Wan Kim, "Multi-Agent Based Cyber Attack Detection and Mitigation for Distribution Automation System," IEEE Access, No. 8, pp. 183495-183504, Oct. 2020

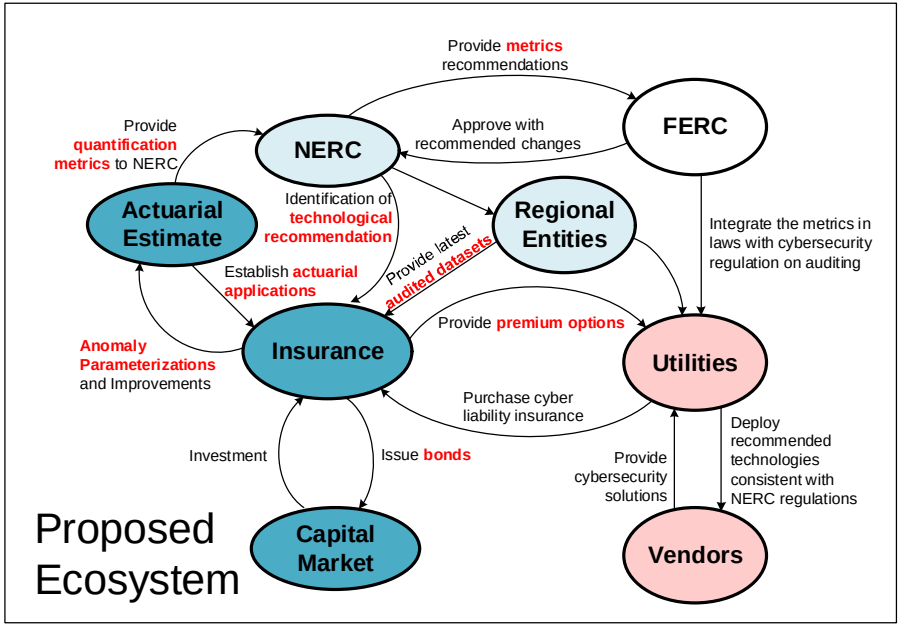
Cross-Correlation Events



Junho Hong, Reynaldo F. Nuqui, Anil Kondabathini, Dmitry Ishchenko, and Aaron Martin, "Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations," IEEE Transactions on Industrial Informatics, Vol. 5, No. 4, pp. 1643-1653, Jul. 2014.

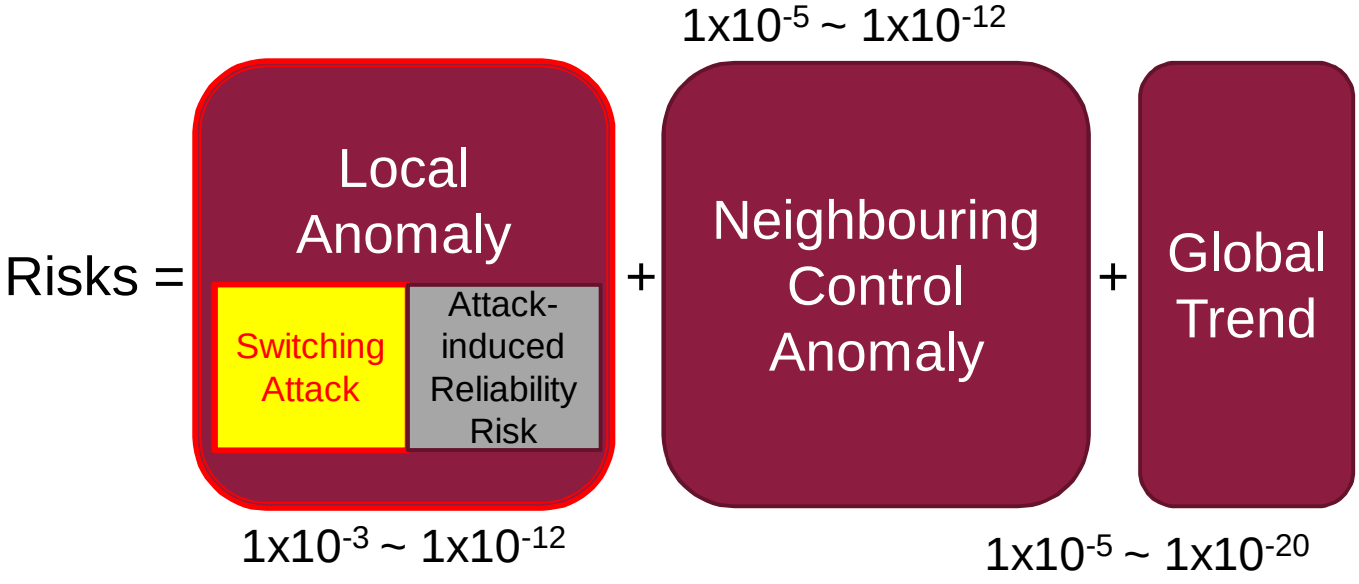
Actuarial Framework for Power Grid Cybersecurity





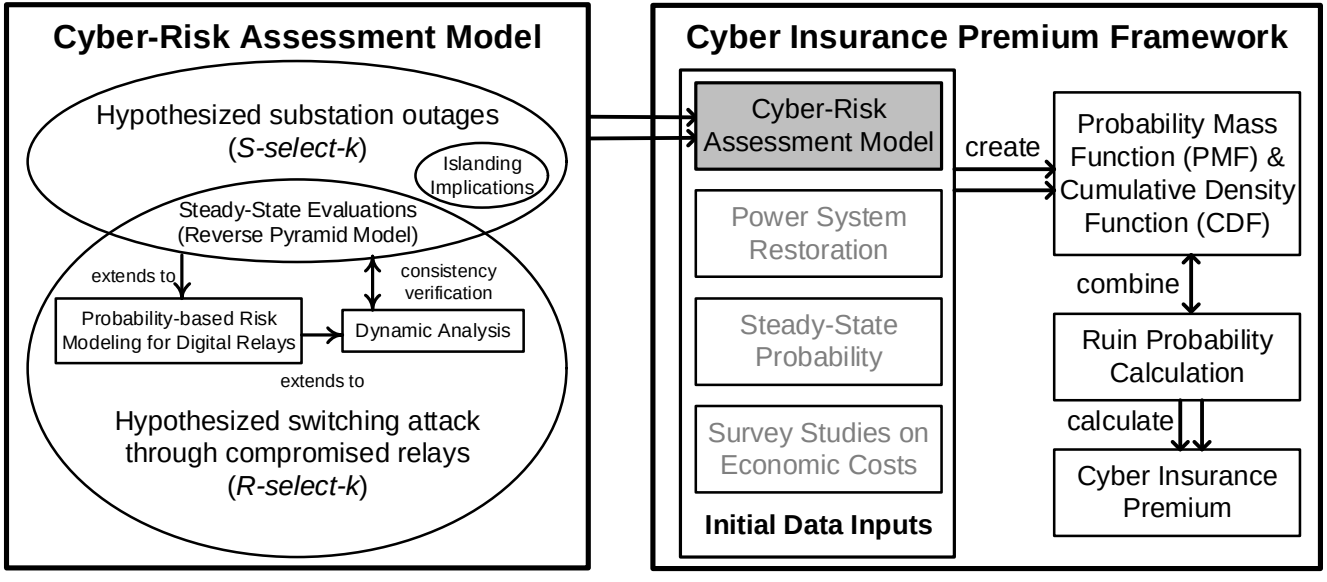
Chee-Wooi Ten (Lead PI) and Yeonwoo Rho, "CPS: Medium: Collaborative Research: An Actuarial Framework of Cyber Risk Management for Power Grid," National Science Foundation, Sep. 1, 2017 – Aug. 31, 2021. Total Amount: $348,866 of $700,975 with University of Wisconsin—Milwaukee.

Risks of Cyberattack



Cyber Insurance Premium for an Interconnected Grid

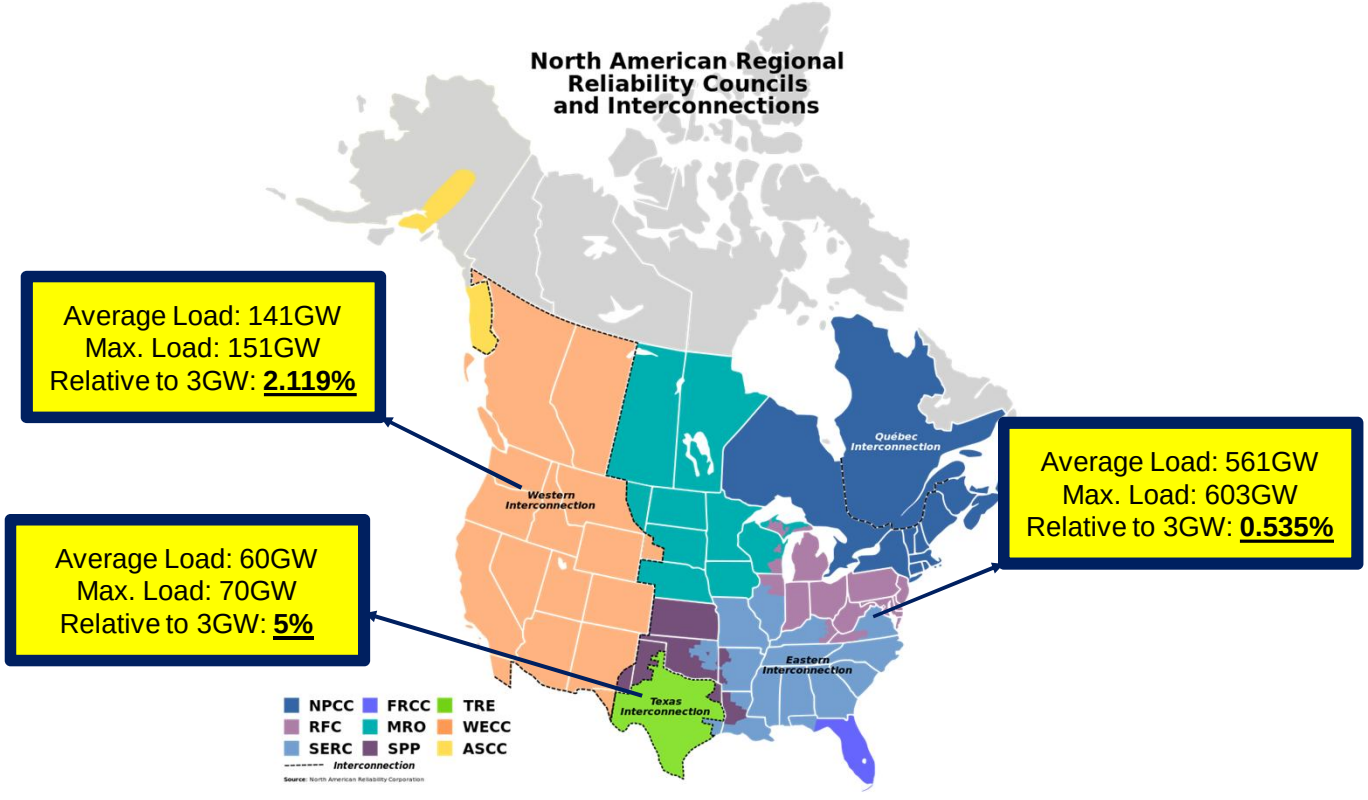
IP-based substations, generating units, and other interconnected grids MUST be qualitatively and quantitatively established in the insurance incentive policies with security technologies against switching cyberattacks.



NERC CIP Definition of High, Medium, and Low Impact Ratings

- **High Impact**
  - Control centers (Reliability coordinator, balancing authority, transmission operator, generator operator) with aggregated amount of 3,000MW within an interconnection
- **Medium Impact**
  - Control center exceeding 1,500 MW
  - 500-kV substations or higher
  - Special Protection Systems (SPS), Remedial Action Schemes (RAS)
  - Automatic Load shedding 300 MW without human operator
- **Low Impact**
  - Everything else

3,000MW Relative to Interconnection

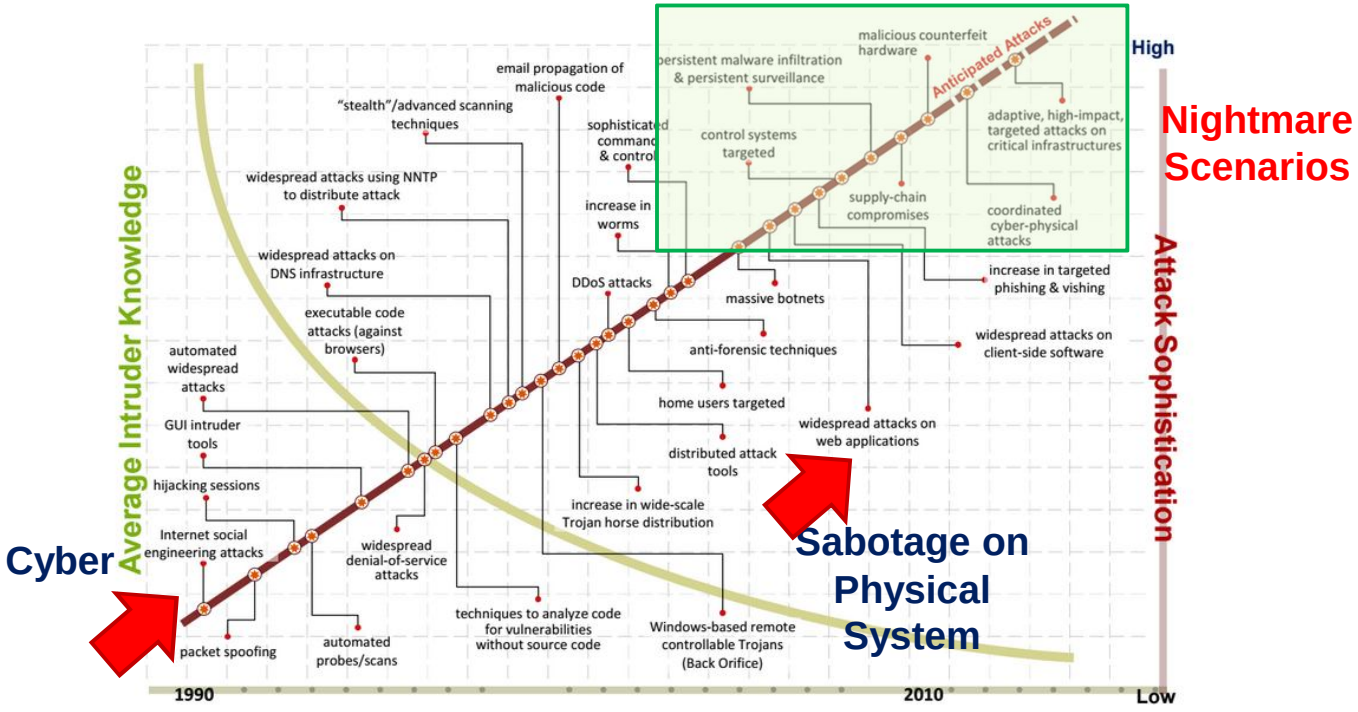


Average Load: 141GW
Max. Load: 151GW
Relative to 3GW: **2.119%**

Average Load: 60GW
Max. Load: 70GW
Relative to 3GW: **5%**

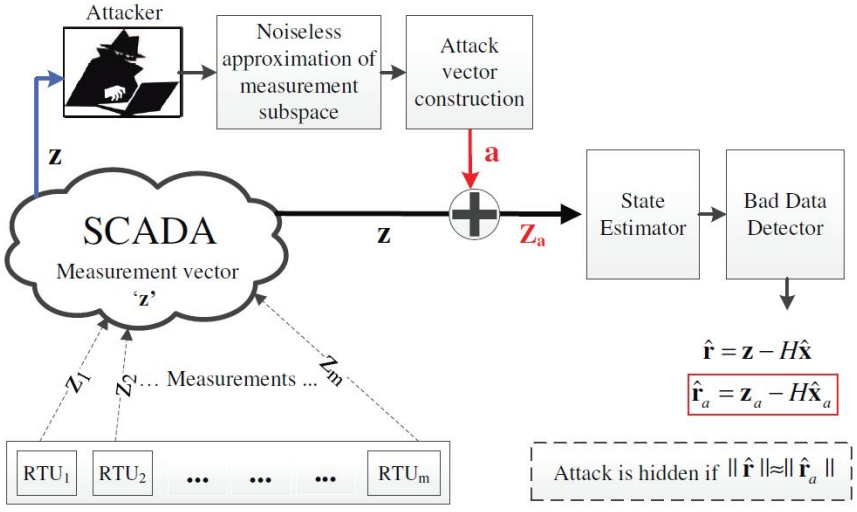
Average Load: 561GW
Max. Load: 603GW
Relative to 3GW: **0.535%**

Evolution of Intelligent Cyber-Physical Attacks



Summary of a workshop: "The resilience of the electric power delivery system in response to terrorism and natural disasters" by the division of Engineering and Physical Sciences, *National Research Council of the National Academies*, 2013

False Data Injection (FDI) Attack

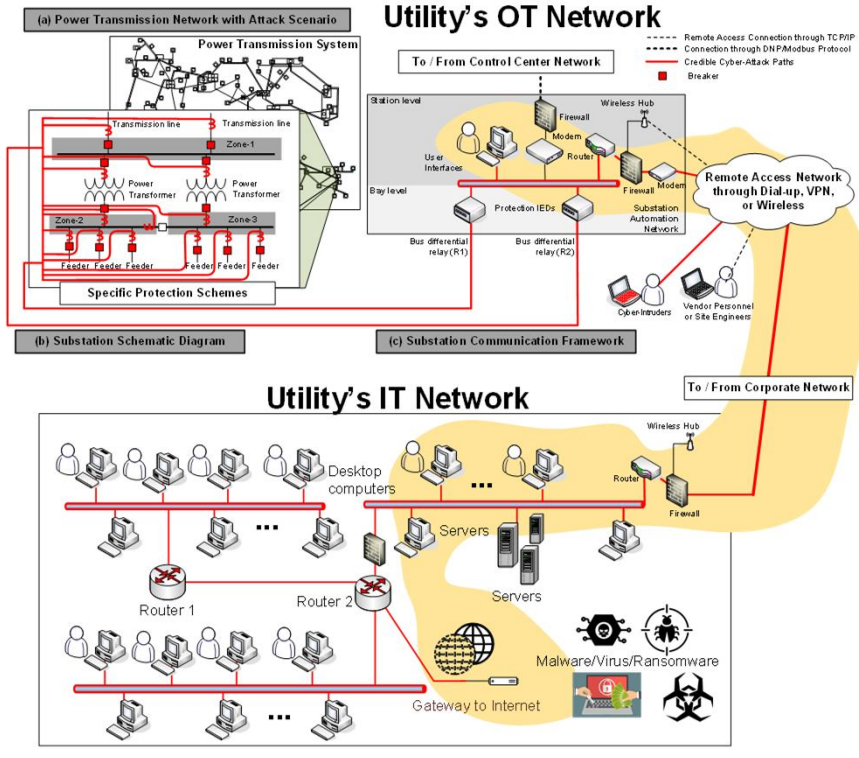


Adnan Anwar, "Data-Driven Stealthy Injection Attacks on Smart Grid," PhD dissertation, The University of New South Wales, Australia, Nov. 2017.

- Assumptions of FDI:
  - Know power system topology
  - Line parameters information
- Change the analog or digital measurements → Generalization is unrealistic!

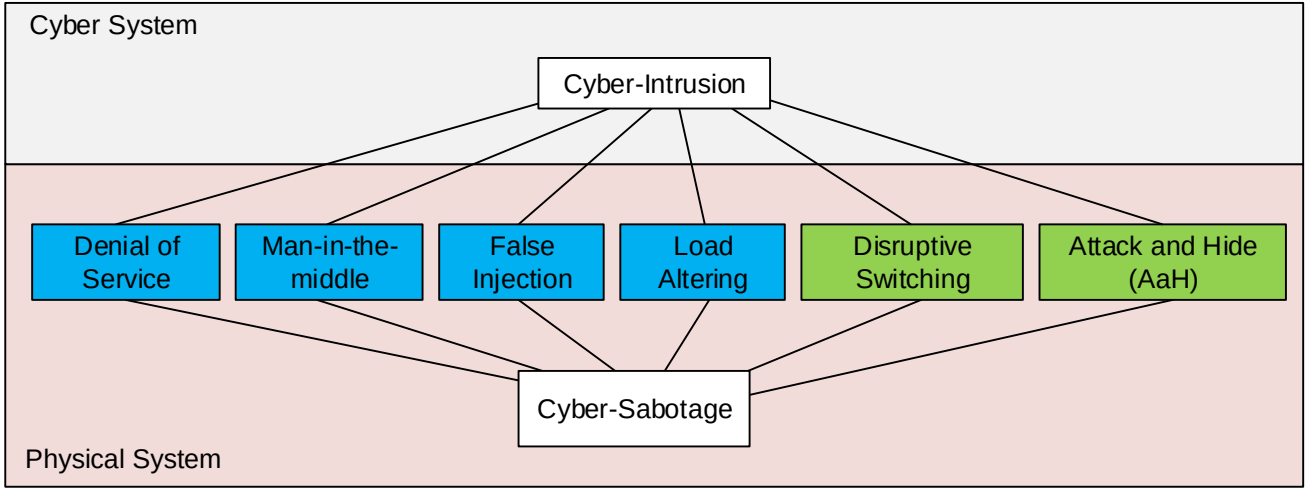
- Realistic aspect of such attack vectors?
  1. **Compromised end point**
  2. **Man-in-middle attack**
- Should we assume insiders and outsiders collaboration as realistic problem?

Ukraine’s Cyberattacks on Power Grid



1. Malware propagates from one network to others
2. Scanning and hope to other hosts in other network
3. Found open SSH (Unix) connecting OT network
4. Connect to other systems, malware propagates to vulnerable computers
5. Destroy the electronic evidence on the installation
6. Ready for cyber-physical attack on the SCADA network

Cyber-Physical Systems Security of a Power Grid



- System instability and system-wide blackout
- Equipment damage
- Mislead operators or conceal actual states
- Obvious cyberattack

A Different Set of Challenges

Enterprise IT

- What?
  - Information
- Risk?
  - Information disclosure
- Security?
  - Confidentiality
- Requirements?
  - 95~99%
- How?
  - Reboot, patching

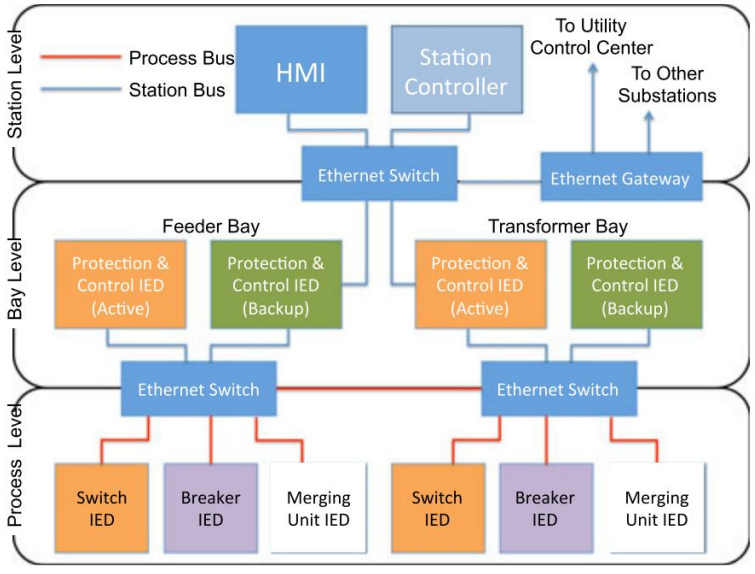
Energy OT

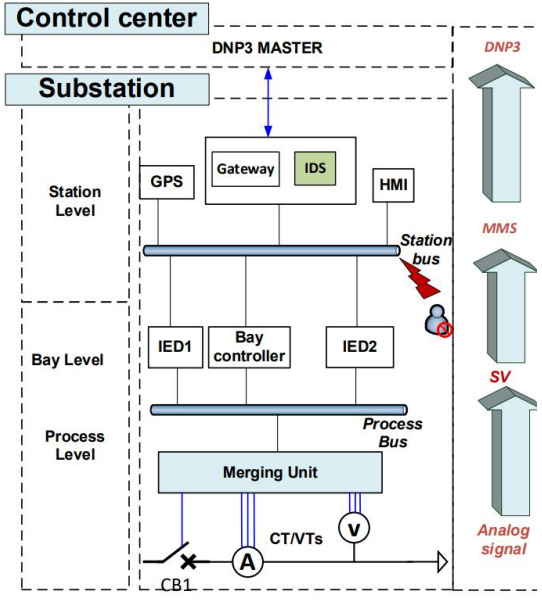
- What?
  - Process
- Risk?
  - Safety
- Security?
  - Availability
- Requirements?
  - 99.9%
- How?
  - Online repair

Unique Cybersecurity Requirements of Energy OT

- Must operate 24/7 (availability and reliability) even after cyber incident
- Rack of computational power to support the additional cybersecurity capabilities (e.g., encryptions)
- Conventional + modernized devices
- Easy to access physically
- Real-time operation (delay is not acceptable)

IEC61850 Standard for Substation Automation and Attack Vectors/Paths

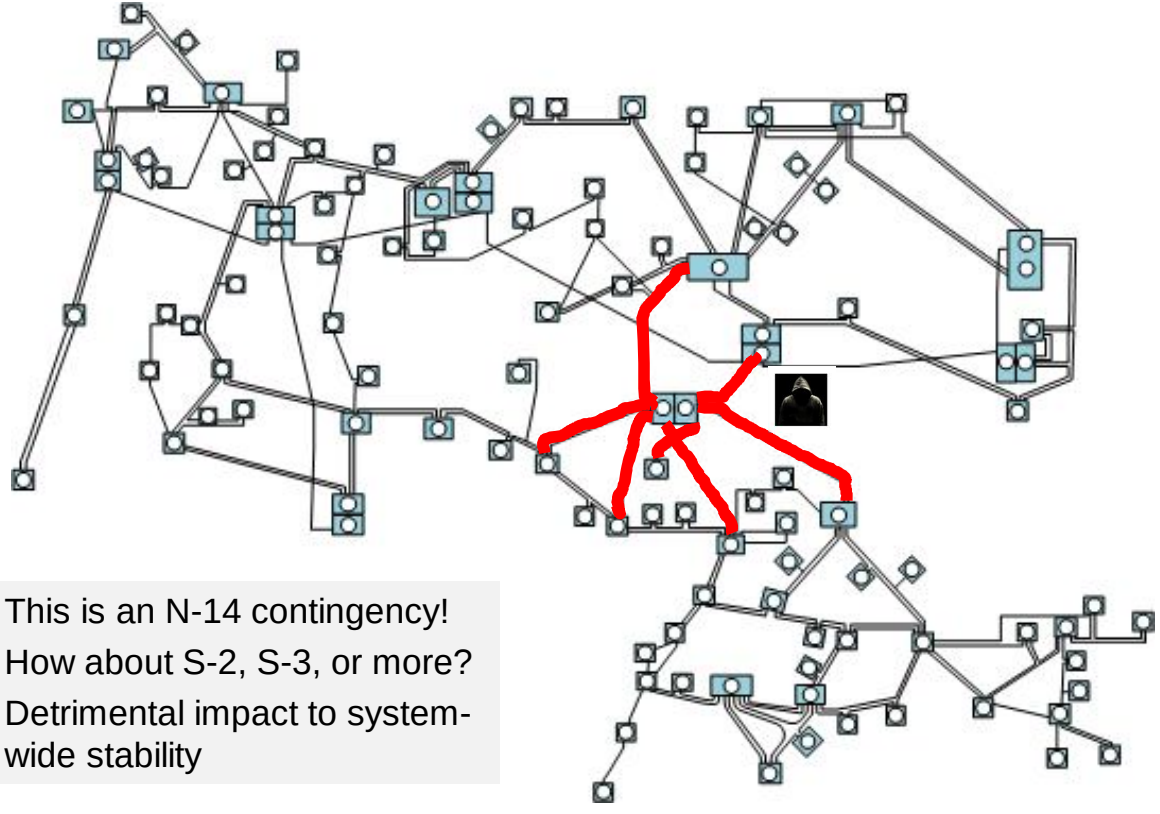




Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, “Toward Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation,” IEEE Trans. Ind. Inf., Vol. 14, No. 6, Jun. 2018.

Ruoxi Zhu, Chen-Ching Liu, Junho Hong, and Jiankang Wang, “Intrusion Detection against MMS-based Measurement Attacks at Digital Substations.” IEEE Access, Vol. 5, pp. 1240-1249, Dec. 2020.

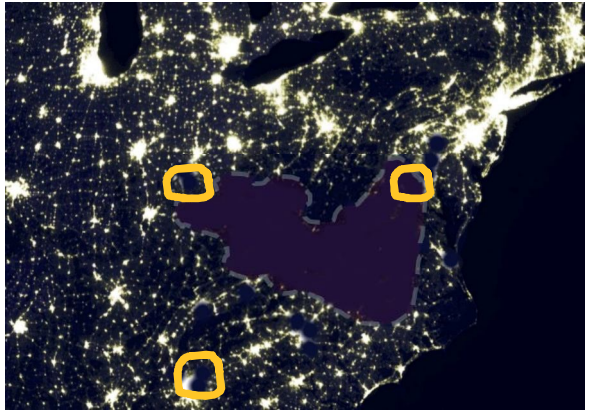
S-1 Contingency

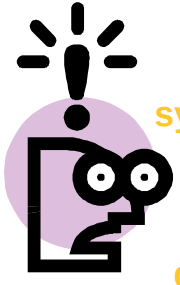


- This is an N-14 contingency!
- How about S-2, S-3, or more?
- Detrimental impact to system-wide stability

A Hypothetical Scenario

Breakers opened, what happened?





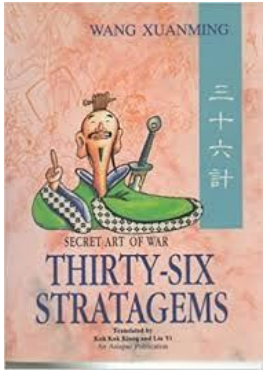
Something bad happened, the EMS system has shown that there are manually switching actions occurring over 3 different substations

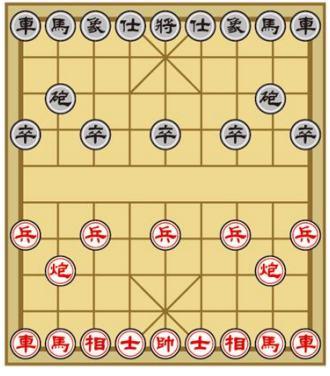
Deception and Gaming

- Tomb Robbing in Ancient Egypt
- Thirty-Six Stratagems
- Western Chess / Chinese Chess 象棋
- Human nature of deception exists in any platform

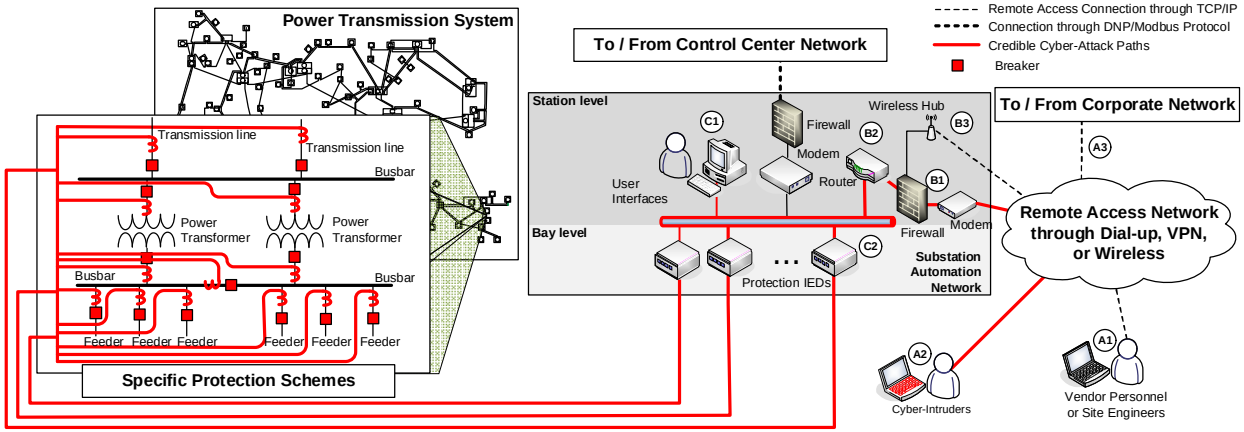
→ Good collaboration with *political science* folks

- Two players (attackers and defenders)



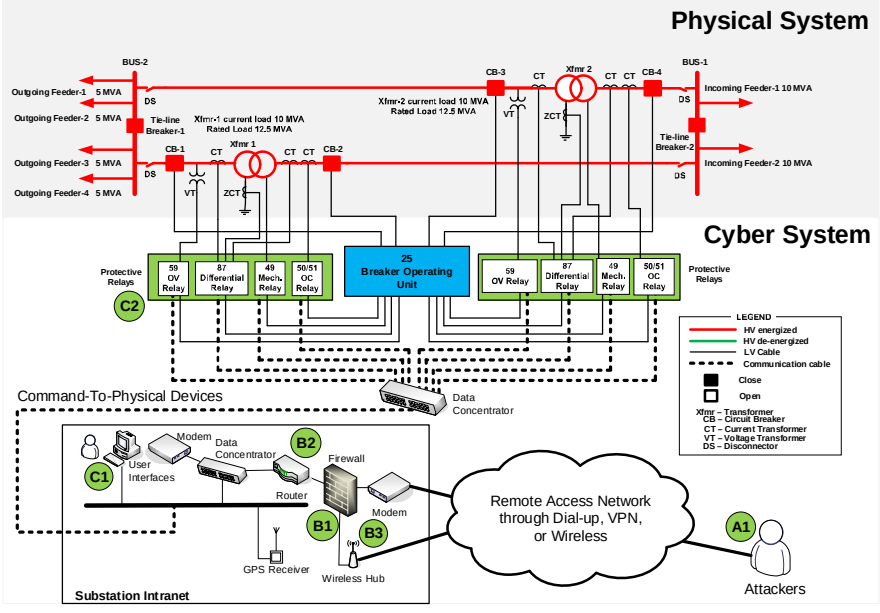


Cyber-Physical Relationship for a Substation Example



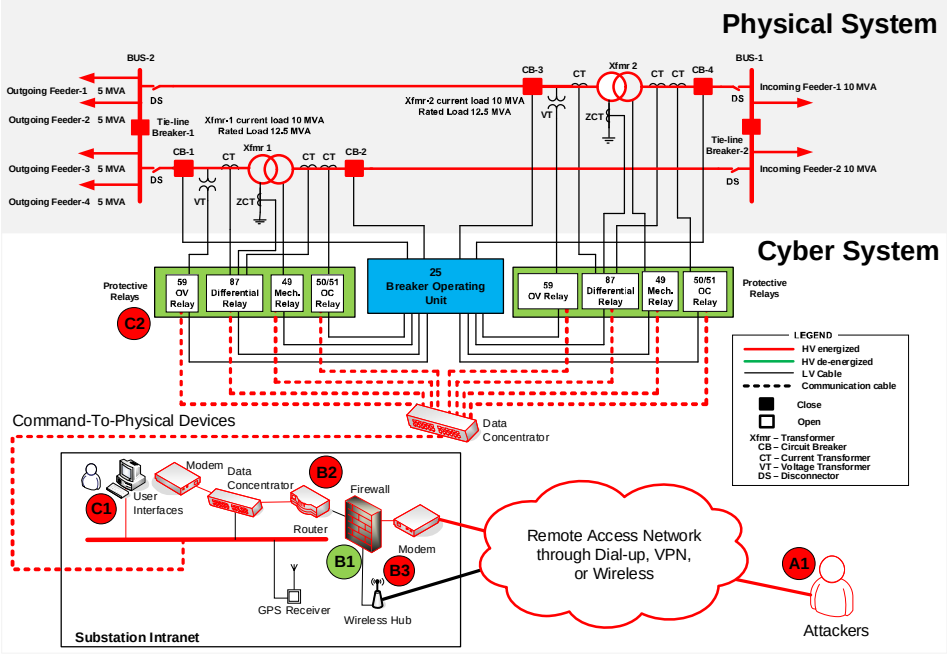
- Remote access availability vs. security protection
- Attack through access points of
  - **C1:** User interface
  - **C2:** Direct IED connections
- Defender (**complete information**) vs. Attackers (**incomplete information**)

Step 1: Two power transformers are in parallel (under normal operating conditions)



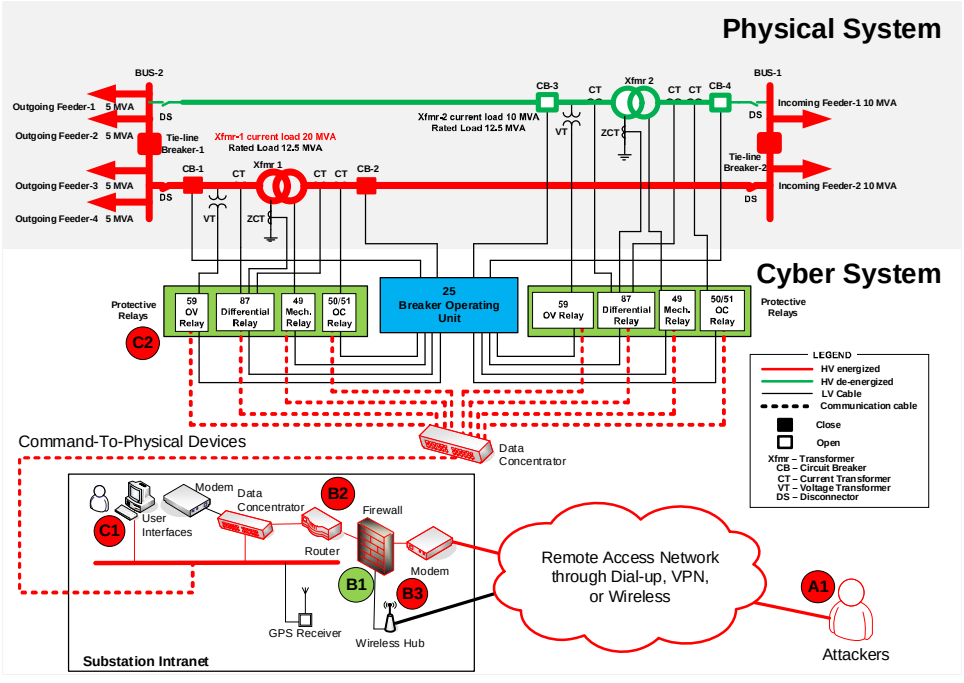
- Node A1 is where attackers begin. They may be using available tools to identify possible access to the substation networks

Step 2: Substation network is compromised



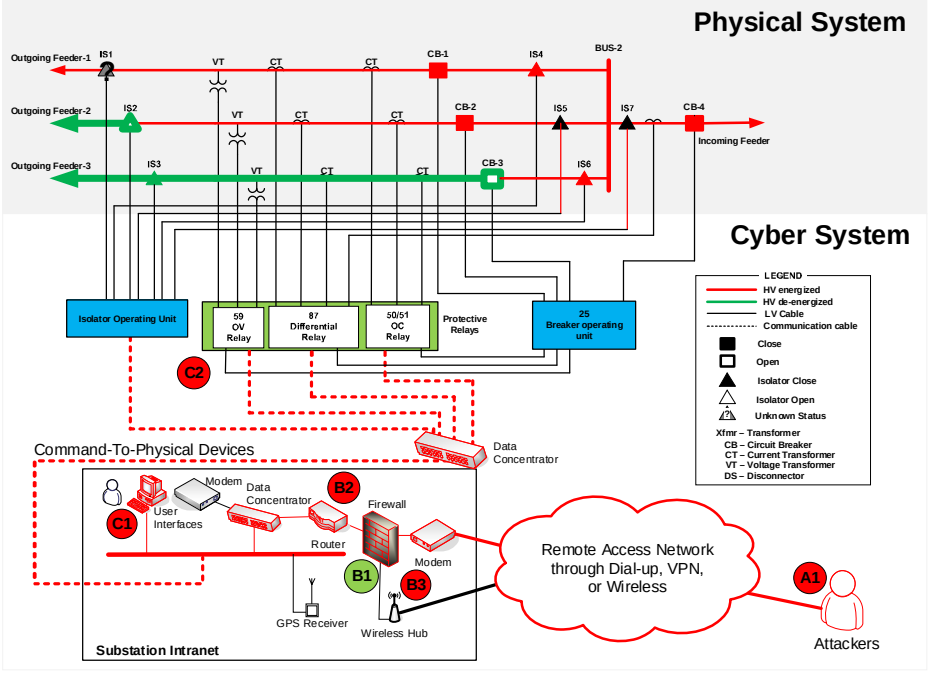
- ❑ **Possibility 1**: (A1→B3→B2→C1) through user interface(s)
- ❑ **Possibility 2**: (A1→B3→B2→C2) through the IEDs

Step 3a: Either circuit breaker 3 or 4 is tripped by the attacker



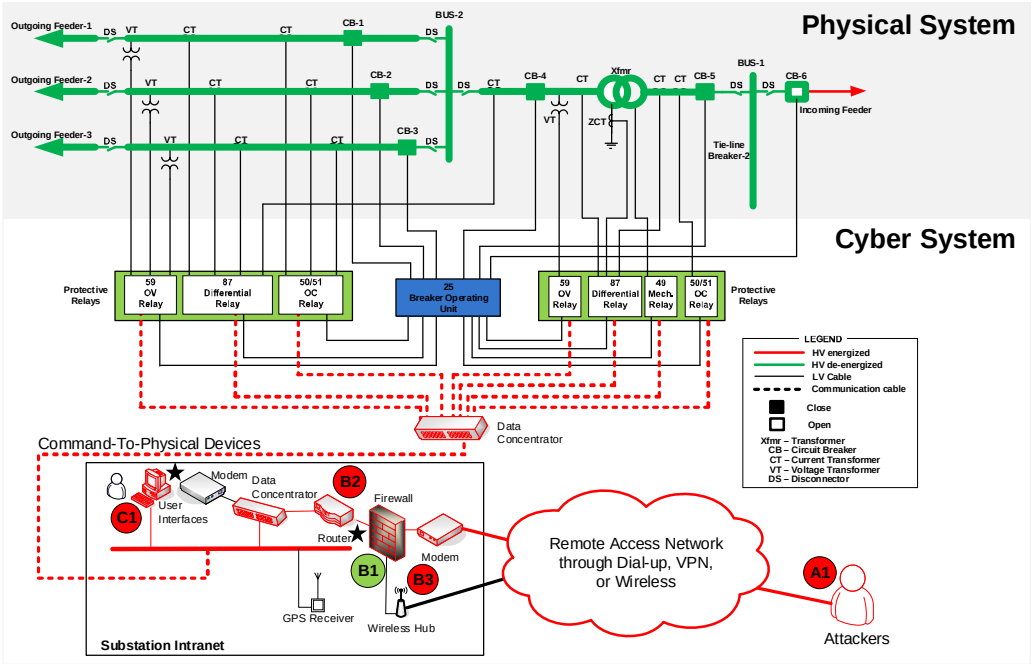
- ❑ **Possibility 1**: (A1→B3→B2→C1) through user interface
- ❑ Learning how the local SCADA system works and link addresses

Step 3b: ***Continuous*** disruptive switching action of circuit breakers and isolators



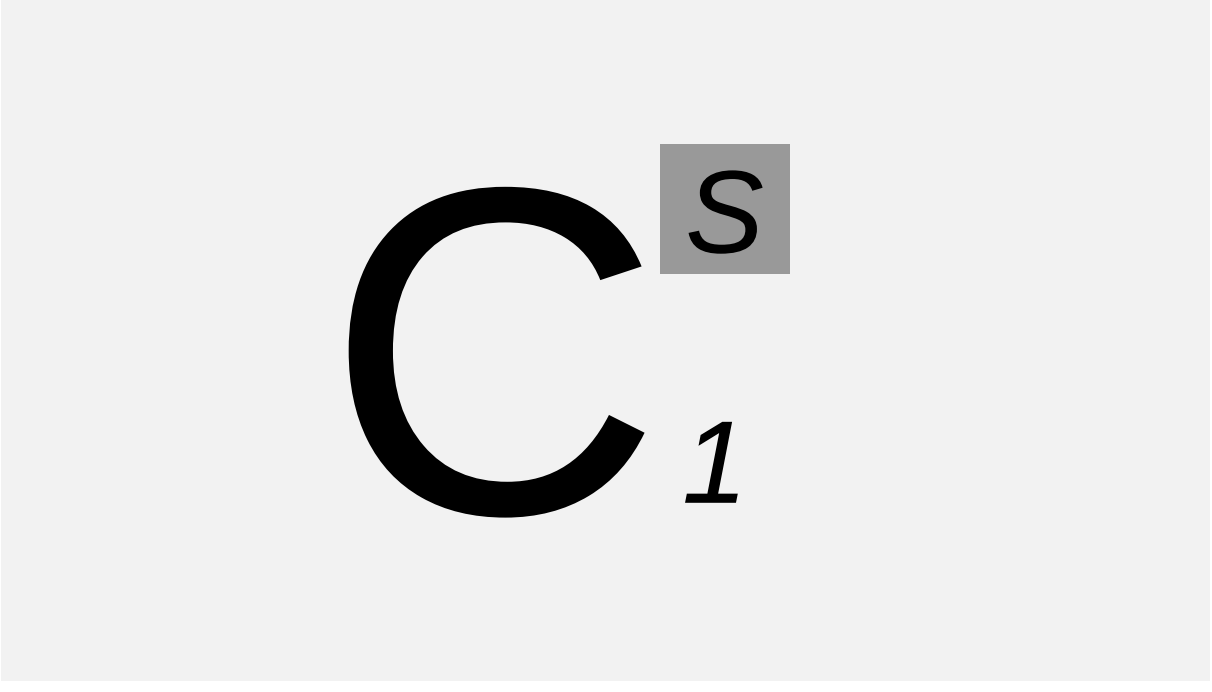
- **Possibility 2**: Learn how to lurk each step and execute disruptive switching actions

Step 3c: Entire substation outage by opening the circuit breaker 6



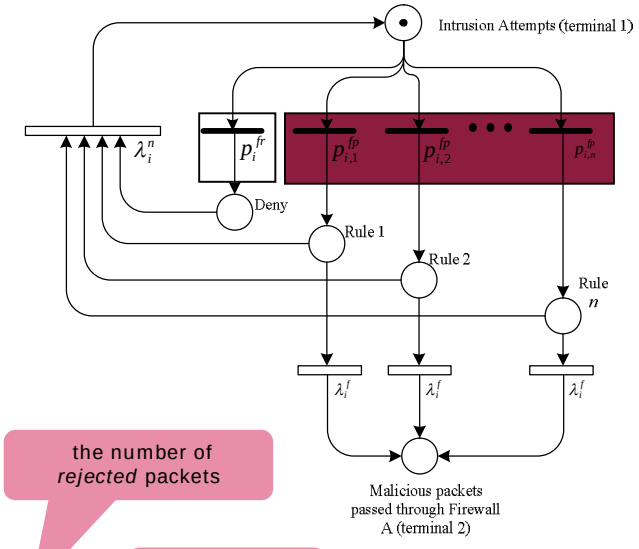
- **Possibility 3**: Disconnect the substation electrically from the grid.

Hypothesized One Substation Outage



Firewall Model

- **The firewall model depicted** includes ***n*** **paths corresponding to *n* rules** in the firewall model
- The submodel consists of circles that are the states **representing the denial or access of each rule**
- Malicious packets **traveling through policy rule *j* on each firewall *i* is taken into account.**



probability of malicious packets traveling through a firewall rule

denotes the frequency of malicious packets through the firewall rule

$$p_{i,j}^{fp} = \frac{f_{i,j}^{fp}}{N_{i,j}^{fp}}$$

total record of firewall rule *j*.

the number of *rejected* packets

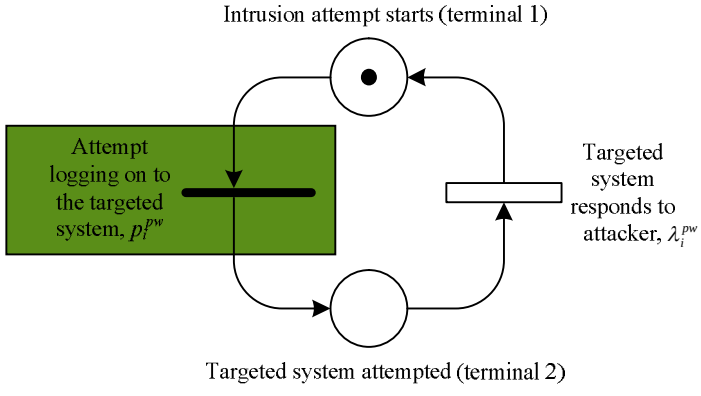
probability of the packets being *rejected*

$$p_i^{fr} = \frac{f_i^{fr}}{N_i^{fr}}$$

denotes the total number of packets in the firewall logs

Password Model

- The **intrusion attempt to a machine** is modeled by a transition probability associated with a solid bar. An empty bar represents the *processing execution* rate that responds to the attacker
- **An account lockout feature**, with a limited number of attempts, can be simulated by initiating the ***N* tokens** (password policy threshold).



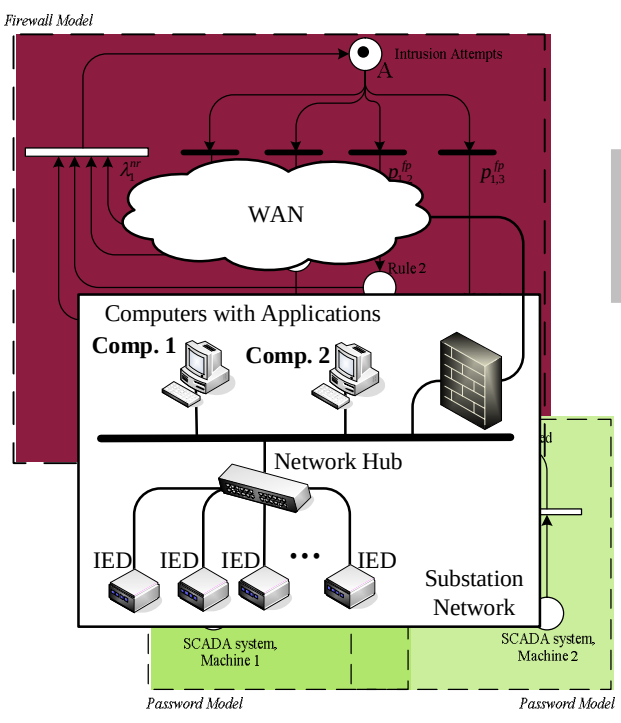
the intrusion attempt probability of a computer system, *i*

$$p_i^{pw} = \frac{f_i^{pw}}{N_i^{pw}}$$

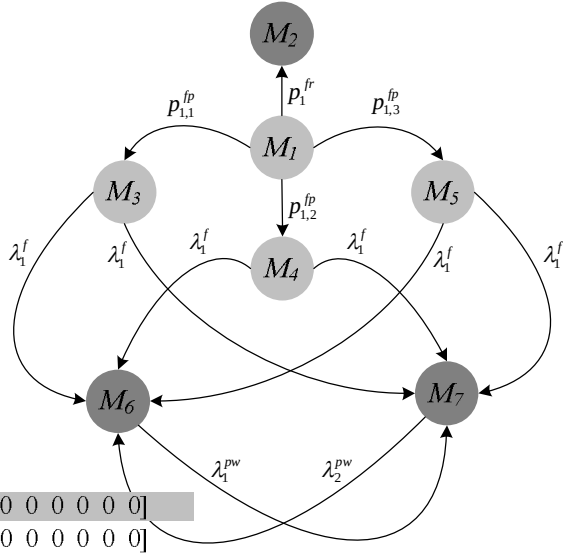
number of intrusion attempts

total number of observed records

One-Firewall-Two-Machine Example

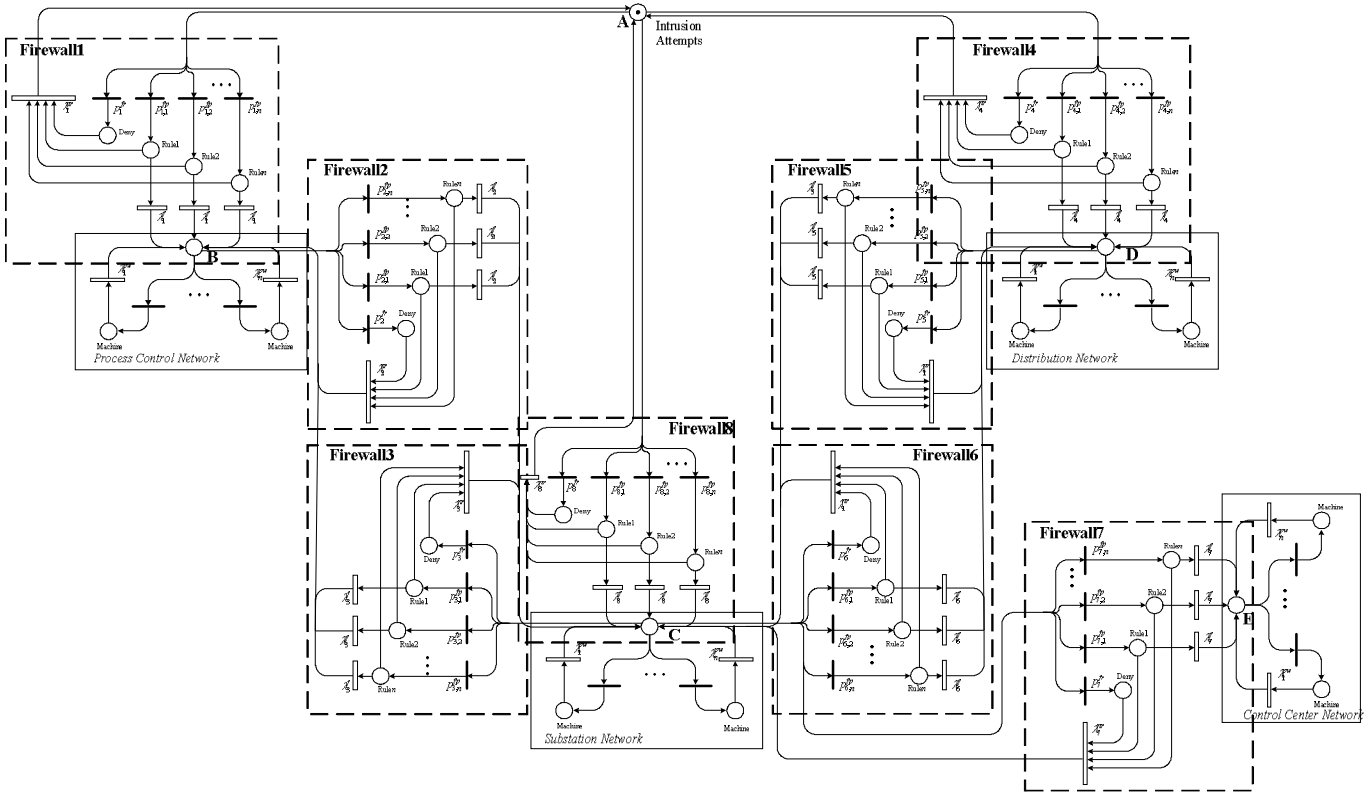


Convert to Reacbability Graph

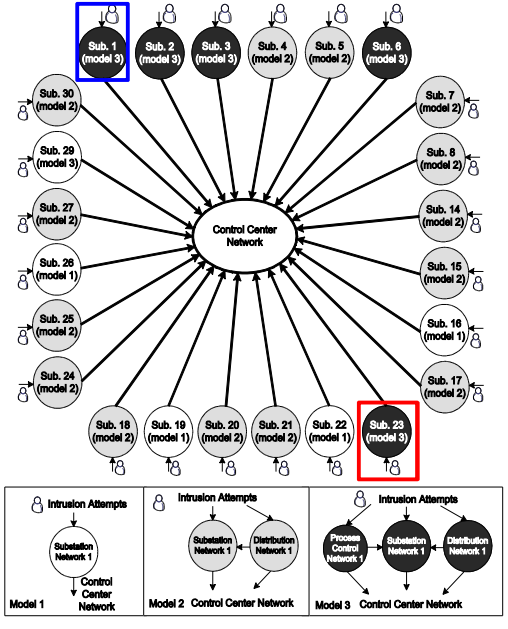


M_1=[1 0 0 0 0 0 0 0]
M_2=[0 1 0 0 0 0 0 0]
M_3=[0 0 1 0 0 0 0 0]
M_4=[0 0 0 1 0 0 0 0]
M_5=[0 0 0 0 1 0 0 0]
M_6=[0 0 0 0 0 0 1 0]
M_7=[0 0 0 0 0 0 0 1]

Model 3 of Cyber-Net



Steady-State Probabilities



STEADY STATE PROBABILITIES FOR SUB. 1 AND SUB. 22

Attack Starts from	Machines	Sub. 1 (Model 3)	Sub. 22(Model 1)
Outside	$SB3$	.5783	–
	$SC4$	.0007	.0004
	$SE5$	.0412	.1401
	$SE7$	.0283	.0141
	$SE8$	.0178	.0380
	$SE9$	.0640	.0405
Inside	$SB3$	.0294	–
	$SC4$	.0015	.0037
	$SE5$	.2521	.4038
	$SE7$	.1722	.0404
	$SE8$	.1086	.1088
	$SE9$	.3903	.1164

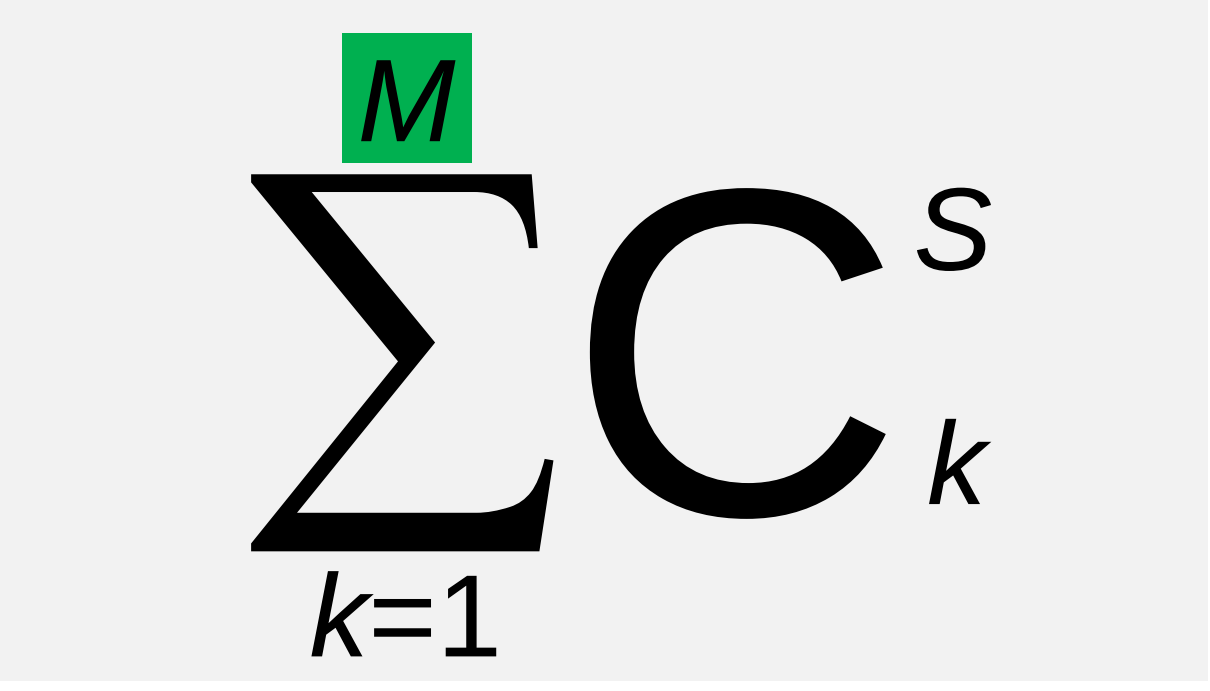
$$V(I_{sub1}) = \left(\sum \pi_x\right) \times \gamma_{sub1} + \left(\sum \pi_y\right) \times \gamma_{CCen}$$
$$= (.5789) \times \left(\frac{.3}{189.2}\right)^{1.5} + (.1512) \times \left(\frac{189.2}{189.2}\right)^{0}$$
$$= .1513.$$

$$x = \{SB3, SC4\} \text{ and } y = \{SE5, SE7, SE8, SE9\}$$

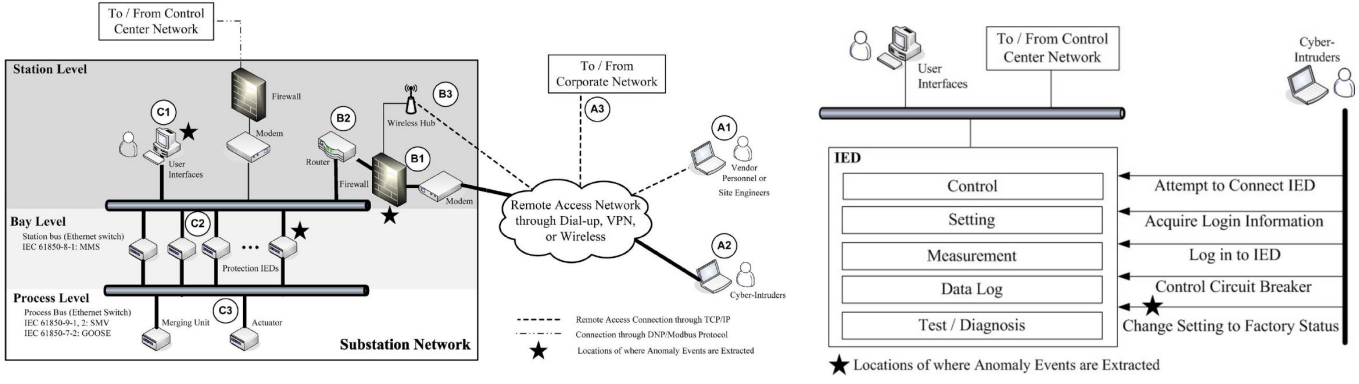
- Modeling of ***Cyber-Net*** between network entities
  - Model 1: Substation and Control Center Networks
  - Model 2: Substation, Distribution, and Control Center Networks
  - Model 3: Substation, Process Control, and Control Center Networks

Chee-Wooi Ten, Chen-Ching Liu, and Manimaran Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836—1846, Nov. 2008. <10.1109/TPWRS.2008.2002298>

Hypothesized Outages Based on A Limited Set of Malicious Substations



Anomaly Detection for Substation Cybersecurity



Outsiders

- ❑ Any point of (A1, A2, A3)-B1-B2
- ❑ Any point of (A1, A2, A3)-B3-B1-B2

Insiders

- ❑ User interface, C1;
- ❑ Direct IED connection, C2;
- ❑ Eavesdropping and data packet modification, C3

Chee-Wooi Ten, Junho Hong, and Chen-Ching Liu, "Anomaly Detection for Cybersecurity of the Substations," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 865—873, Dec. 2011. <10.1109/TSG.2011.2159406>

Temporal Correlation of Substation Anomaly

- Weight assignment for each anomaly property on a substation cyber network

$$\mathbf{\Pi}_{(1\times k)} = \left(1 \quad \pi^{\mathbf{a}}{}_{(T\times L)} \quad \alpha\cdot\pi^{\mathbf{fs}}{}_{(T\times M)} \quad \beta\cdot\pi^{\mathbf{o}}{}_{(T\times N)} \quad \varepsilon\cdot\pi^{\delta}{}_{(T\times O)} \right)$$

- Normalized row vector corresponds to each

$$\hat{\Pi}_j = \frac{\Pi_j}{\|\Pi_j\|_2}$$

- Temporal anomaly

$$\mathbf{\Delta}_{ta} = 1 - \frac{\hat{\Pi}_j \cdot \hat{\Pi}_{j-1}^{\top}}{\|\hat{\Pi}_j\|_2 \cdot \|\hat{\Pi}_{j-1}\|_2}$$

Combinatorial Evaluation

- Assumption of *S* select *k* components where *S* is limited.
  - *M* is the total number of anomalous substations
  - *k* is the hypothesized substation outage

- Criticality of hypothesized categories
  - ***Critical List***: List of substations which results non-convergent power flow solution
  - ***Priority-1 List***:
    (1) Substations not included in critical list,
    (2) Combinations with 2 substations in *S* list
  - ***Priority-2 List***: Combinations consists of more than 2 substations

Spatial Correlation and Simultaneous Attacks

- Anomaly matrix represents each substation that is determined from each problem event

$$\mathbf{P} = \begin{cases} \mathbf{0} & \text{if } \zeta = 0 \\ \hat{\mathbf{\Pi}} \cdot \mathbf{B} \cdot \mathbf{\Delta_{ta}} & \text{Otherwise} \end{cases}$$

- Qualifier is determined by

$$\varrho \quad = \quad \max \mathbf{P} - \overline{\mathbf{P}}$$

- Combination of simultaneous attacks
  - Priority 1 and 2 Lists

$$\sum_{k=1}^{m} \mathbf{C}_k^n = \sum_{k=1}^{m} \frac{n!}{k!(n-k)!}$$

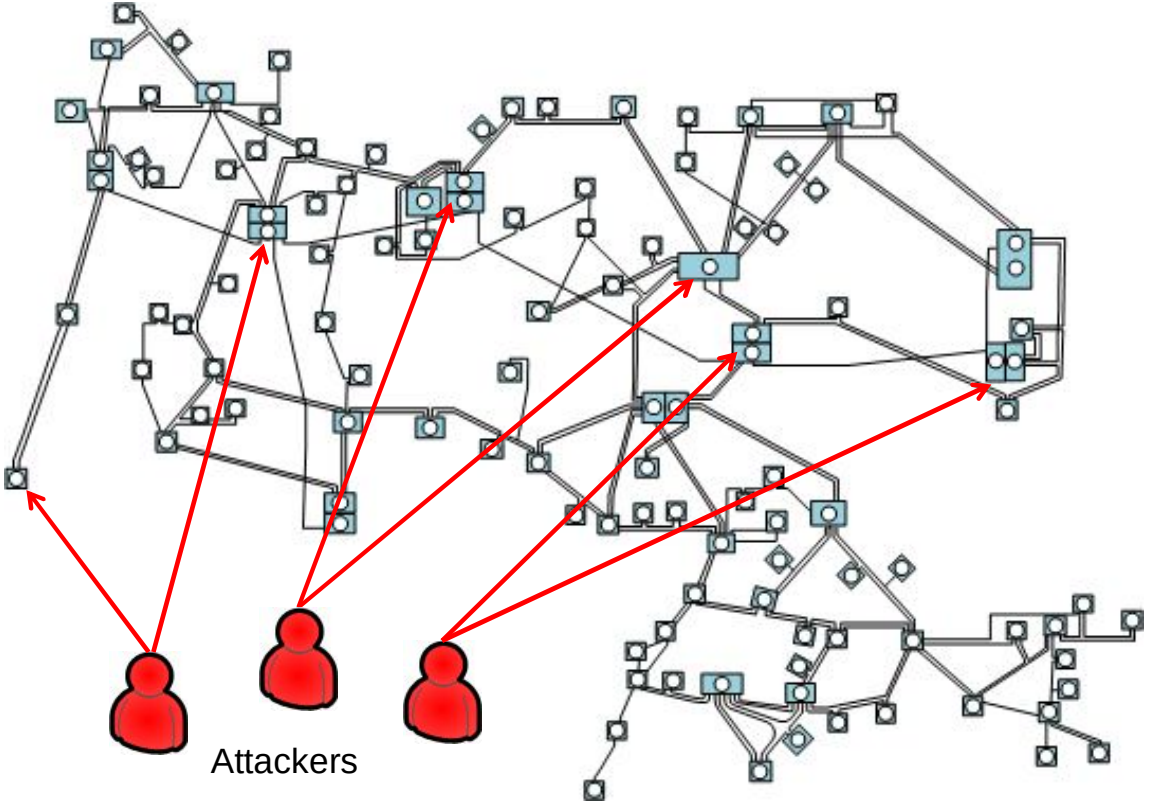
$$= \frac{n!}{(n-1)!} + \cdots + \frac{n!}{m!(n-m)!}$$

Priority 1 List

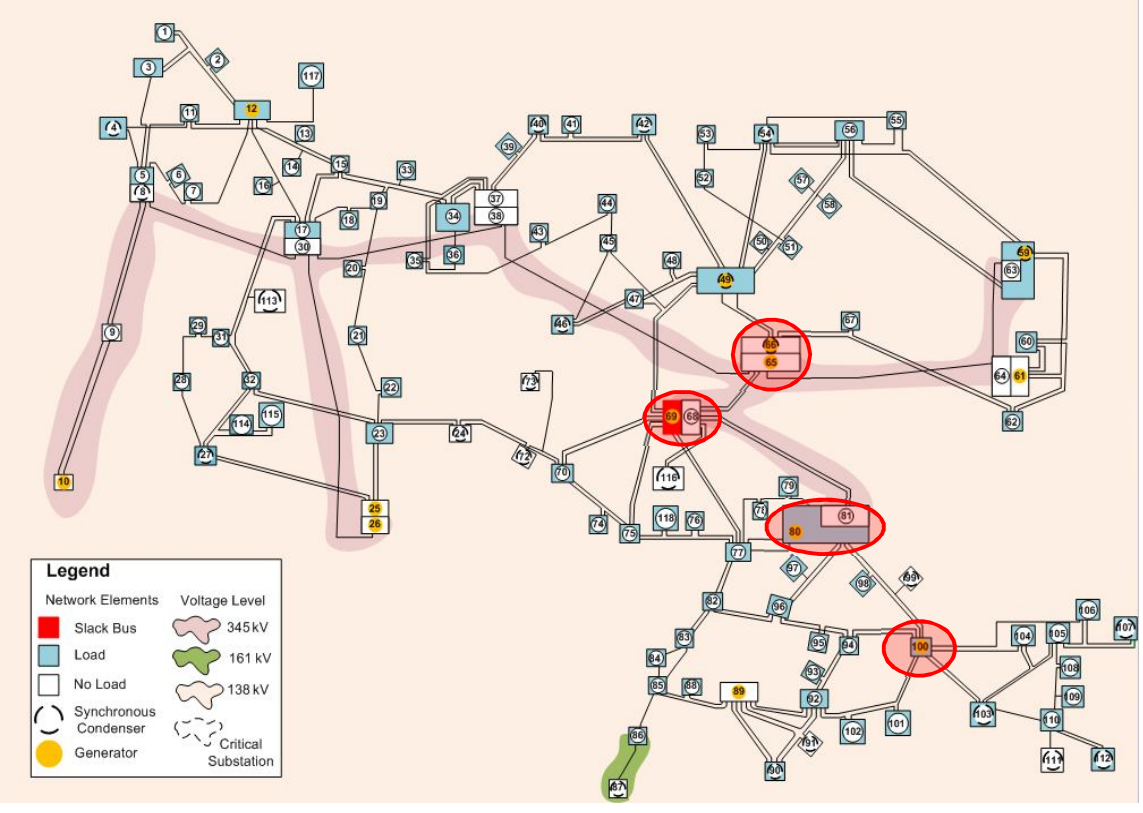
$$\mathcal{P}_1 \quad = \quad \sum_{k=1}^{2} \mathbf{C}_k^n$$

$$V_{sub}(i,j) = \gamma_{i,j} \cdot \max(\varrho_i, \varrho_j)$$

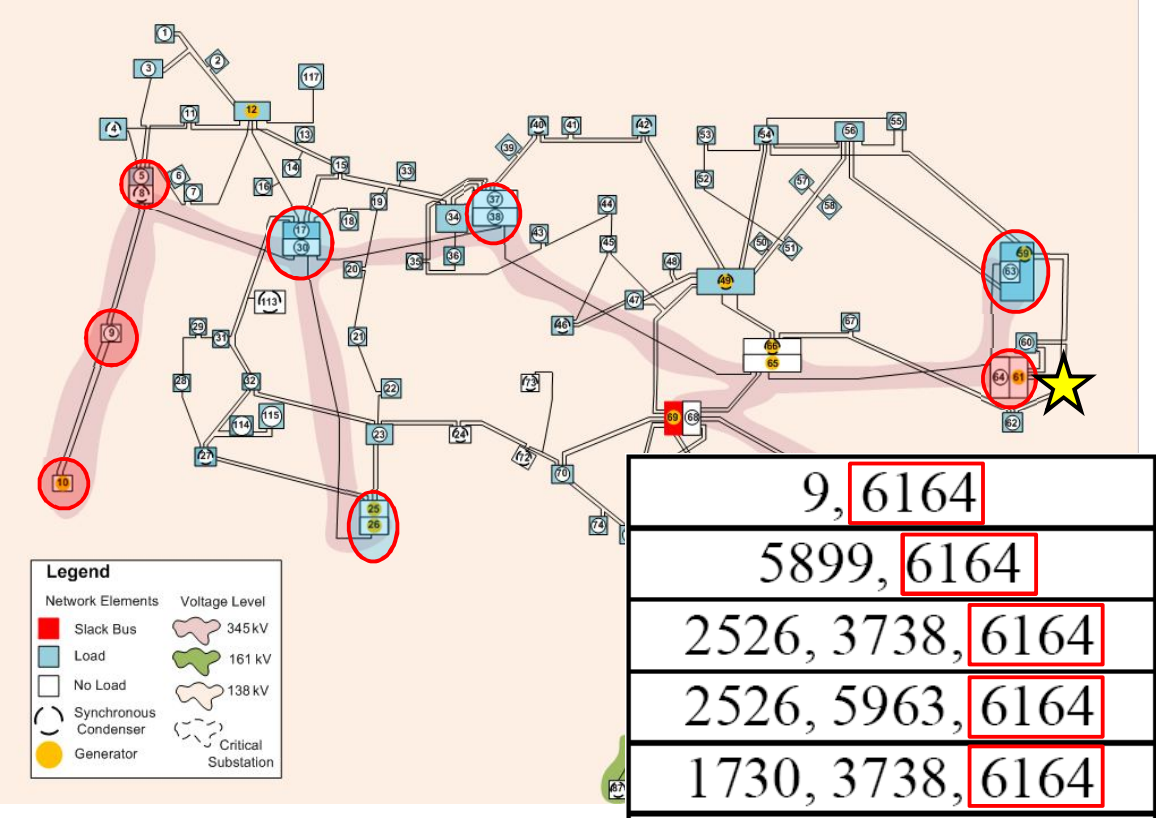
Detecting anomaly behaviors generated by multiple locations in IEEE-118 Bus System



Finding the most critical substations

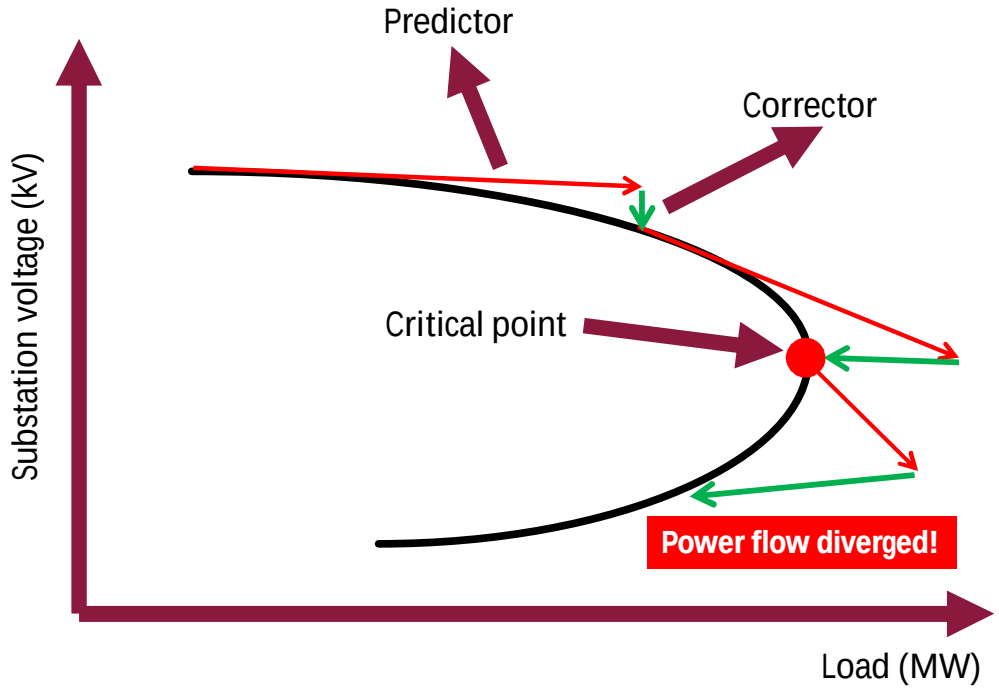


Finding critical scenarios of combinations



9, 6164
5899, 6164
2526, 3738, 6164
2526, 5963, 6164
1730, 3738, 6164

Inspired by Continuation Power Flow



Venkataramana Ajjarapu and Colin Christy, “The continuation power flow: A tool for steady-state voltage stability analysis,” IEEE Transactions on Power Systems, vol. 7, no. 1, pp. 416—423, Sep. 2015. <10.1109/59.141737>

M=14 and Simulation Results

- **Credible substation list from IEEE 30-bus system**
  - Substations [2, 4, 5, 6, 8, 10, 15, 16, 18, 19, 22, 23, 24, 28]

- **Findings:**
  - Critical list: Substations 9, 12, 25, 27
  - 105 combinations in priority-1 list; 16 combinations with highest impact.
  - 20 combinations in priority list-2
  - No new combination after $k > 9$
  - A total of 1293 combinations evaluated from 16383 scenarios

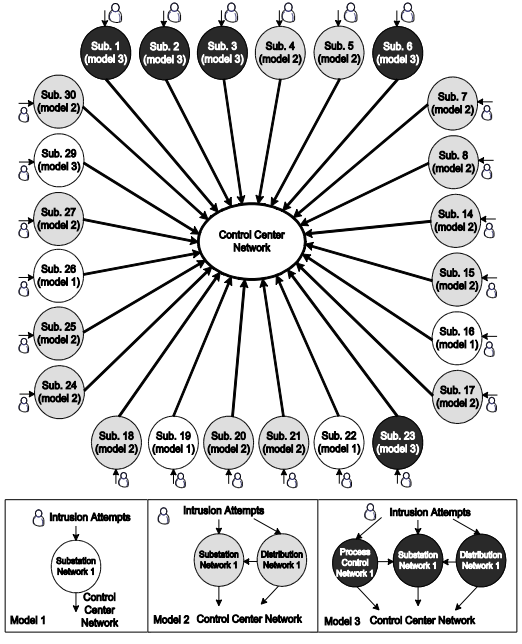
k	Total Comb.	Reduced New Comb.	Highest Impact
1	14	-	0
2	91	-	16
3	364	216	11
4	1001	338	6
5	2002	339	3
6	3003	208	0
7	3432	73	0
8	3003	13	0
9	2002	1	0
10	1001	0	0
11	364	0	0
12	91	0	0
13	14	0	0
14	1	0	0
sum	16383	1188	37

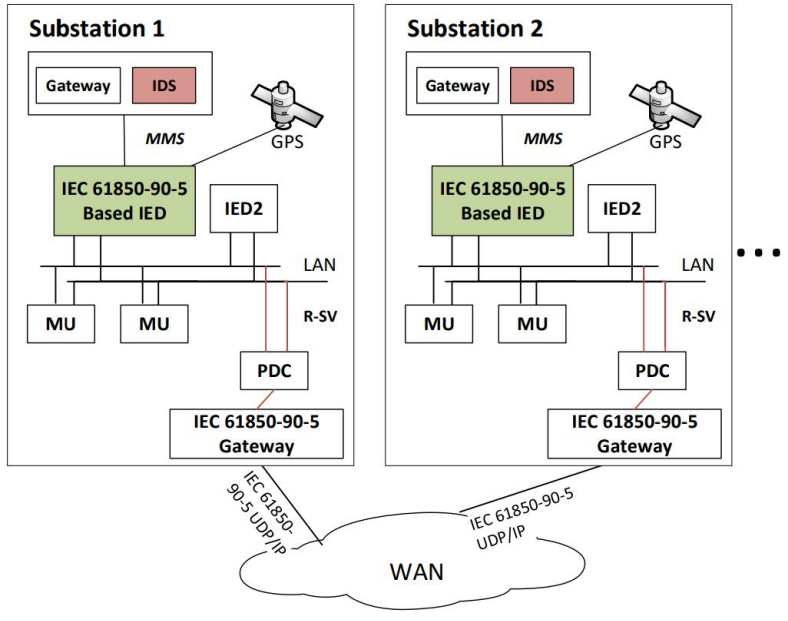
Rashiduzzaman Bulbul, Chee-Wooi Ten, and Andrew Ginter, "Cyber-Contingency Evaluation for Multiple Hypothesized Substation Outages," *Proc. 5th IEEE-PES Conference on Innovative Smart Grid Technologies*, Feb. 19-22, 2014, Washington, DC, USA.

We **MAY NOT have all successful/failures cases**, but we **CAN simulate all plausible outcomes**!

Hypothesized Outages for All Substations

Centralized SCADA Control to **Distributed Inter-Substation** Communication



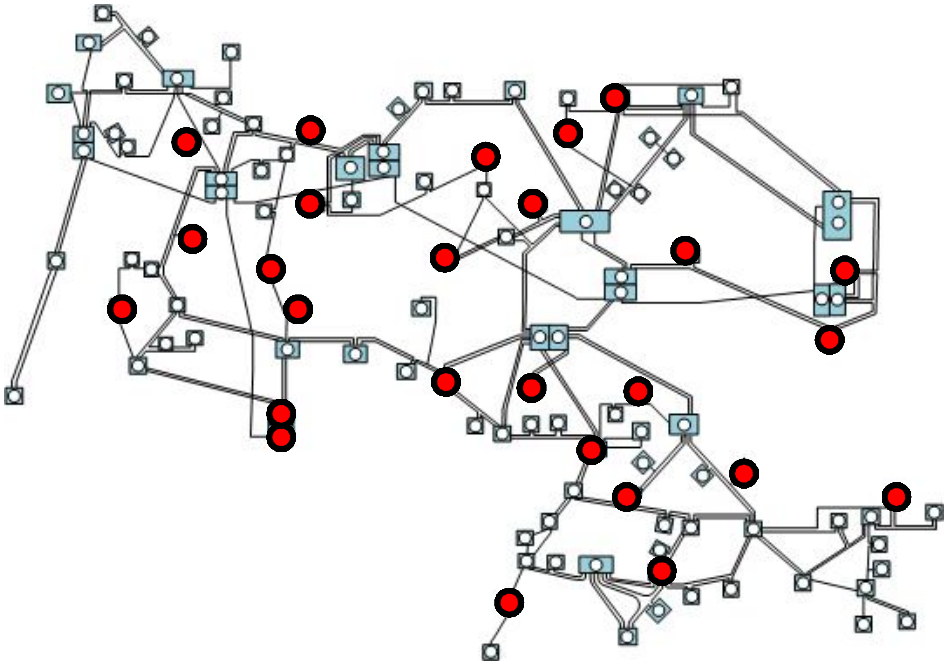


Chee-Wooi Ten, Chen-Ching Liu, and Manimaran Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836—1846, Nov. 2008. <10.1109/TPWRS.2008.2002298>

Ruoxi Zhu, Chen-Ching Liu, Junho Hong, and Jiankang Wang, "Intrusion Detection against MMS-based Measurement Attacks at Digital Substations." IEEE Access, Vol. 5, pp. 1240-1249, Dec. 2020.

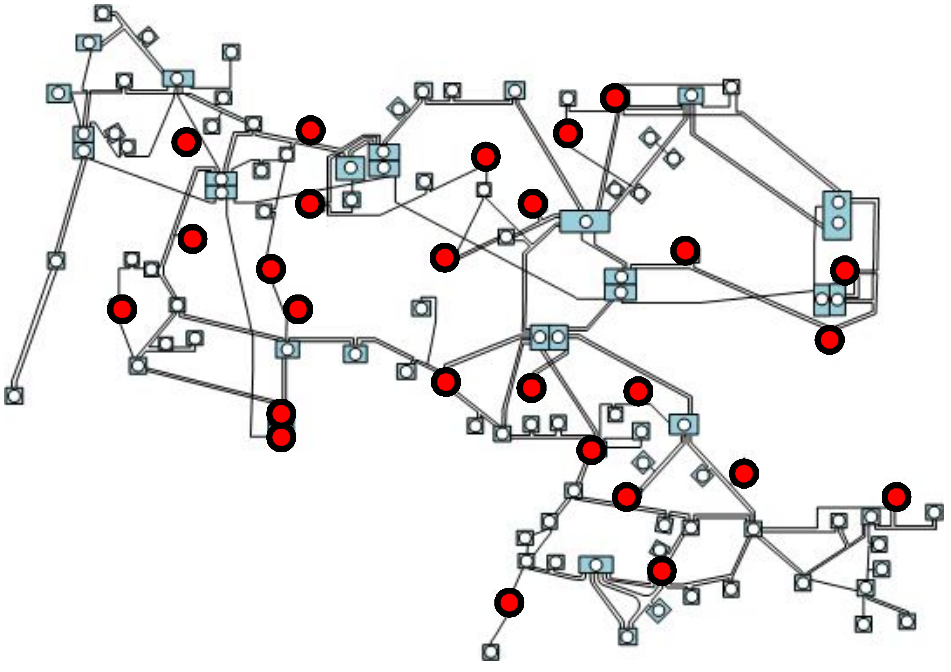
Coordinated Cyber-Physical Attacks

- Complexity of Combinatorial Evaluation
- **Intrusion attempts** and **successful intrusions** made no difference to control center – they are not informed at all!
- Thousands of intrusion attempts each day!

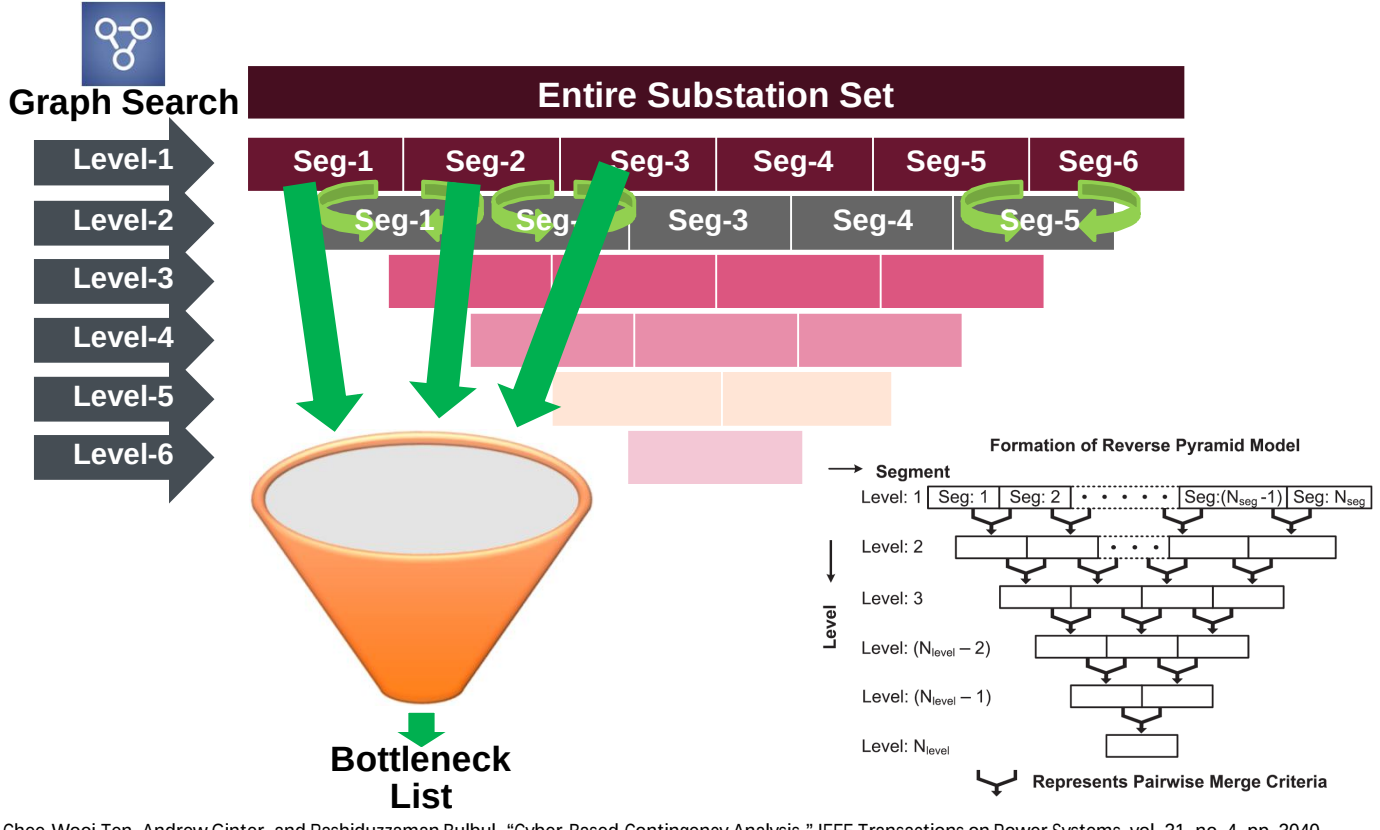


Coordinated Cyber-Physical Attacks

- Complexity of Combinatorial Evaluation
- **Intrusion attempts** and **successful intrusions** made no difference to control center – they are not informed at all!
- Thousands of intrusion attempts each day!

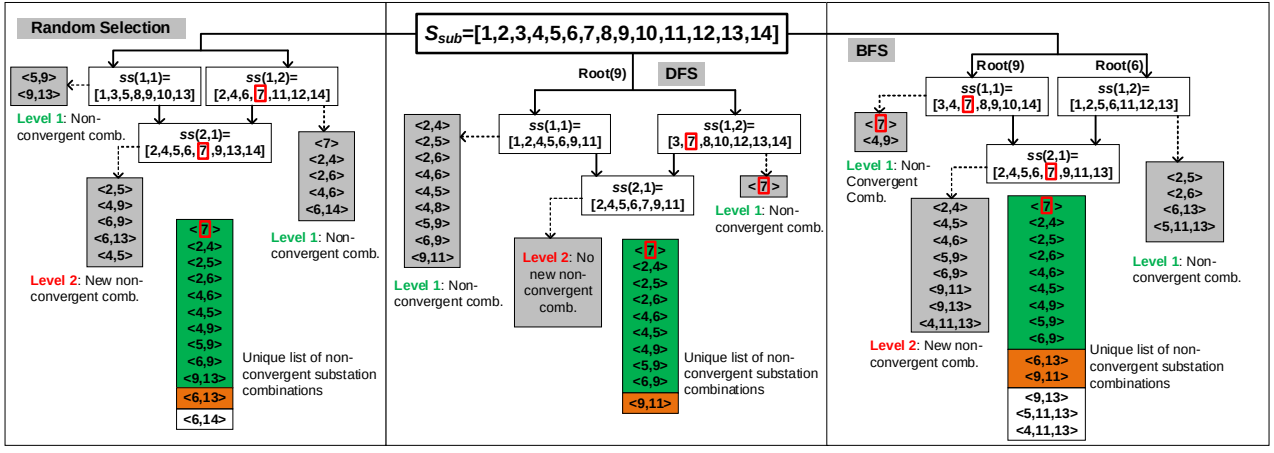


Formation of Reverse Pyramid Model (RPM)



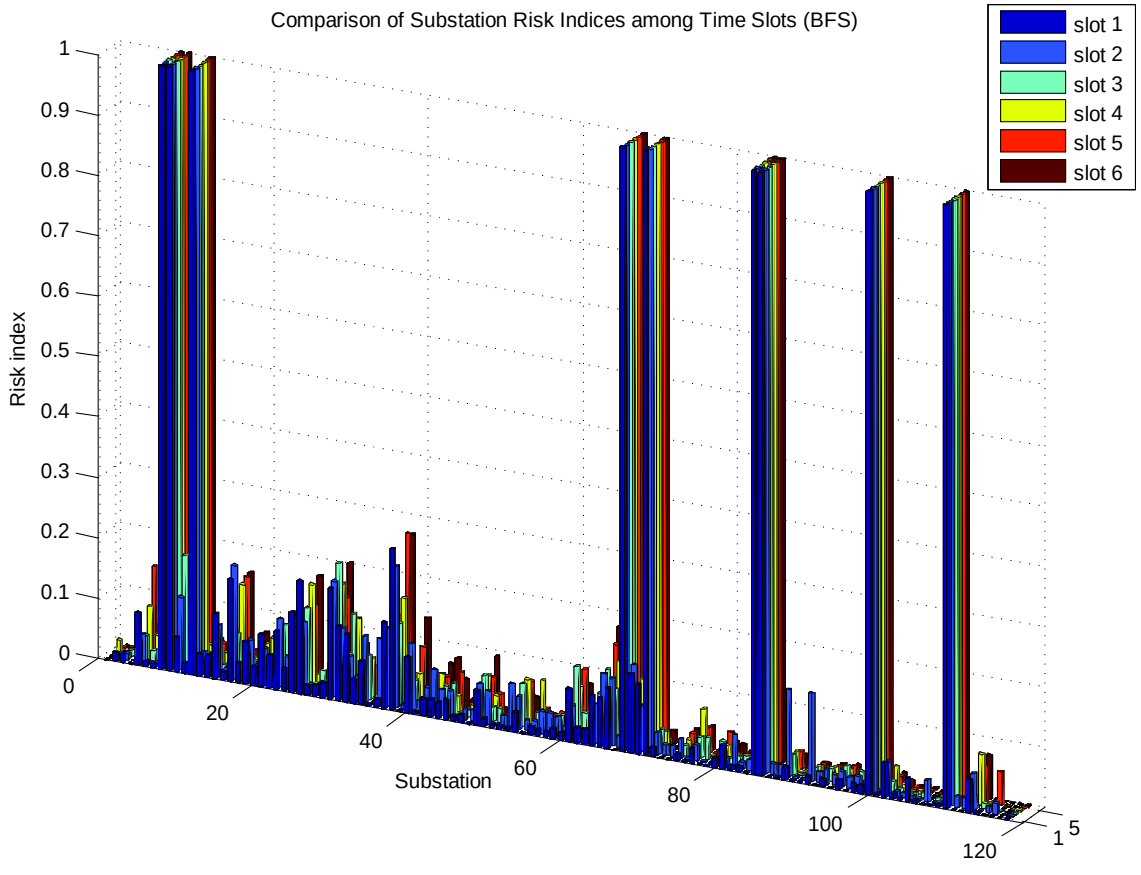
Chee-Wooi Ten, Andrew Ginter, and Rashiduzzaman Bulbul, "Cyber-Based Contingency Analysis," IEEE Transactions on Power Systems, vol. 31, no. 4, pp. 3040—3050, Sep. 2015. <10.1109/TPWRS.2015.2482364>

Segmentation Approaches on IEEE 14-Bus System

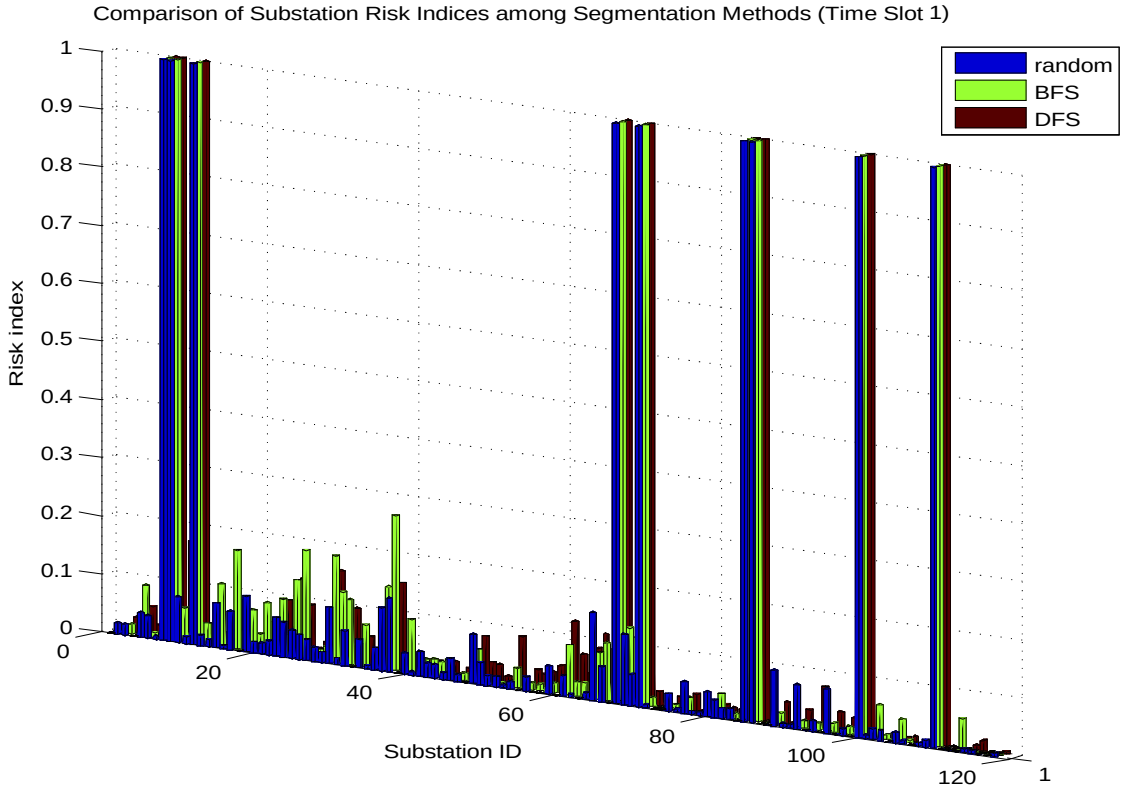


- Graph-based heuristic approaches
- 9 combinations are common (green zones)
- 1 or 2 combinations are common in two methods (orange zones)

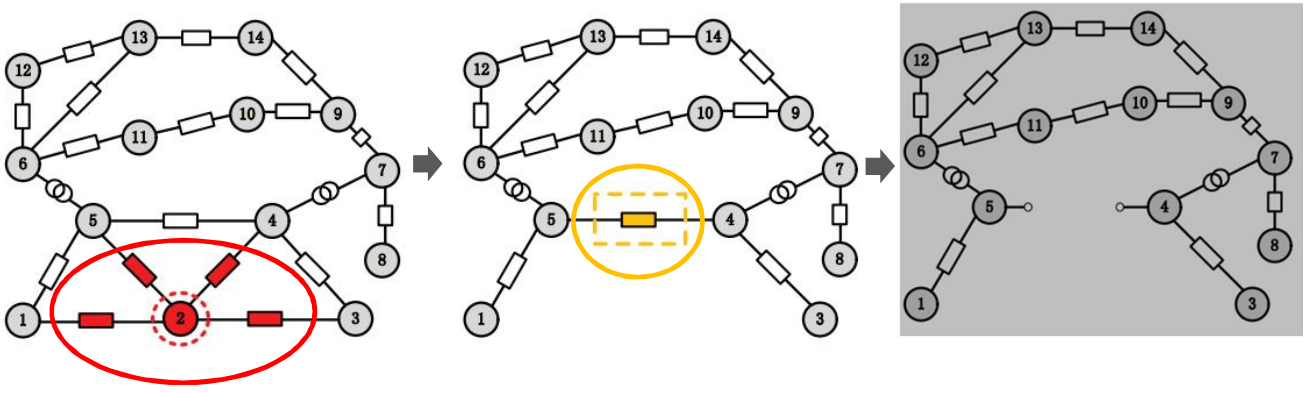
Risk Index on IEEE-118 Bus System



Comparison of Segmentation Approaches on IEEE 118-Bus System



Modeling the Disruptive Switching and Cascading Effects



(a) Initial topology of a substation under attack $G(V,E)$

(b) Overloaded line incurred from the switching attack G'(V',E')

(c) Cascading line outage under the same attack scenario G''(V',E'')

$$\underbrace{G(V,E)}_{\text{(a) Original } G} \xrightarrow[\text{cyberattack}]{\text{Switching}} \underbrace{V'(G') = V(G) \setminus V_k \subset S_{sub}}_{\text{(b) Hypothesized substations outages}} \xrightarrow[\text{overloading}]{\text{Potential}} \underbrace{E'(G'') = E(G') \setminus E_k \subset \mathcal{L}}_{\text{(c) Overloading outages}}$$

Zhiyuan Yang, Chee-Wooi Ten, and Andrew Ginter, "Extended Enumeration of Hypothesized Substations Outages Incorporating Implications of Overloading," To appear in IEEE Transactions on Smart Grid. <10.1109/TSG.2017.2728792>

Enumeration Model

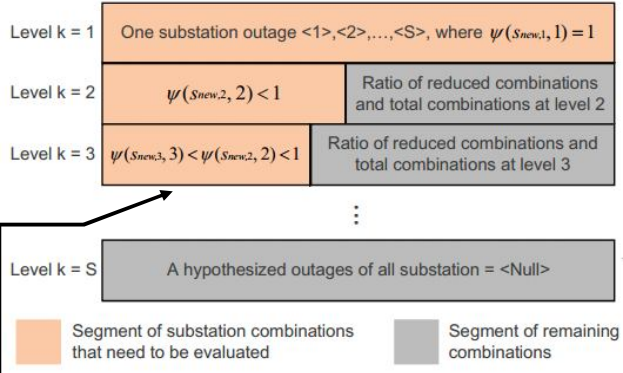
Enumeration from k = 1 to S' with decreasing ratio $\Psi(.)$

$$\psi(s_{new,k}, k) = \begin{cases} \frac{s_{new,1}}{\mathbf{C}_1^S} = 1.0, & k = 1 \\ \frac{s_{new,2}}{\mathbf{C}_2^S} < 1.0, & k = 2 \\ \frac{s_{new,k}}{\mathbf{C}_k^S} < \frac{s_{new,k-1}}{\mathbf{C}_{k-1}^S} < 1.0, & k \geq 3 \end{cases}$$

$$s_{new,k} = \left(\mathbf{C}_k^S - \chi\right)$$

where χ is the total reduction number that was extracted from the last level

$\mathbf{SS}_{failed}(k-1)$



At level k:

$$\mathbf{SS}_{failed}(k) = \mathbf{PF}_{failed}\left(G'(k)\right) \bigcup \mathbf{PF}_{failed}\left(G''(k)\right)$$

Summarize,

$$ss_{failed} = \mathbf{SS}_{failed}(1) \cup \mathbf{SS}_{failed}(2) \cup \cdots \mathbf{SS}_{failed}(S')$$

Where, $\mathbf{PF}_{failed}(\cdot) \in [0,1]$ es either a converged or diverged outcome, respectively.

Comparison of Segmentation Approaches on IEEE 118-Bus System

Incorporation of overloading consequences

$$\text{Condition\_A}: \left(|I_l| > |I_{p,l}|\right)$$

- $|I_l|$ The current flows through transmission line l
- $|I_{p,l}|$ Pickup value set on the transmission line l

$$\text{Condition\_B}: \left(\mathcal{L}_{\mathbf{pf}} > O_{limit,S}(\mathcal{L})\right)$$

- $\mathcal{L}_{\mathbf{PF}}$ The power flow through transmission line l
- $O_{limit,S}(\mathcal{L})$ The short-term thermal limits of transmission line l

$$\text{Condition\_C}: \left(\mathcal{L}_{\mathbf{pf}} > C_l\right) \bigwedge \left(O_{limit,L}(\mathcal{L}) < O(l,\tau)\right)$$

- $O(l,\tau)$ The accumulative heating power on the line l during time interval τ
- $O_{limit,L}$ The long-term thermal limits of transmission line l
- C_l The ampacity ratings of transmission line l

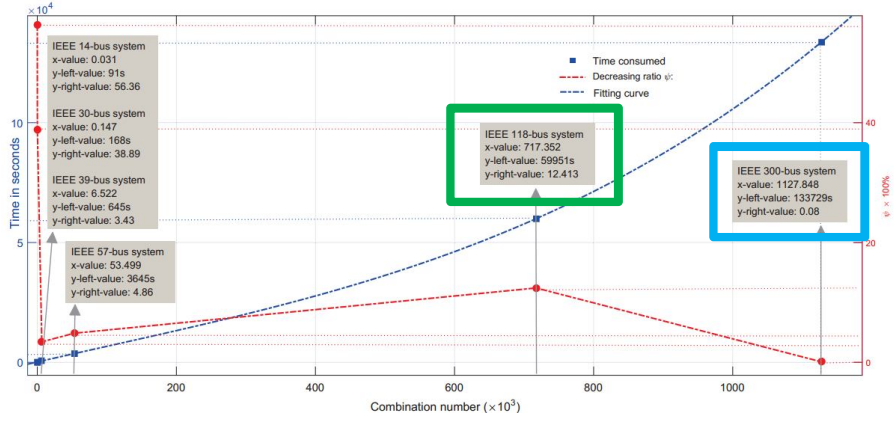
The “tripped signals” will be sent by the protective relays based on the criteria as follows

$$(\text{Cond.\_A} \bigvee \text{Cond.\_B} \bigvee \text{Cond.\_C}) \rightarrow l_{trip}.$$

Simulation Results

TABLE II: Summary of the results of IEEE test systems with implementation of overcurrent protection scheme

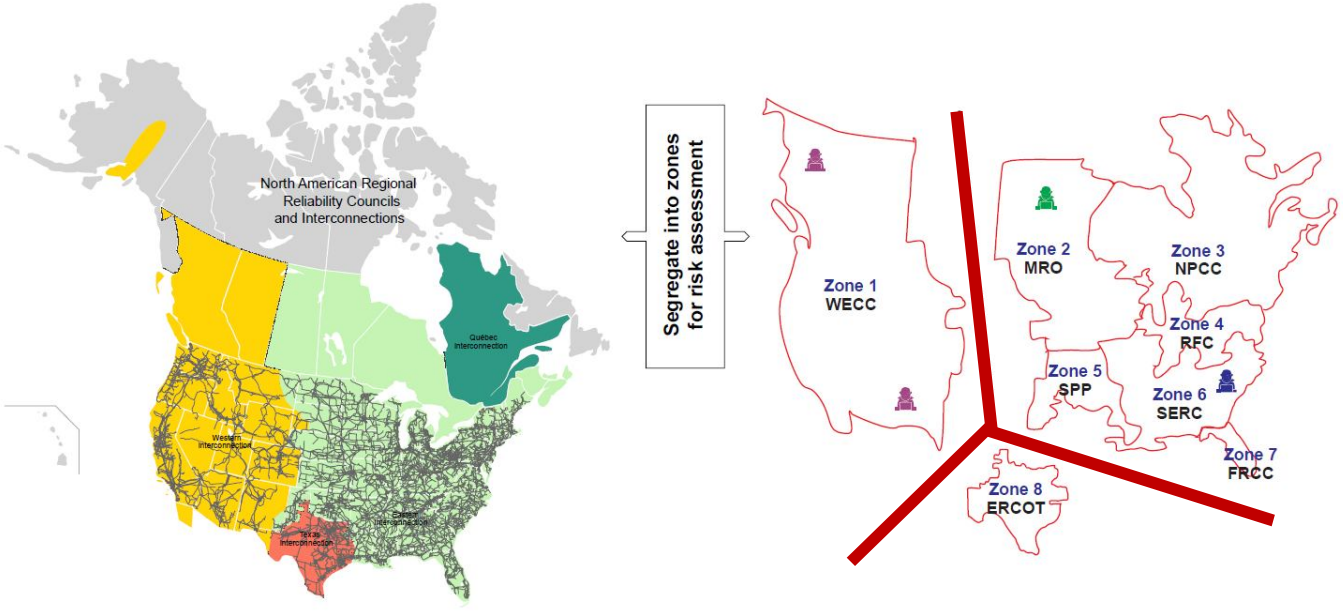
Cases #	k	# Total Comb. s_k	# Reduction χ	# New $s_{new,k}$	$\mathbf{PF}_{failed}$ = 1
14-bus	1	10	-	10	3
	2	45	24	25	1
30-bus	1	24	-	24	8
	2	276	156	120	5
	3	2,024	1,593	493	15
	4	10,626	9,354	1,272	17
	5	42,504	40,315	2,189	39
	6	134,596	132,172	2,424	59
39-bus	1	27	-	27	11
	2	351	231	120	30
57-bus	1	43	-	43	18
	2	903	603	300	7
	3	12,341	10,197	2,144	10
	4	123,410	112,594	10,816	21
	5	962,598	922,402	40,196	39
118-bus	1	109	-	109	42
	2	5,886	3,675	2,211	44
	3	209,934	164,673	45,261	347
	4	5,563,251	4,893,480	669,771	3,717
300-bus	1	176	-	176	112
	2	15,400	13,384	2,016	82
	3	893,200	856,221	36,979	274
	4	38,630,900	38,137,765	493,135	2,099
	5	1,328,902,960	1,328,307,418	595,542	111,552



For IEEE 118-bus system, 717,353 cases are evaluated, which takes approximate 16 hours to complete calculation

In IEEE 300-bus system, 1,127,848 cases are evaluated, which takes approximate 37 hours to complete calculation

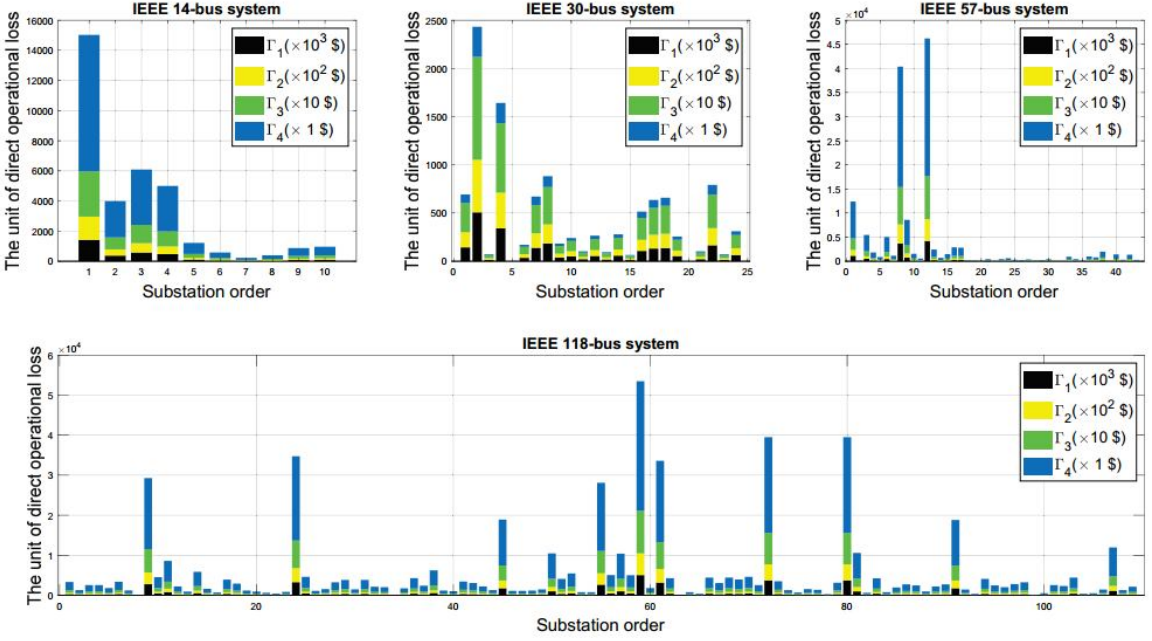
North America’s Major Interconnection and Zone Segregation



- Involved assessment of risks between zones in an interconnection with respect to technology investment and mitigation of risks and insurance policy adjustment

Direct Operational Losses in Financial Term

- Intrusion anomalies and security event extraction from cyber systems
- Relationship between pre-disturbance (prior execution of switching attacks)
- During power outage on locational marginal pricing
- Restoration efforts and time



Preliminary results Based on Claim Size and Premium Policy

The ruin probability $\varphi(u)$ for the initial risk reserve u is fundamentally defined as:

$$\varphi(u) = Pr\{M > u\} = 1 - F_M(u)$$

$M = L_1 + L_2 + \cdots + L_n + \cdots + L_N$, is defined as maximal aggregate loss

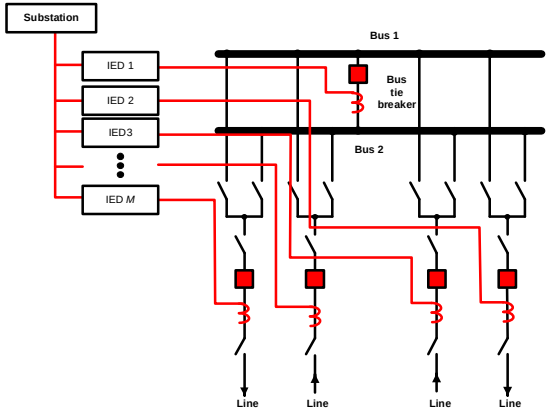
$F_M(u)$ represents the cumulative density function (CDF)

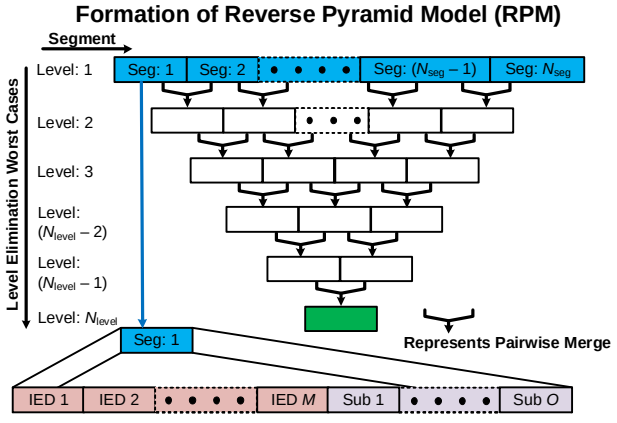
Each random variable L_n represents claimed loss for insurance company. It is assumed that the number of claims N follows a geometric distribution, satisfying: $Pr\{N = n\} = (1 - q)q^n$, where $q = 1/(1 + \theta)$

Results of Ruin Probabilities and Premium Policy												
IEEE 14-bus system (10 substations)			IEEE 30-bus system (24 substations)			IEEE 57-bus system (43 substations)			IEEE 118-bus system (109 substations)		
initial reserve	theta	Ruin Prob.	initial reserve	theta	Ruin Prob.	initial reserve	theta	Ruin Prob.	initial reserve	theta	Ruin Prob.
0		1.586E-03	0		6.376E-04	0		3.971E-04	0		1.016E-03
5	100	5.276E-05	5	100	3.254E-06	5	100	3.971E-04	5	100	6.977E-06
10		7.250E-05	10		3.628E-06	10		3.404E-08	10		5.987E-06
System Constants	lambda	0.0067	System Constants	lambda	0.0157	System Constants	lambda	0.0289	System Constants	lambda	0.0724
	h	0.5		h	0.5		h	0.5		h	0.5
Mean Claim Size	VOLL	$ 4,467,000	Mean Claim Size	VOLL	$ 3,166,400	Mean Claim Size	VOLL	$ 19,895,000	Mean Claim Size	VOLL	$ 139,010,000
	DC	$ 480,170		DC	$ 340,360		DC	$ 2,138,600		DC	$ 14,943,000
	AREP	$ 93,851		AREP	$ 66,525		AREP	$ 418,000		AREP	$ 2,920,600
	LMP	$ 28,373		LMP	$ 1,954		LMP	$ 134,920		LMP	$ 891,590
Feasible Premium Policy	VOLL	$ 3,022,819	Feasible premium policy	VOLL	$ 5,020,960	Feasible premium policy	VOLL	$ 58,071,516	Feasible premium policy	VOLL	$ 1,016,496,724
	DC	$ 324,931		DC	$ 539,709		DC	$ 6,242,360		DC	$ 109,269,193
	AREP	$ 63,509		AREP	$ 105,489		AREP	$ 1,220,100		AREP	$ 21,356,595
	LMP	$ 19,200		LMP	$ 3,098		LMP	$ 393,818		LMP	$ 6,519,663

Zhiyuan Yang,Yun Liu, Meghan Campbell, Chee-Wooi Ten, Yeonwoo Rho, Lingfeng Wang, and Wei Wei, "Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations," IEEE Access, vol. 8, pp. 78890-78900, Apr. 2020.

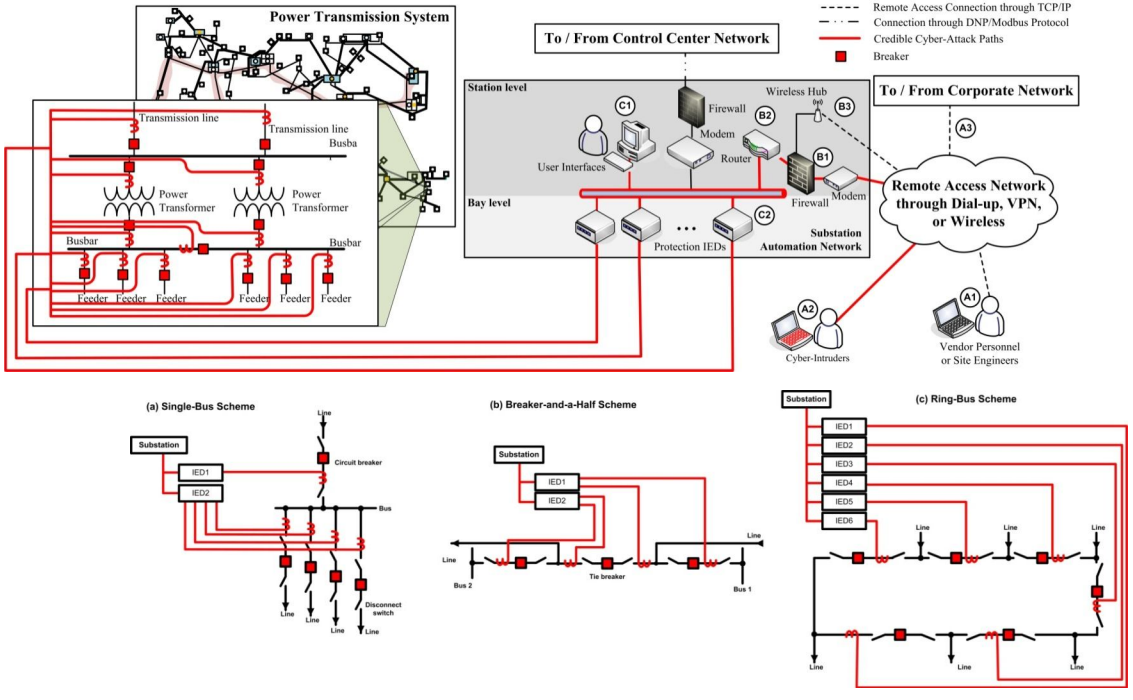
Combinatorial Extensions to Hypothesized IED Outages, Control Areas, etc.





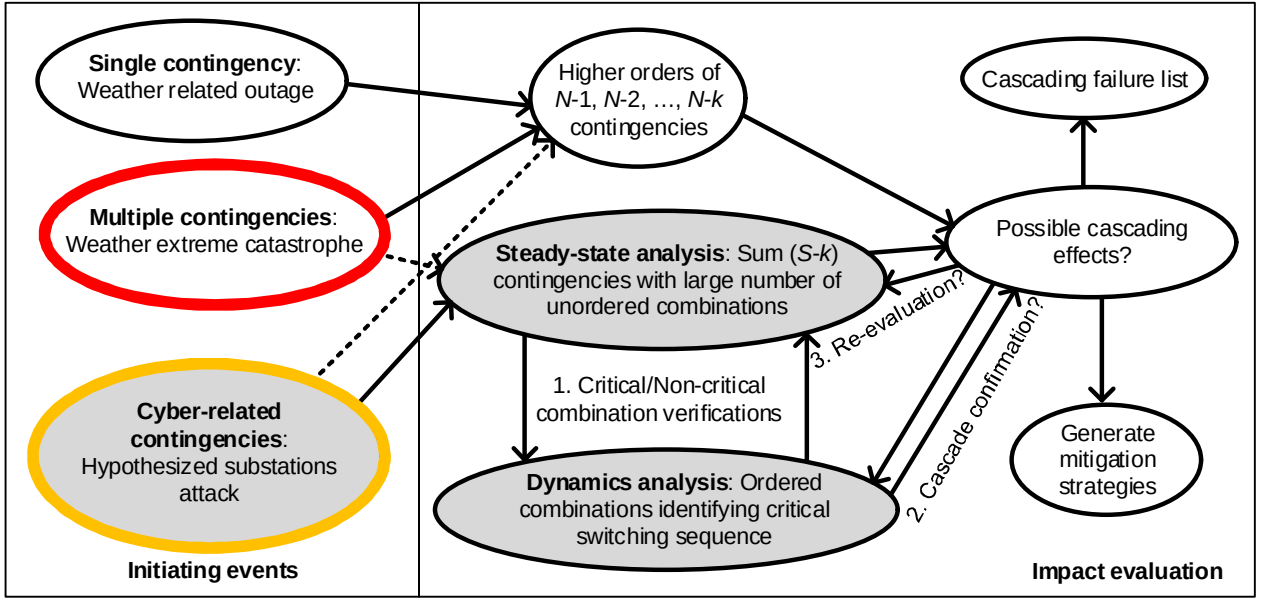
- ❑ Exhaustive enumeration with hypothesized IED outages
- ❑ Extension to combination of control area outage
- ❑ Permutation of switching sequence and verification of power flow diverged with dynamic and stability simulation

Exploring the Details of Substation Topology



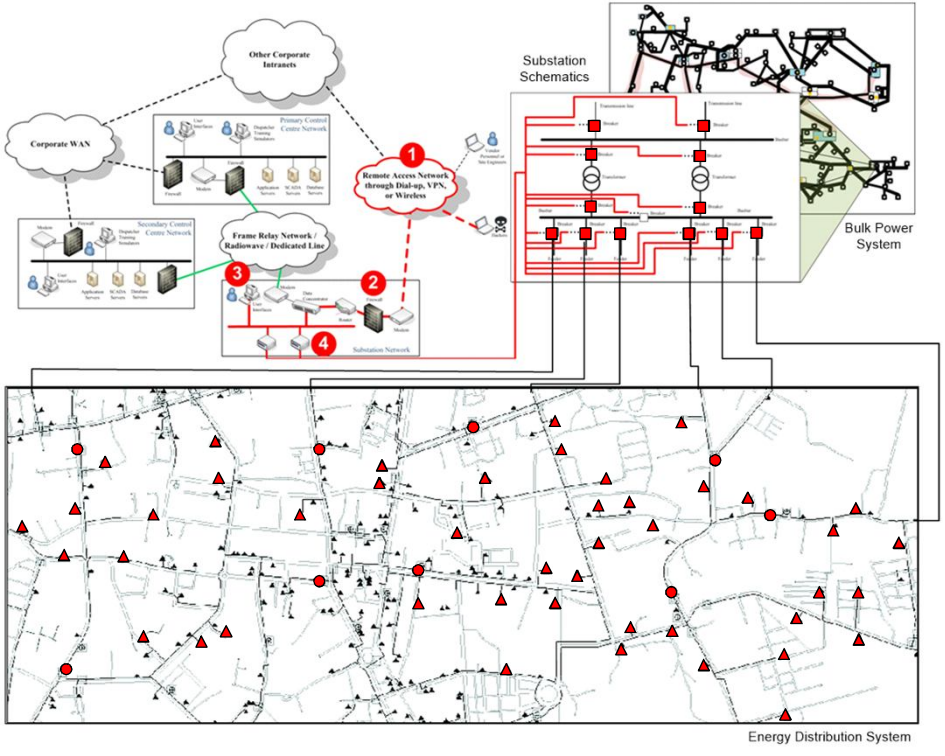
- Permutations of switching sequence that will cause maximum damage to system instability.

Metric Enhancement, Verification, Confirmation, Re-evaluation Using Steady-State and Dynamics Approaches



Chee-Wooi Ten, Koji Yamashita, Zhiyuan Yang, Athanasios Vasilakos, and Andrew Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4405—4425, Sep. 2018. <10.1109/TSG.2017.2656068>

Interdependencies Between Transmission and Distribution Circuits

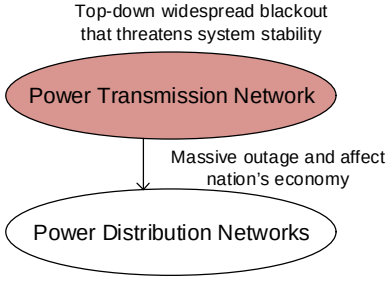


❑ Details of geographic information system (GIS)

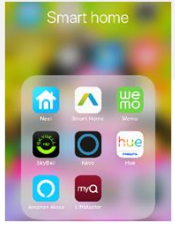
Research Problems:

- Cyber-physical Modeling
- Altered Control States (Safety issues)
- Data Validation against Cyber-Tampering
- Mitigation Strategies
- Resilience development

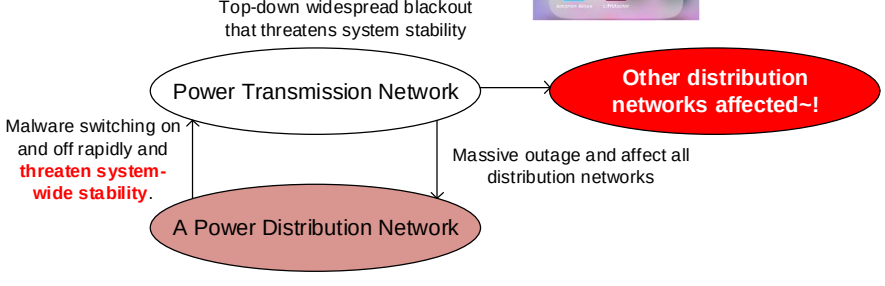
Rethinking about the Future Plausible Scenarios



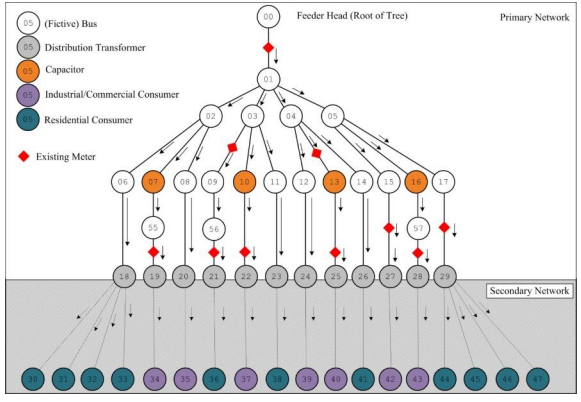
- The current mentality for cybersecurity issues that start at SCADA-level centralized framework on bulk power transmission, distribution, and generation
- **1000+ MW scale**



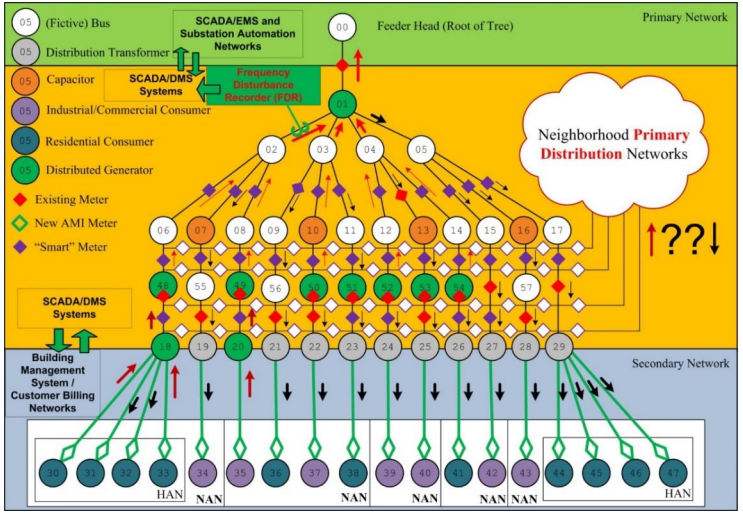
- Ubiquitous controllable IP-based sensors may be infected with malware…
- **1,000,000 customers would translate 1kW/energy user** to **1,000+MW scale**



Future Challenges – Collaborative Research



- Today's distribution grid topology
- Tomorrow's technology and future trend of Electrical Distribution Network



- More sensors to be deployed, more controllable devices…
- More possibilities to reconfigure!