Strategic Investment Planning for Cyberinfrastructure

Chee-Wooi Ten
Michigan Technological University
ten@mtu.edu

CIResilience
Interdependability – Reconfigurability – Sustainability

NSF

U.S. DEPARTMENT OF ENERGY

PSERC

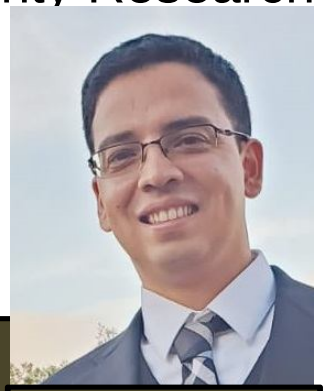
PSERC Webinar, Jan. 25, 2022, Tuesday, 2:00 pm

Acknowledgment of Research Contribution (Thesis/Dissertation) for Cyber-Physical ***Power*** System Security Research since 2010

Dr. Koji Yamashita

Bhairavi Pandya

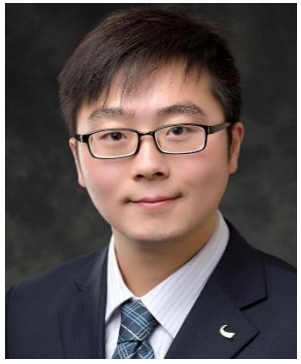
Dr. Yonghe Guo



Dr. Diego Aponte Roa

Dr. Chee-Wooi Ten

Anurag Nagpure



Dr. Yachen Tang

Rashiduzzaman Bulbul

Dr. Zhiyuan Yang

Pingal Sapkota

Nathan S. Fettinger

Research Experiences for Undergraduates (REUs)

Charlie Ciuk

Tyler Sommer

Hillori (Mitchell) Weimer

Brent Nix

Giovana Fenocchio Azzi

Presentation Outline

1. Grid operation
2. Supply chain
3. Emerging security technologies

Grid Operation

Power Control Centers

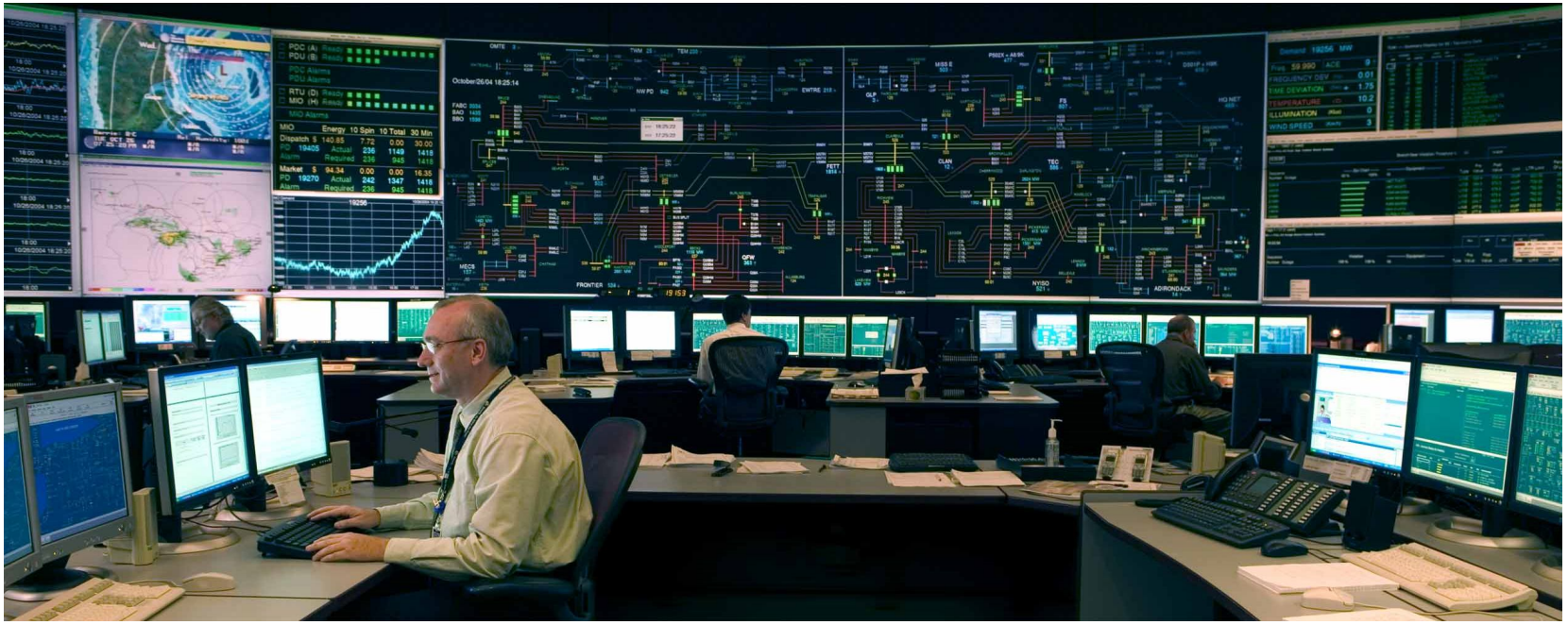


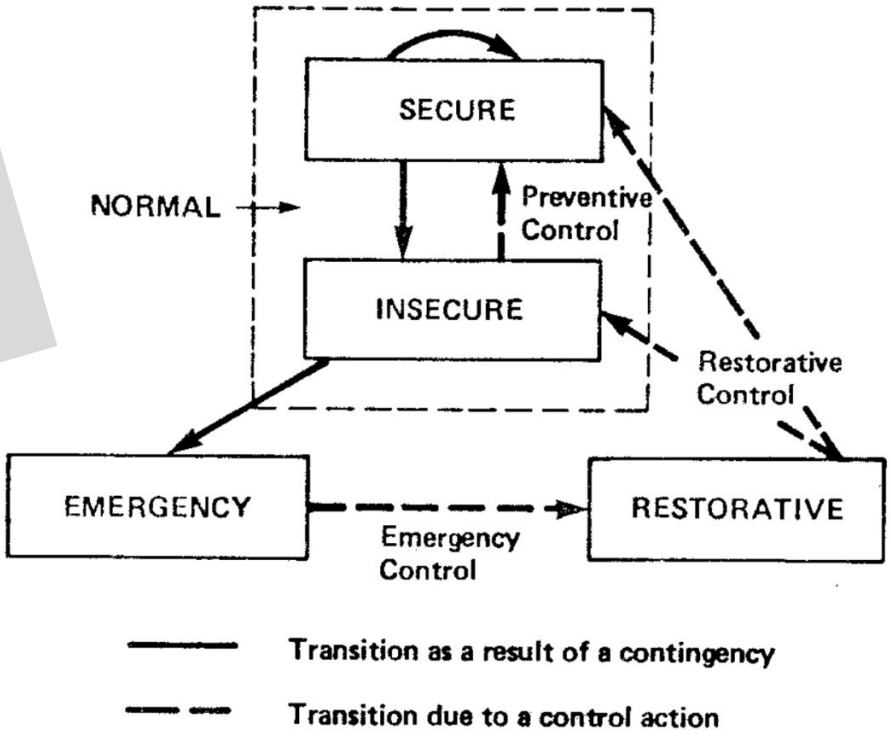
Photo Courtesy: http://www.temetprotection.com.ar/temet_advanced_shelter_control_system.html

- Supervisory Control and Data Acquisition (SCADA)
  - Data acquisition – analog (P, Q, V, etc.) and digital (switch status) measurements
  - **Alarms are derived** from these measurements over given time
  - Preventive and remedial controls

- Complete information of the physical health of a power system under a utility's grid territory

Security State Transitions

Classic old look on the figure in journal published in 1967

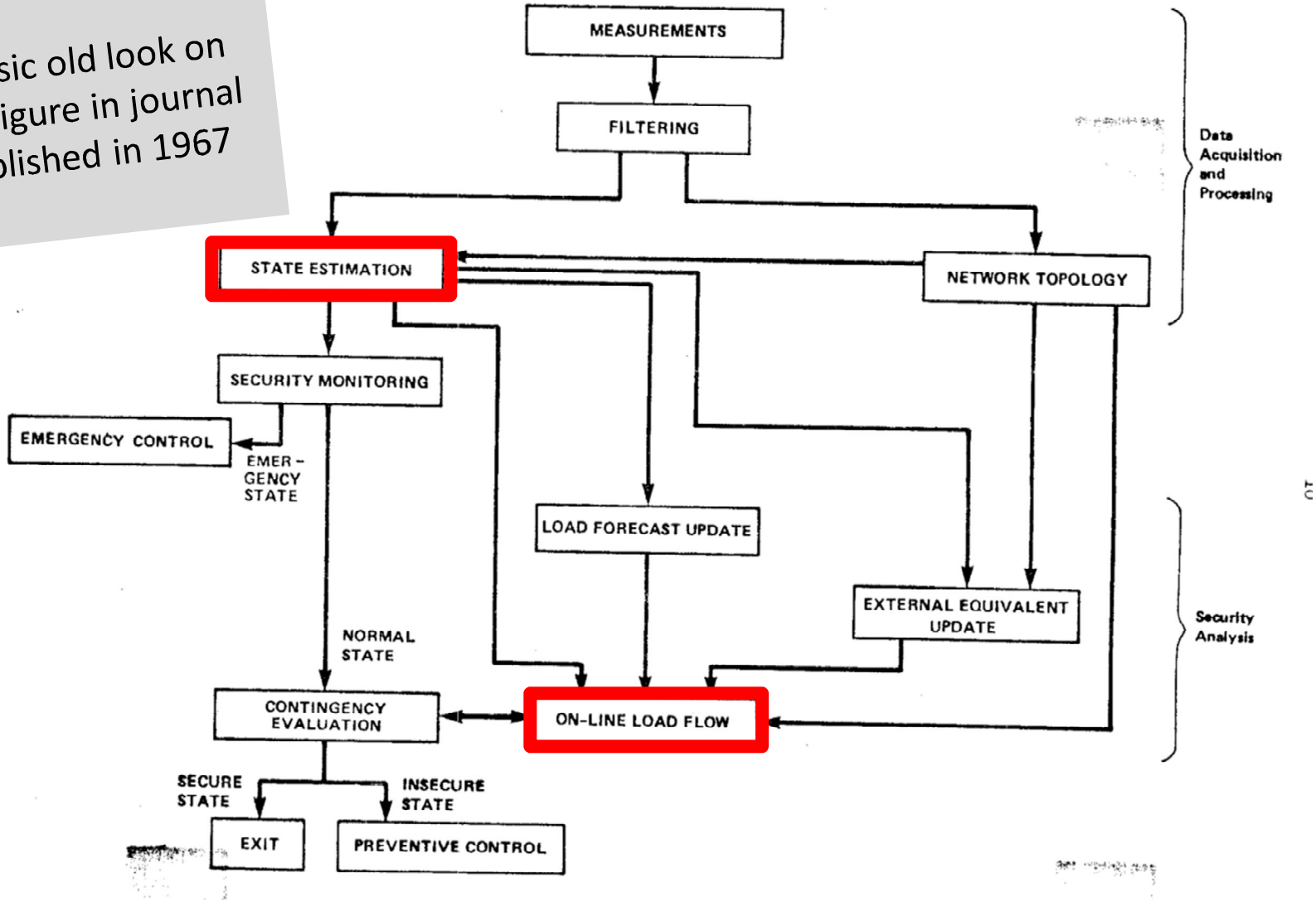


- Power system operating states and the associated state transitions due to CONTINGENCIES and CONTROL functions

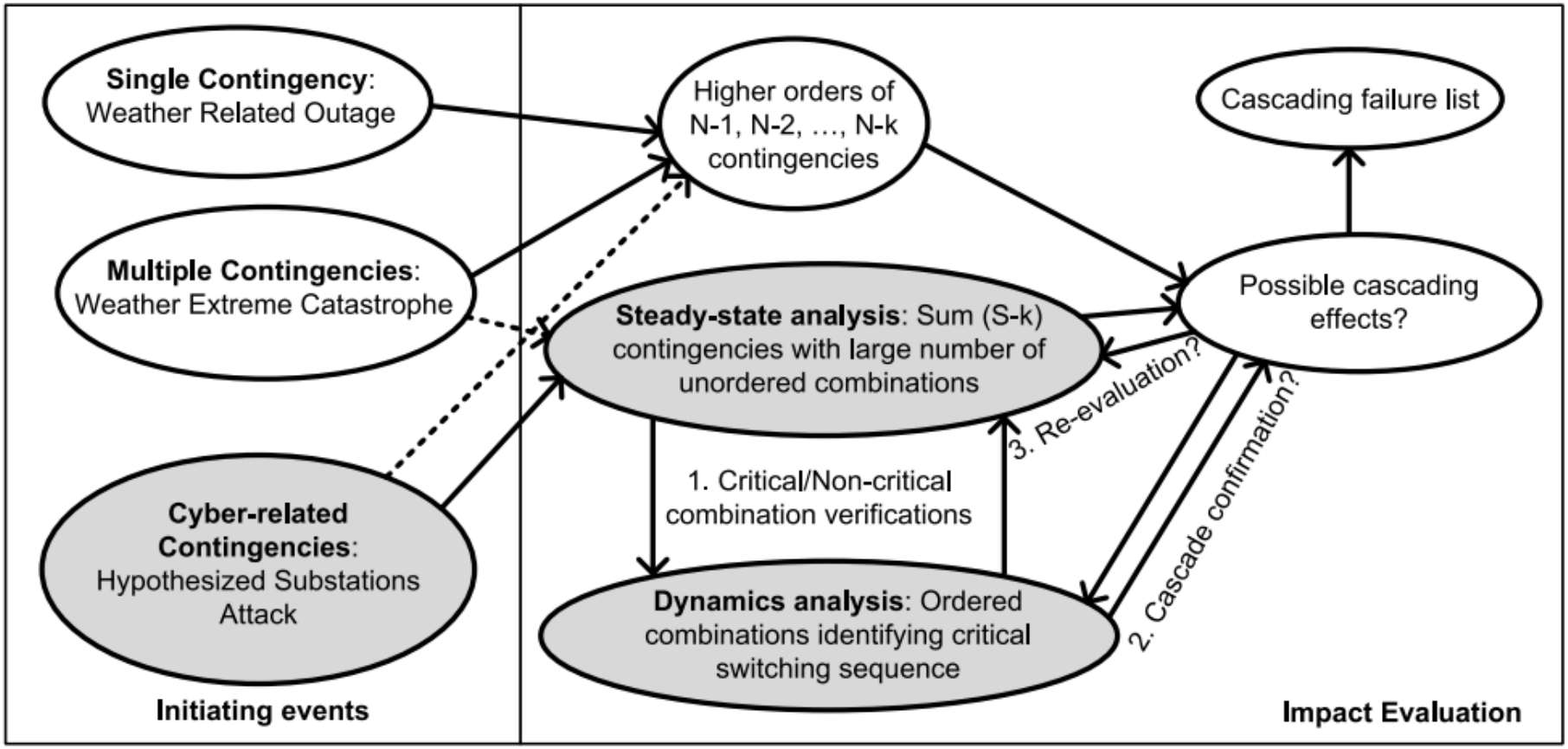
- Thomas E. Dy Liacco, "The Adaptive Reliability Control System," *IEEE Transactions on Power Apparatus and Systems*, Vol. PAS-86, No. 5, May 1967.

Centralized Security Control Functions

Classic old look on the figure in journal published in 1967

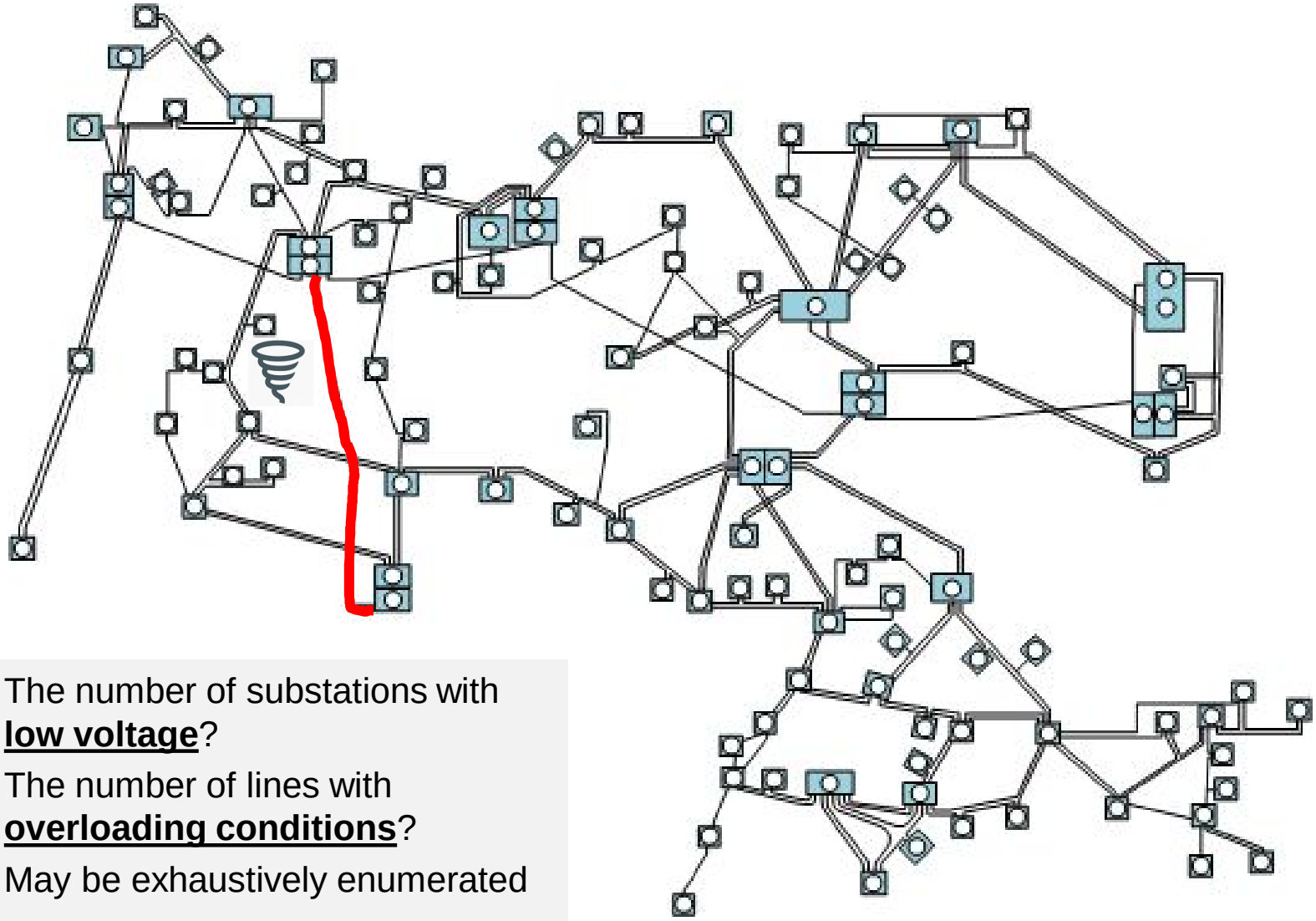


Initiating Events and Grid-Wide Impacts



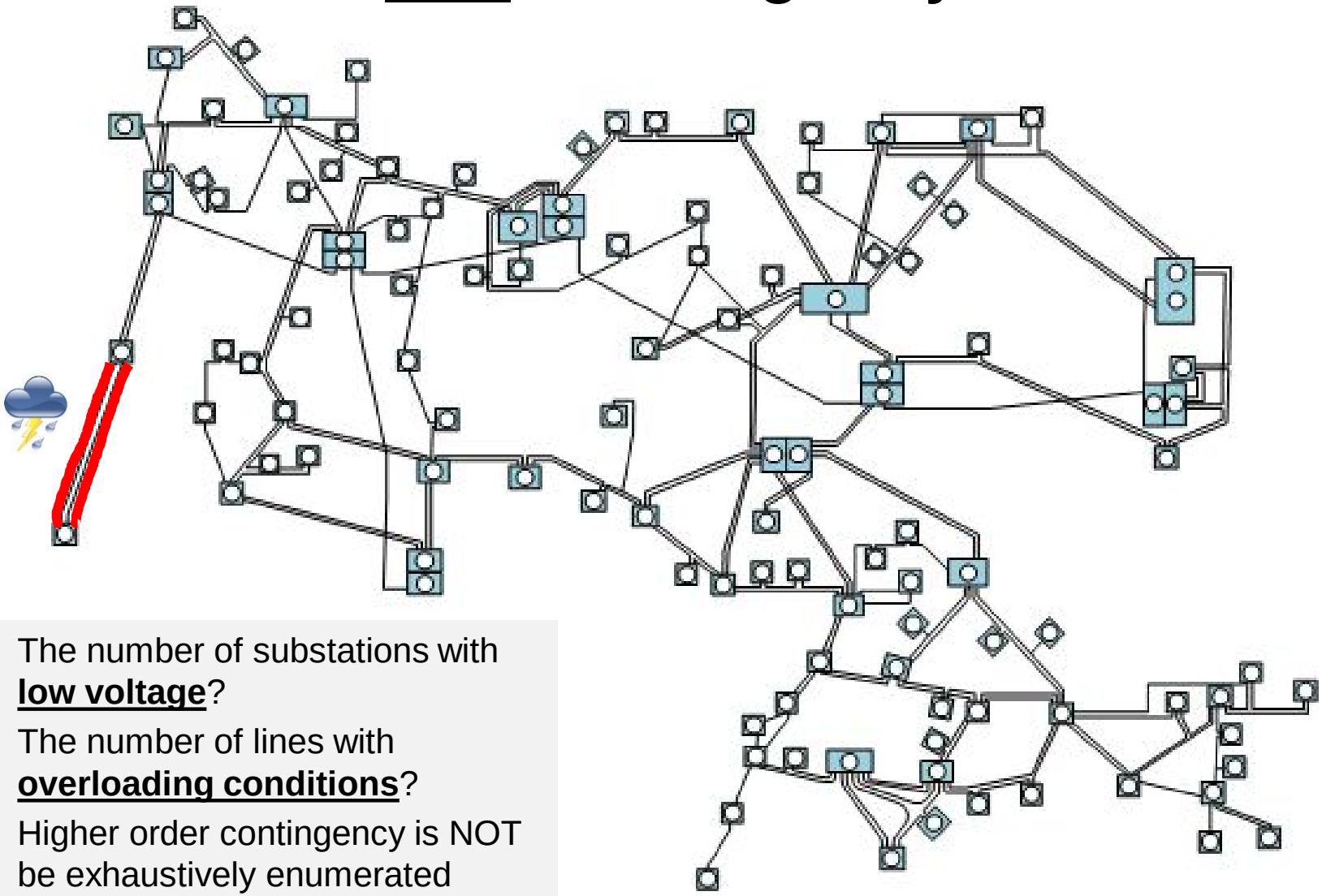
Chee-Wooi Ten, Koji Yamashita, Zhiyuan Yang, Athanasios Vasilakos, and Andrew Ginter, "Impact Assessment of Hypothesized Cyberattacks on Interconnected Bulk Power Systems," IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4405—4425, Sep. 2018. <10.1109/TSG.2017.2656068>

Traditional Power System **Security**: N-1 Contingency



- The number of substations with **low voltage**?
- The number of lines with **overloading conditions**?
- May be exhaustively enumerated

N-2 Contingency



- The number of substations with **low voltage**?
- The number of lines with **overloading conditions**?
- Higher order contingency is NOT be exhaustively enumerated

Supply Chain

Tens of Thousands of Electrical Substations

- High voltage (200kV, 345 kV, 500kV, 765kV…)
- Complex process to commissioning a substation and automation
- Stringent compliance and long process

Substation Switchgear and Automation

Circuit Breaker

Substation Computer

Transmission lines

Disconnector

Digital Relay

- 3-phase circuits
- Transmission/distribution utilities
- Long distance power transfer
- Long process to commission a substation
- Research thrusts: Power Systems Modeling, Power Delivery and Automation

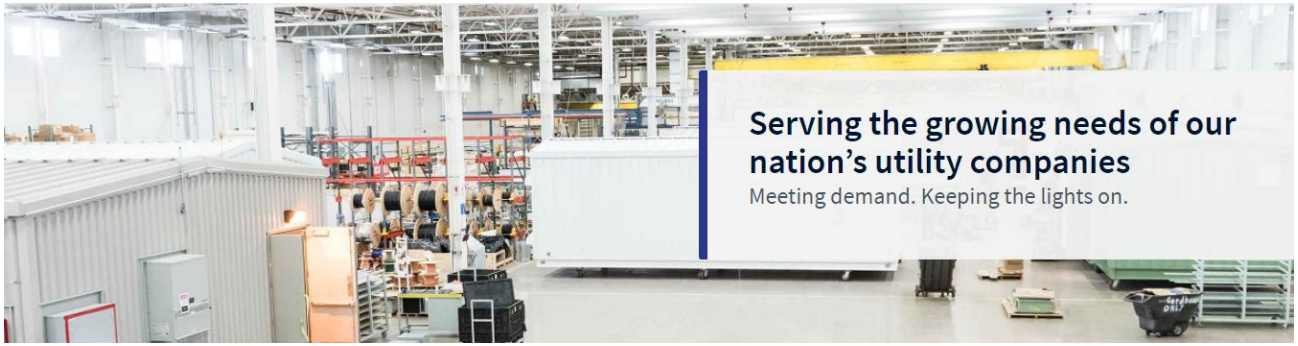
Relaying Framework

- Electromechanical Relay
  - Malfunction
  - Misoperation
  - Permissive relaying scheme
  - Zone 3 backup
- Digital Relays
  - New relays are all microprocessor-based
  - Relay settings can be altered leading to malfunction and misoperation

Our Community's Industry Constituent

SYSTEMS CONTROL

TURNKEY SOLUTIONS EQUIPMENT ENCLOSURES CONTROL & RELAY PANELS ENGINEERING SERVICES



EQUIPMENT ENCLOSURES

We have the capabilities to design Equipment Enclosures to your unique specifications for a truly customized solution.

CONTROL & RELAY PANELS

At Systems Control, our control and relay panels are custom-designed and built to meet your exact specifications.

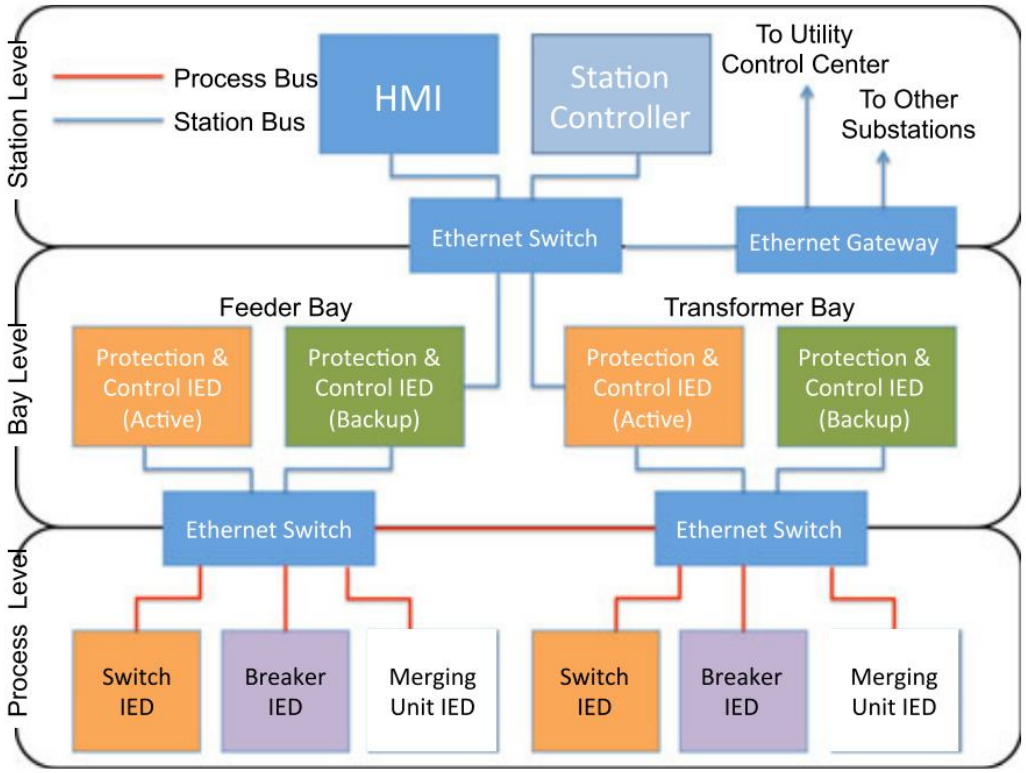
ENGINEERING SERVICES

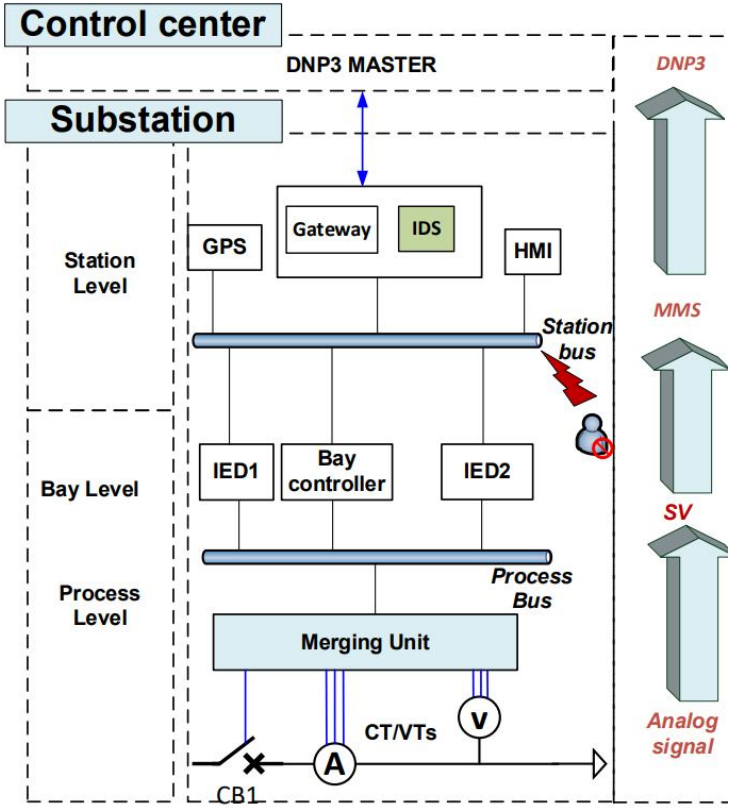
Our design and engineering team is designed to supplement your core engineering team across all disciplines.

- ❑ Substation automation and solutions
- ❑ Tradition to hire our engineering students
- ❑ Tens of thousands of Substations in North America will transition to IP-based substations
- ❑ Templates

Michigan Tech

IEC61850 Standard for Substation Automation and Attack Vectors/Paths

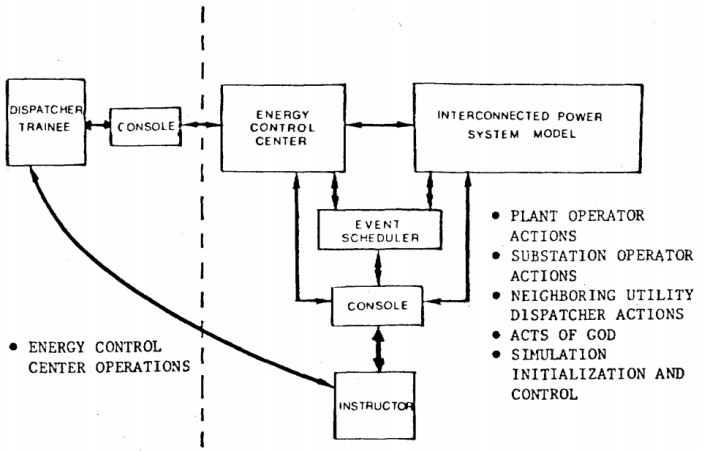


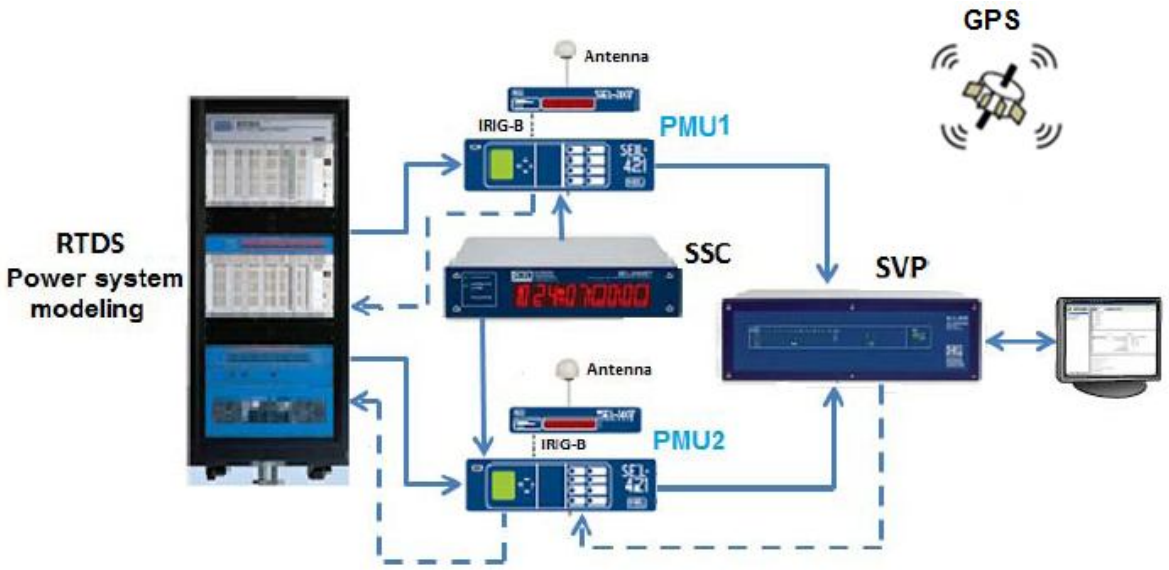


Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward Threat of Implementation Attacks on Substation Security: Case Study on Fault Detection and Isolation," IEEE Trans. Ind. Inf., Vol. 14, No. 6, Jun. 2018.

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.

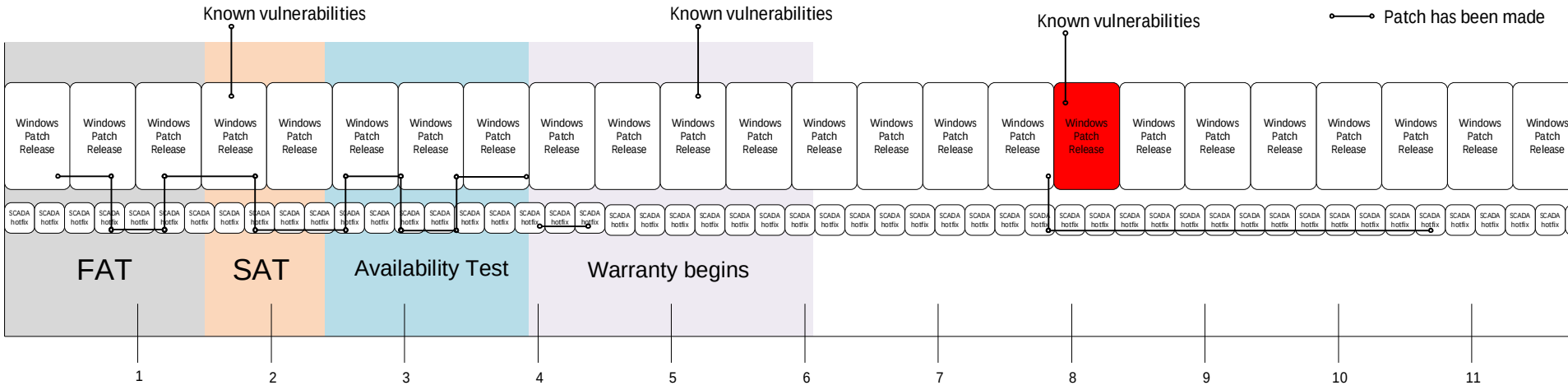
Dispatcher Training Simulators (DTS) vs. Real-Time Digital Simulator (RTDS) to **Faster Than Real Time**. Then **Digital Twin**





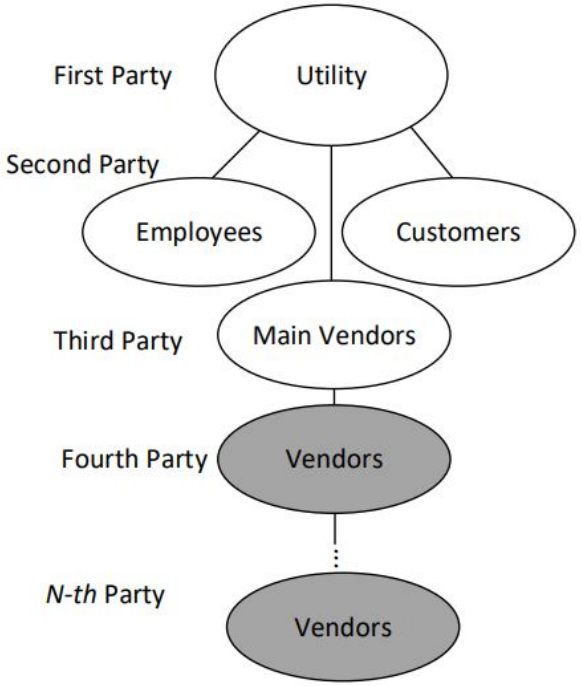
- ❑ Computing advancement (both software and hardware performance)
- ❑ Higher data resolutions
- ❑ Mimic more real-world environment with dynamic models (power flow is a steady-state model)
- ❑ PMU, RTU, legacy system, fault diagnosis
- ❑ Training operators / dispatchers to be more decisive based on information observed.

Long process to system acceptance tests

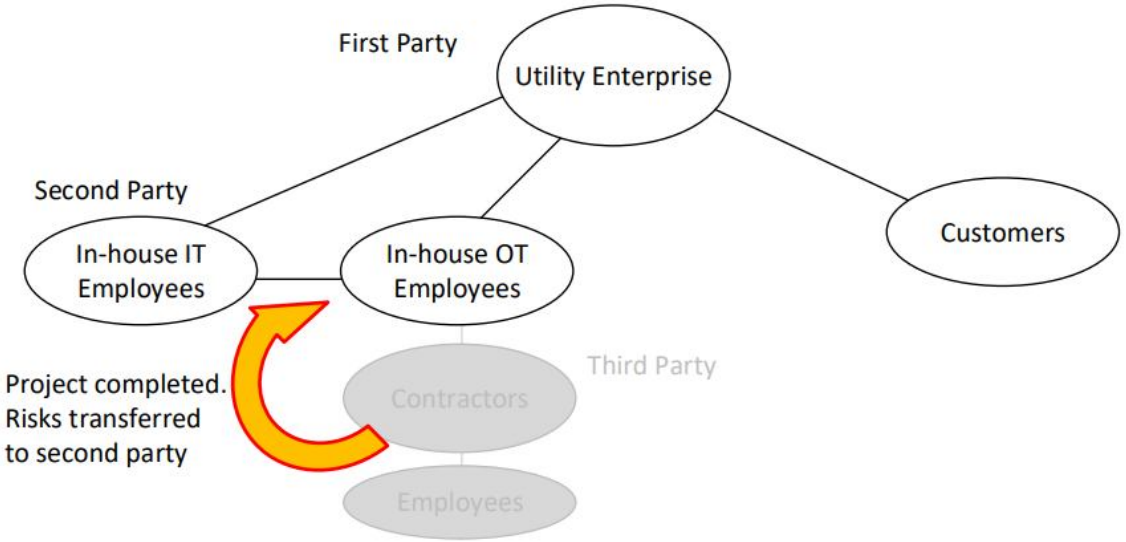


- Risk profiling should be tightly-coupled with software system installation/updates
- Zero-day vulnerabilities on deployed system
- Breaching log files would contaminate the credibility of electronic evidence
- Storing the security events in a more trustworthy location increases the effectiveness of logging and accountability where all associated alarms and security events
- Implications of software variants on patch update

Ownership Transfer and Party Risks



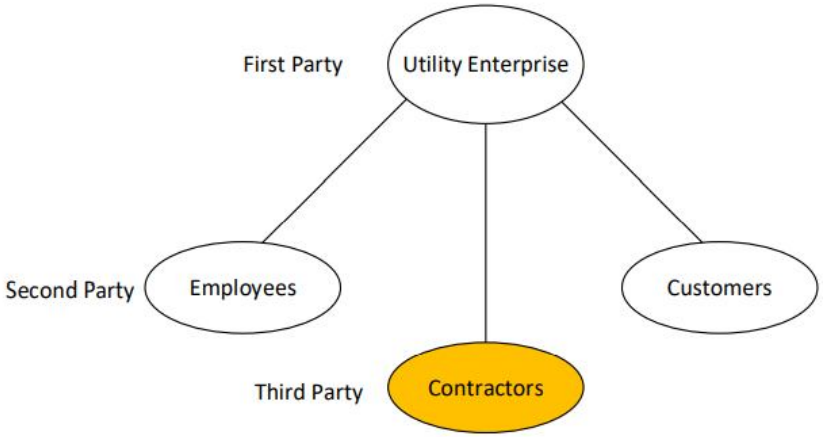
(a) Generalization of *n*-th party risks



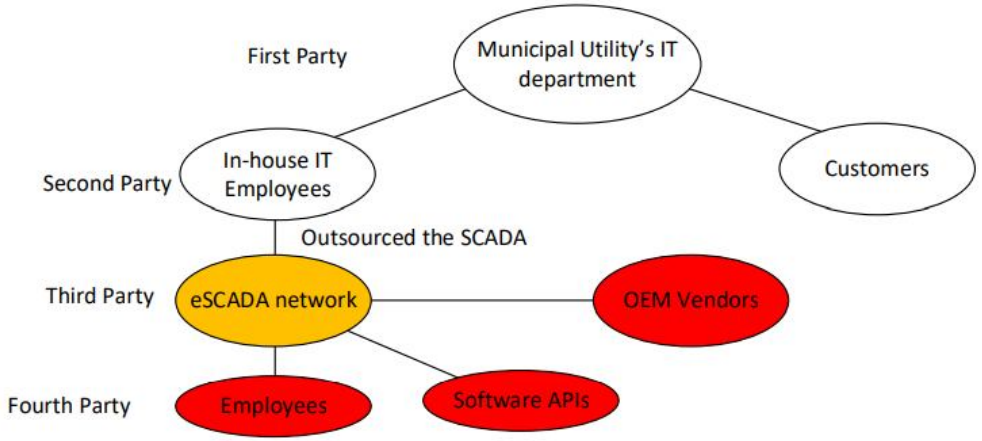
(b) Utilities with in-house OT and IT employees

Fig. Source: C.-W. Ten, “Utility Cyber Risk Management,” Protect Our Power Report, 2020.

Ownership Transfer and Party Risks



(a) Utilities *without* in-house OT/IT expertise



(a) Fourth-party dependency of risks

Fig. Source: C.-W. Ten, "Utility Cyber Risk Management," Protect Our Power Report, 2020.

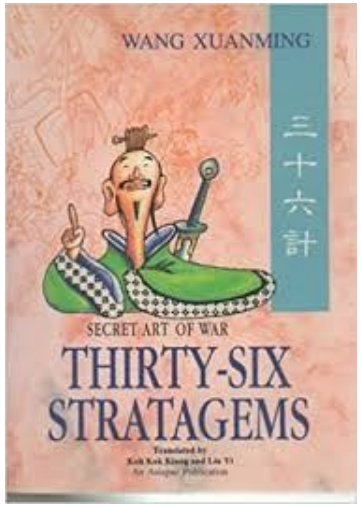
Emerging Security Technologies

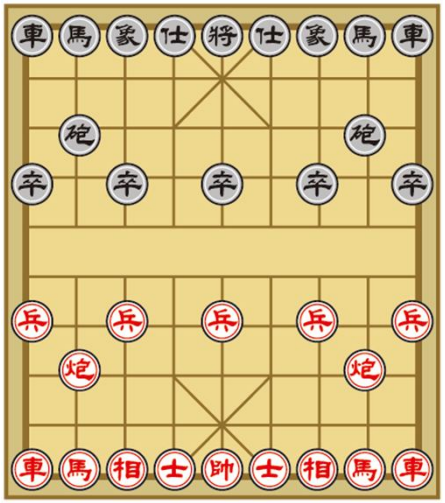
Deception and Gaming

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

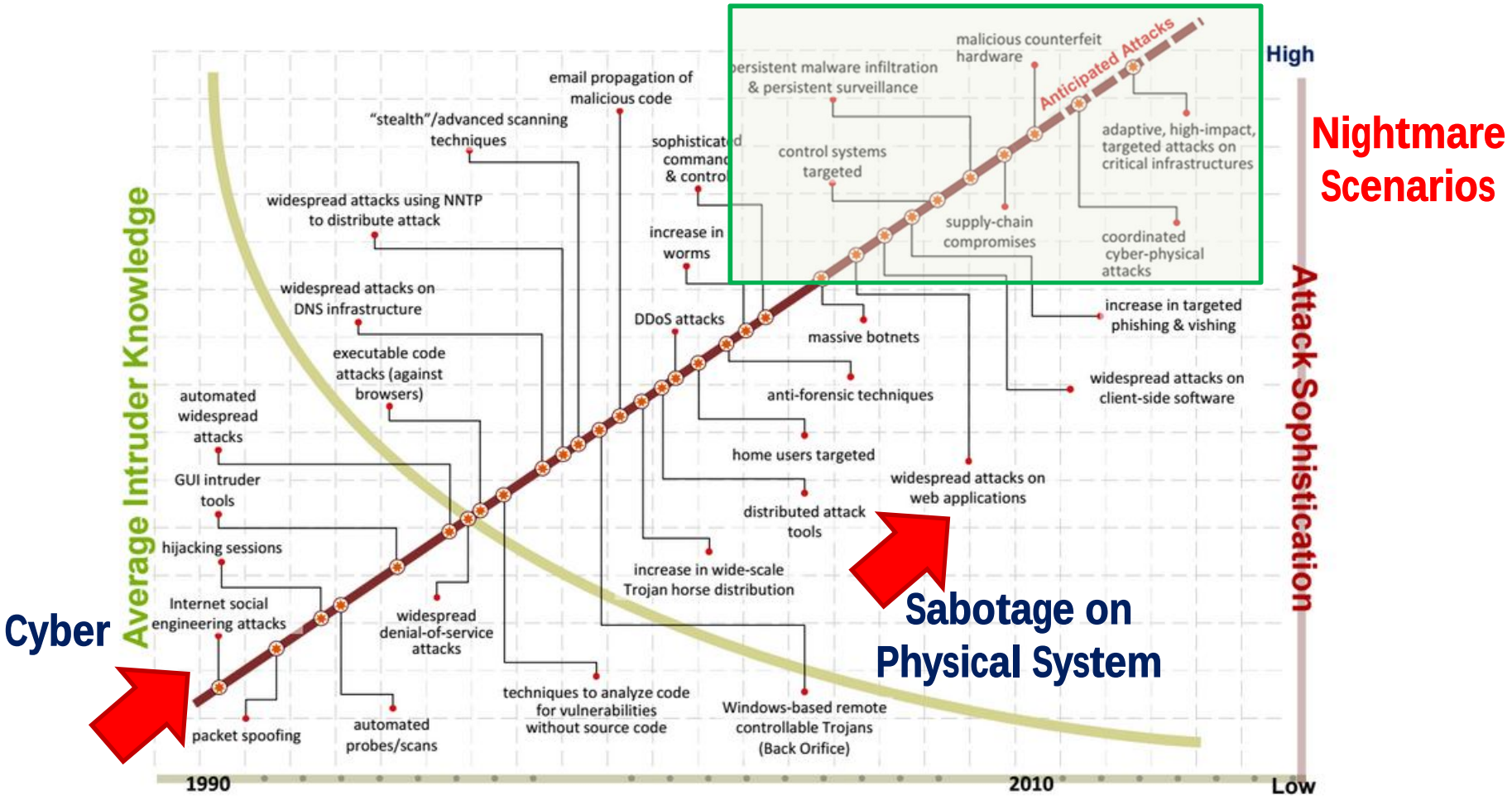
→ Good collaboration with *political science* folks

- Two players (attackers and defenders)





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

Available Security Technologies

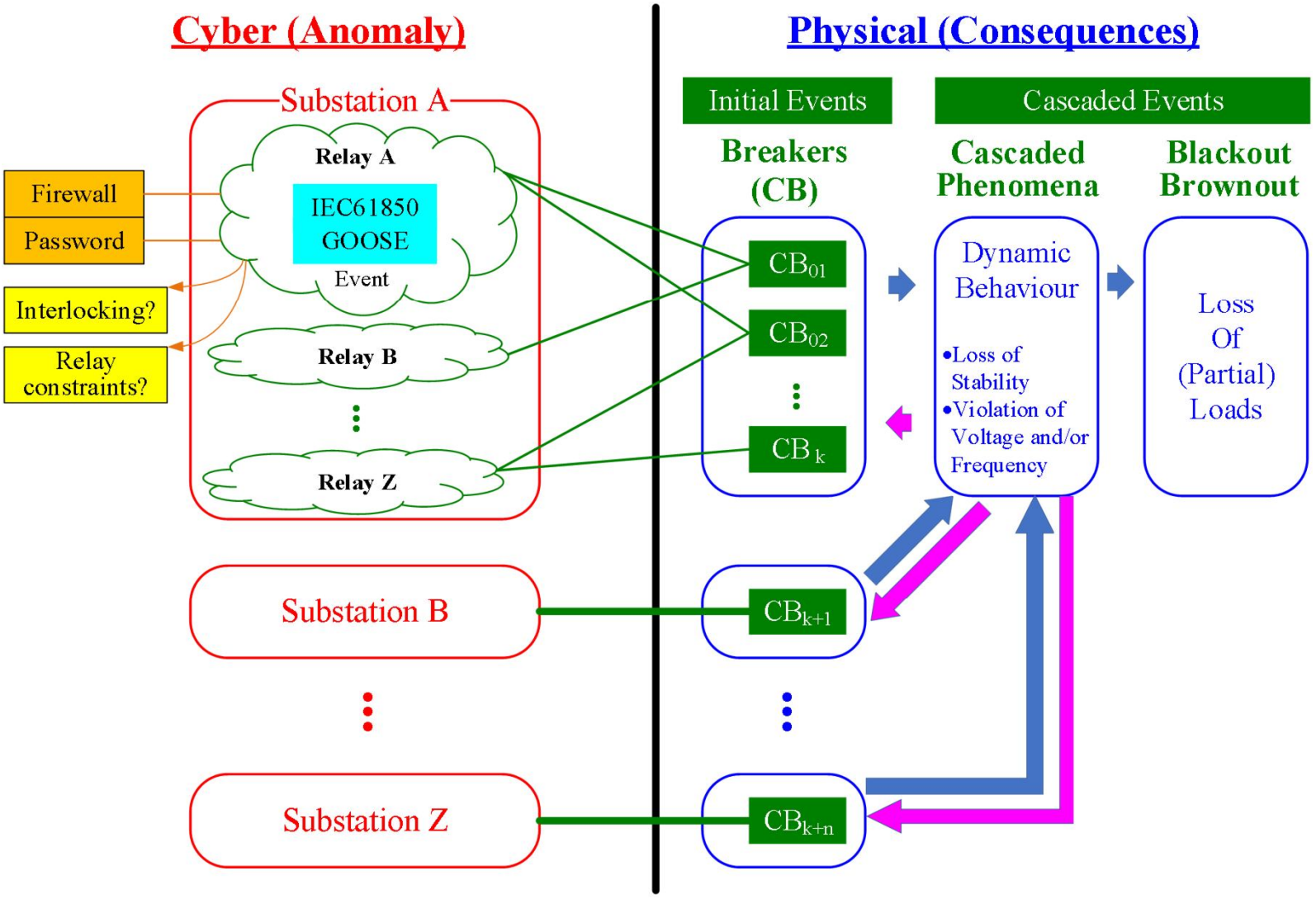
Commonly installed system

- ❑ Boundary protection, Firewall, password authentication
- ❑ Malware detection
- ❑ Other basic security features from the OS and SCADA systems
- ❑ Card reader for physical access
- ❑ Camera surveillance

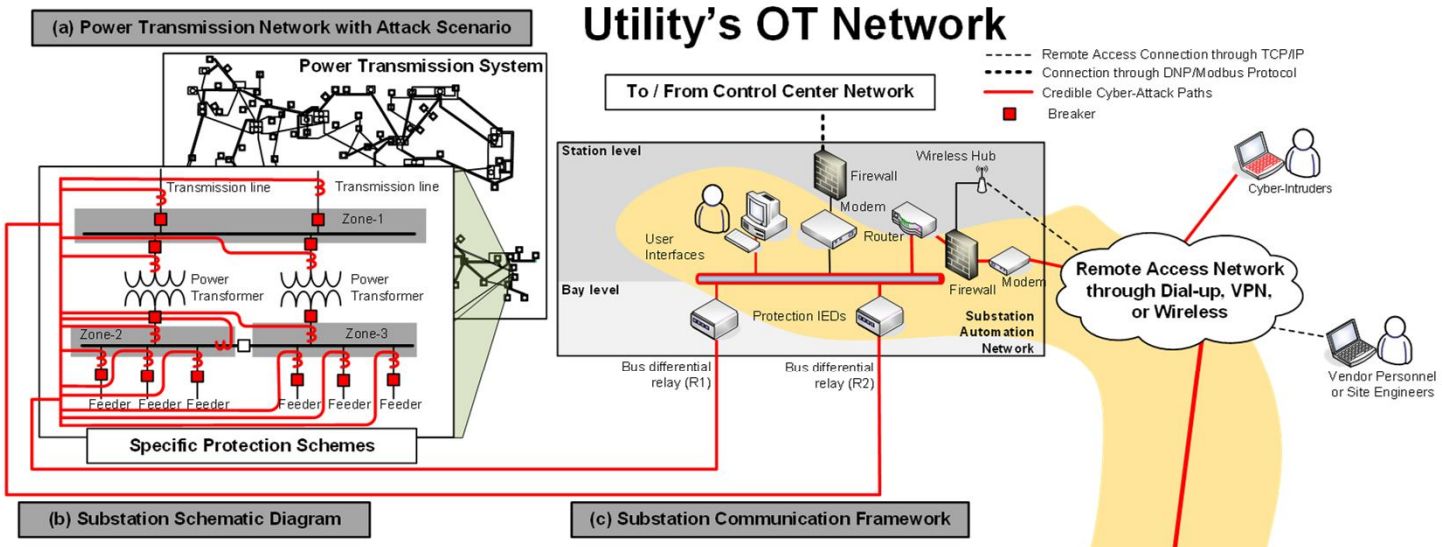
Emerging technologies

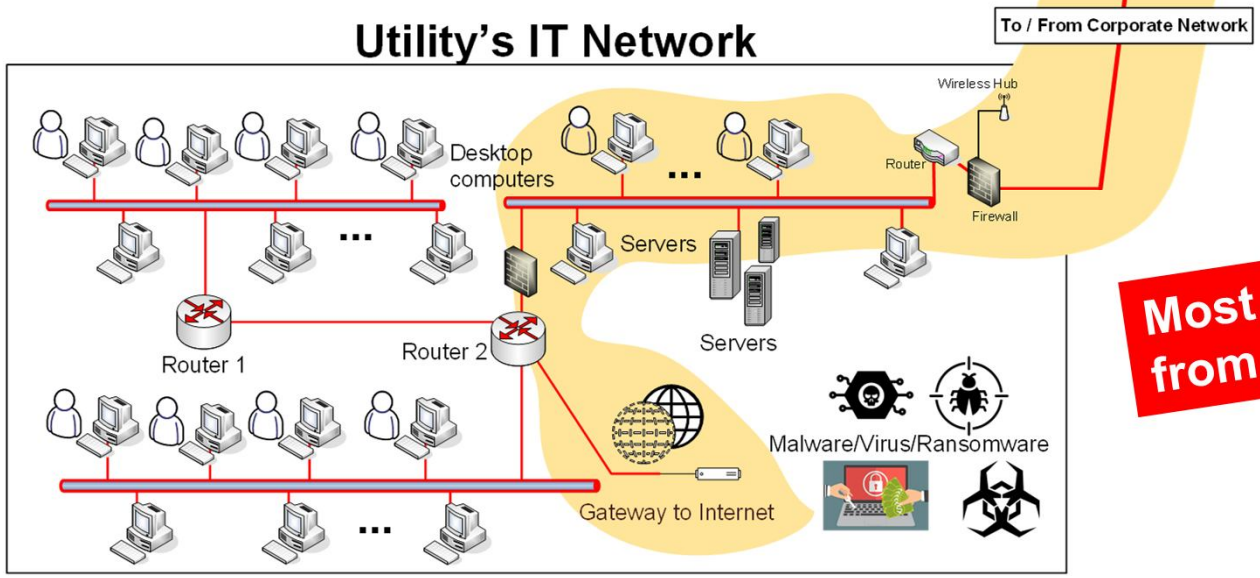
- ❖ User role/password management system
- ❖ Intrusion detection system (network traffic or host based)
- ❖ Honeynet
- ❖ Hardware-enforced unidirectional gateway
- ❖ Two-factor authentication
- ❖ Patch management
- ❖ Sandboxes
- ❖ Threat detection
- ❖ Anomaly detection (came from any of the above combinations)

Components of Cyber-Physical Relationship



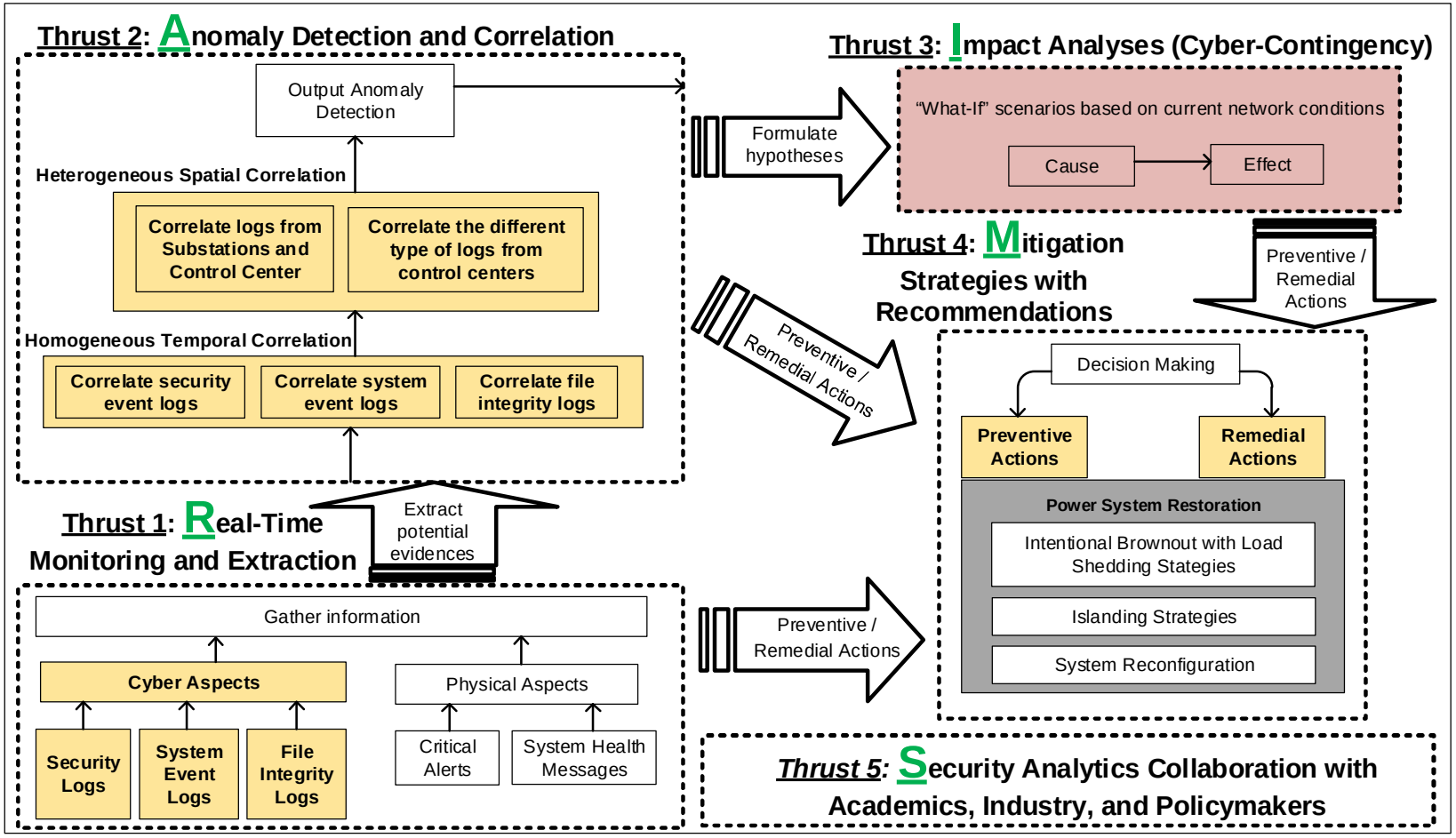
OT & IT Interconnectivity





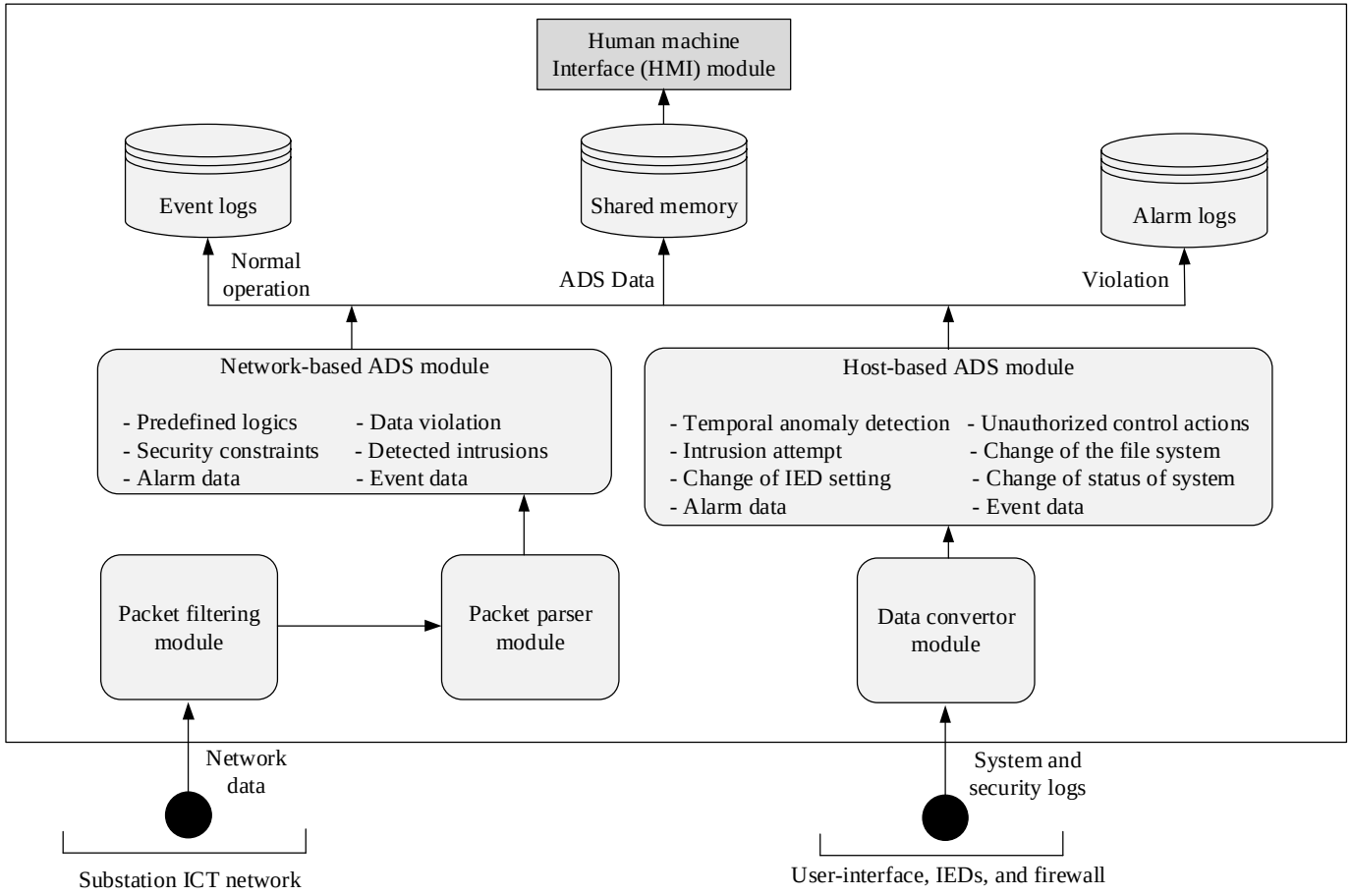
Most OT attacks start from IT networks

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



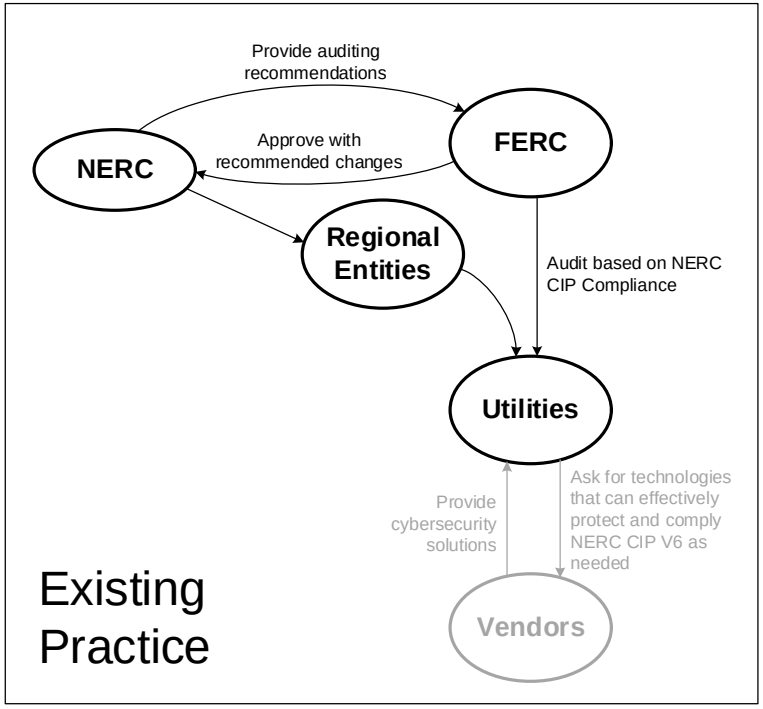
Chee-Wooi Ten, Manimaran Govindarasu, and Chen-Ching Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Trans. Syst., Man, Cybernetics, Part A*, vol. 40, no. 4, pp. 853—865, Nov. 2010.

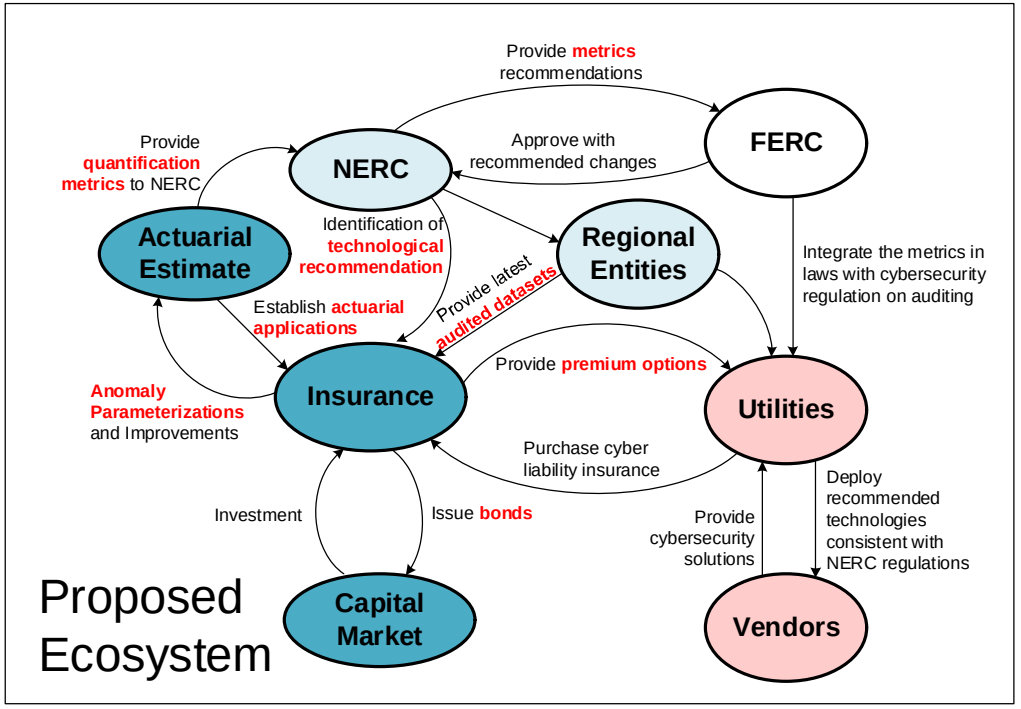
Integrated Anomaly Detection System (SCADA + Cyber Alarms)



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

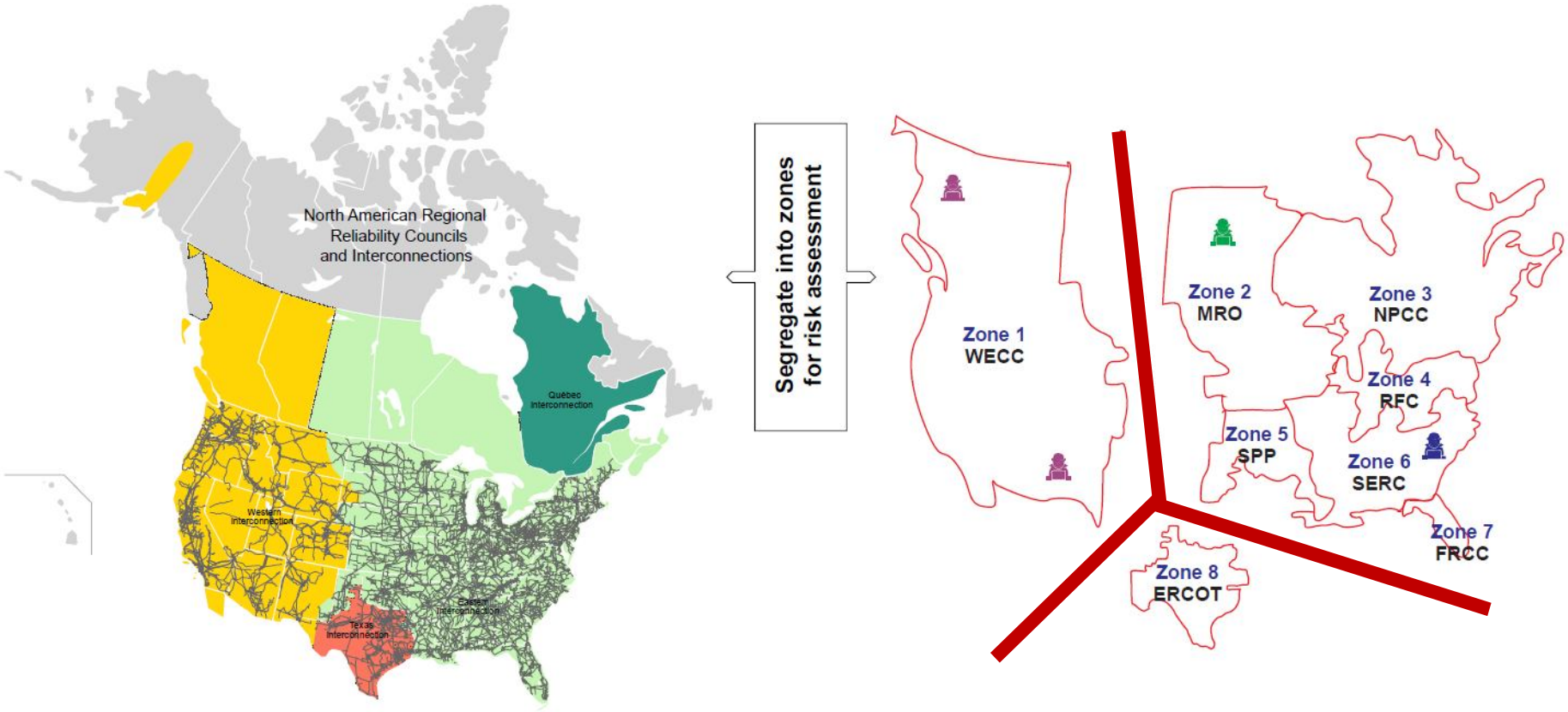
Actuarial Framework for Power Grid Cybersecurity





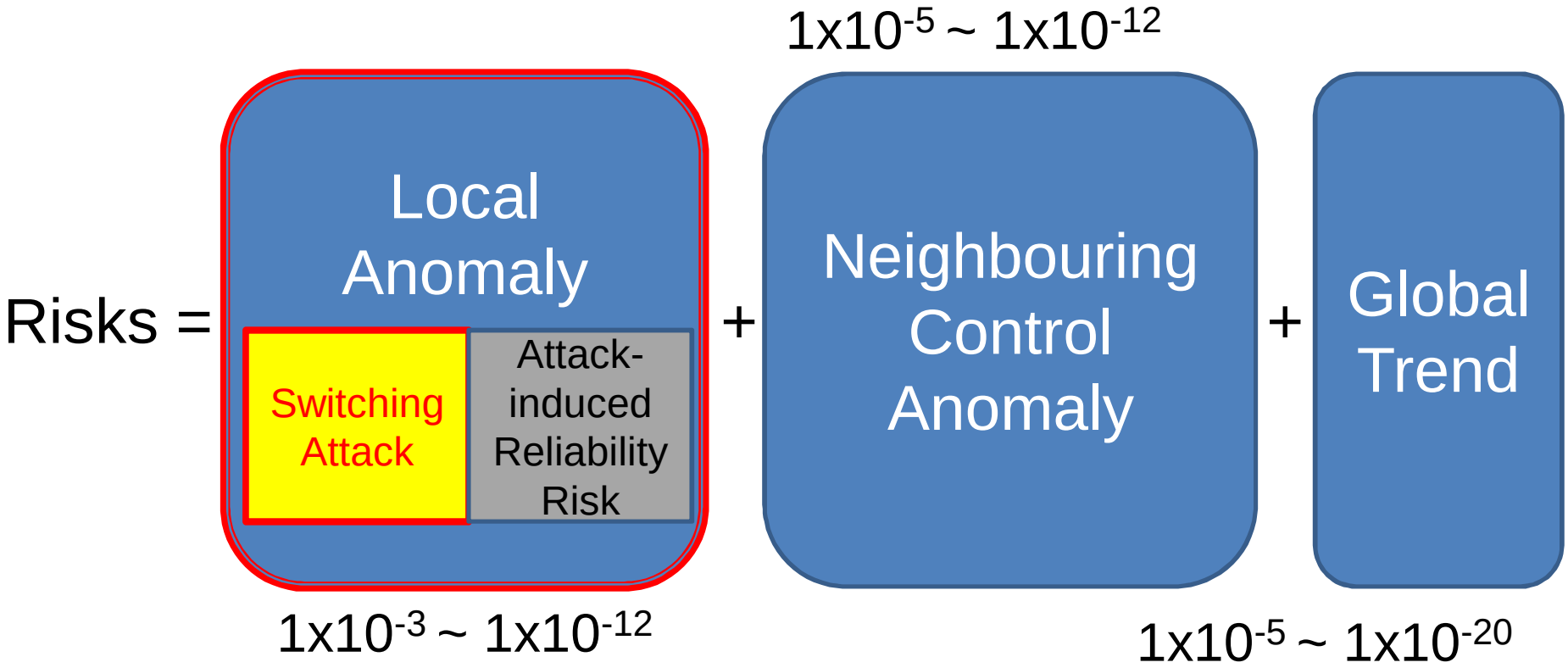
Chee-Wooi Ten, Lingfeng Wang, Wei Wei, and Yeonwoo Rho, "CPS: Medium: Collaborative Research: An Actuarial Framework of Cyber Risk Management for Power Grid," National Science Foundation, Sep. 1, 2017 – Aug. 31, 2021 with **University of Wisconsin—Milwaukee**.

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

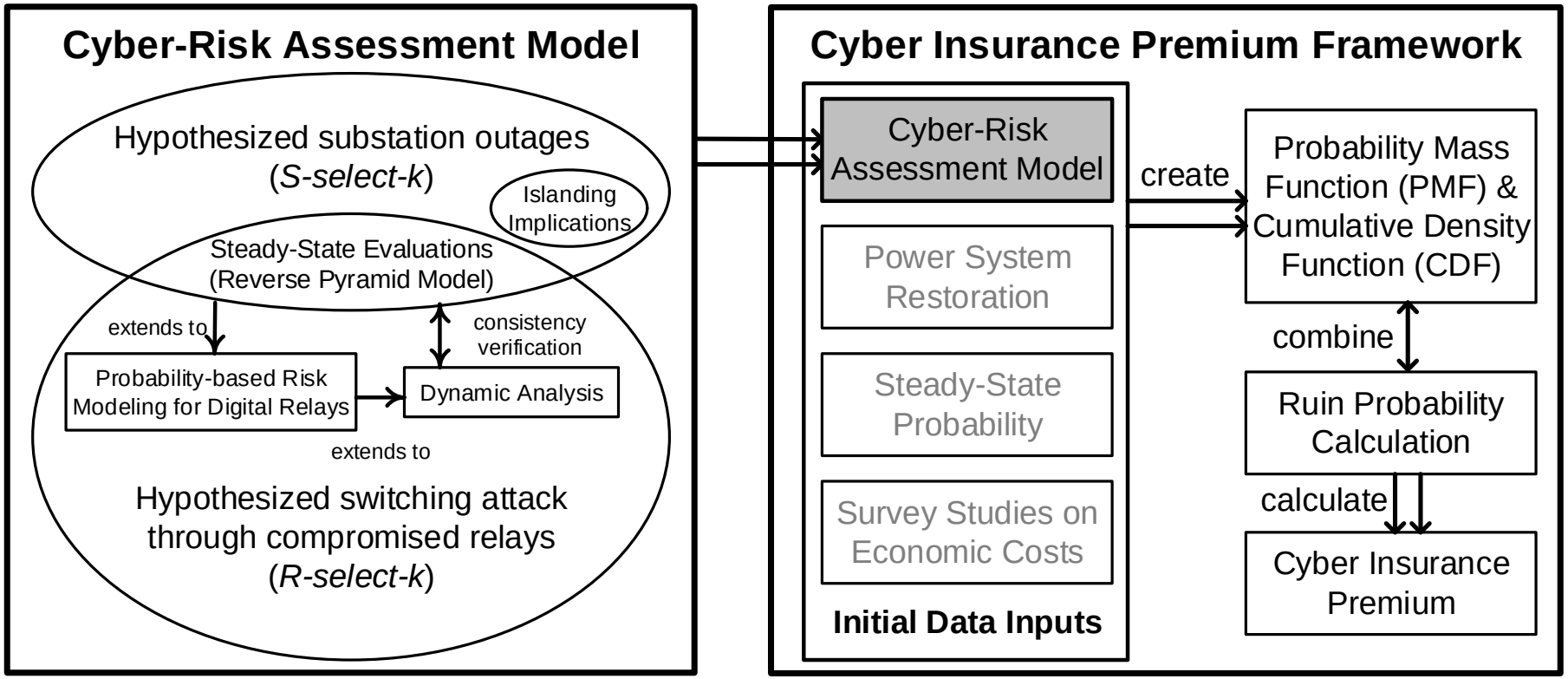
Risks of Cyberattack



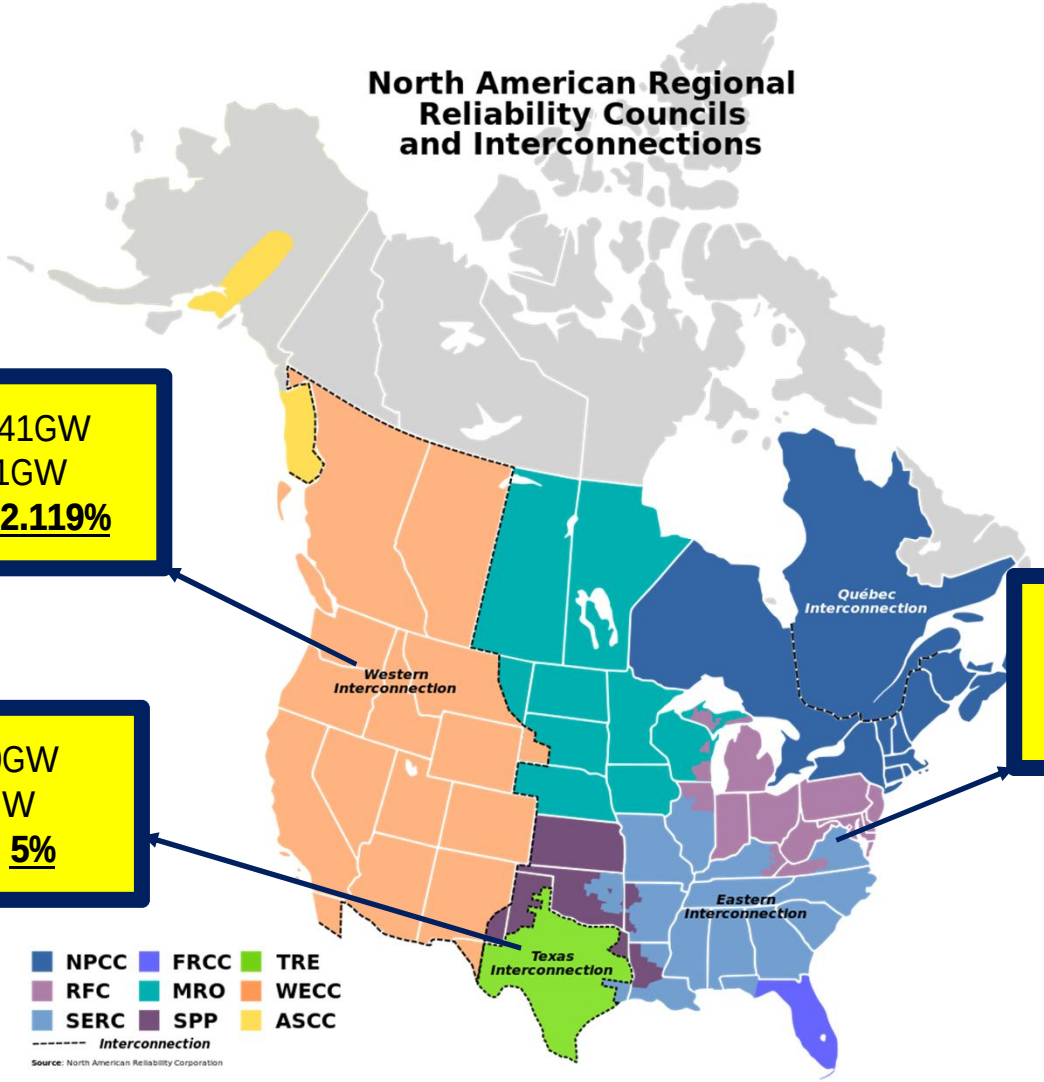
Cyber Insurance Premium for an Interconnected Grid

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.

Goals of This Project



3,000MW Relative to Interconnection

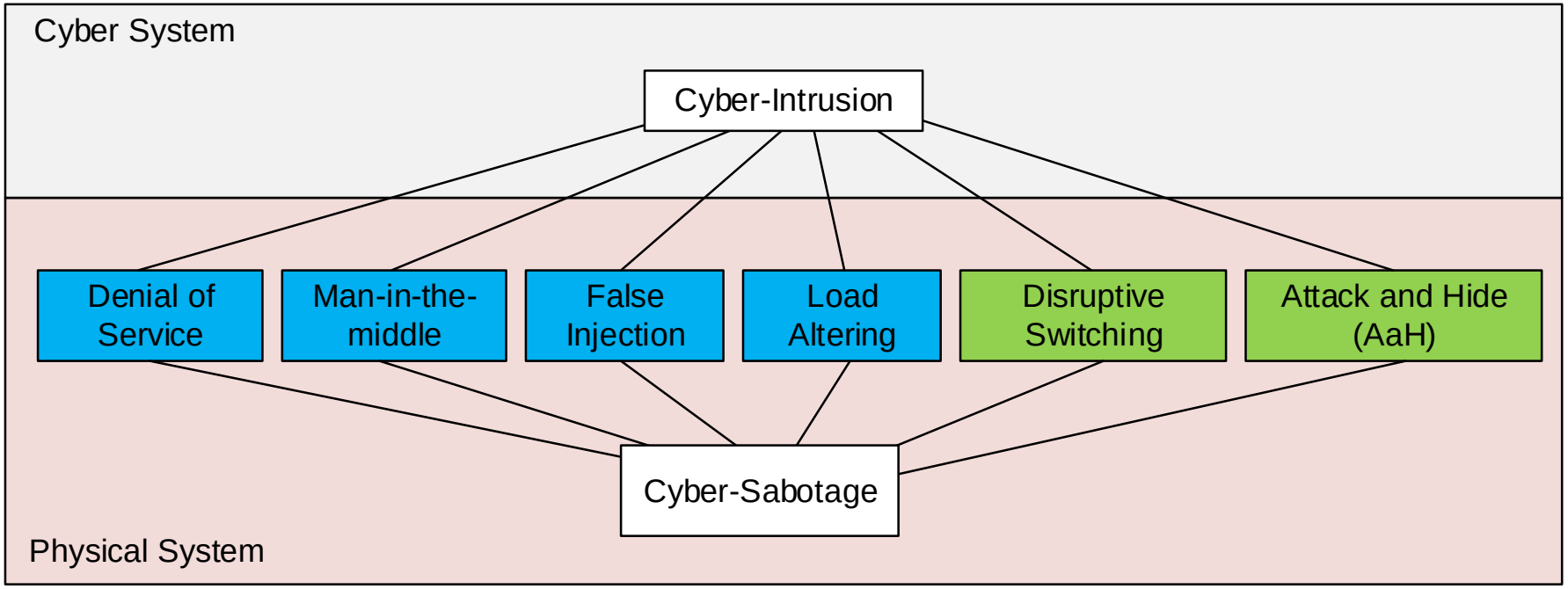


Average Load: 141GW
Max. Load: 151GW
Relative to 3GW: **2.119%**

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

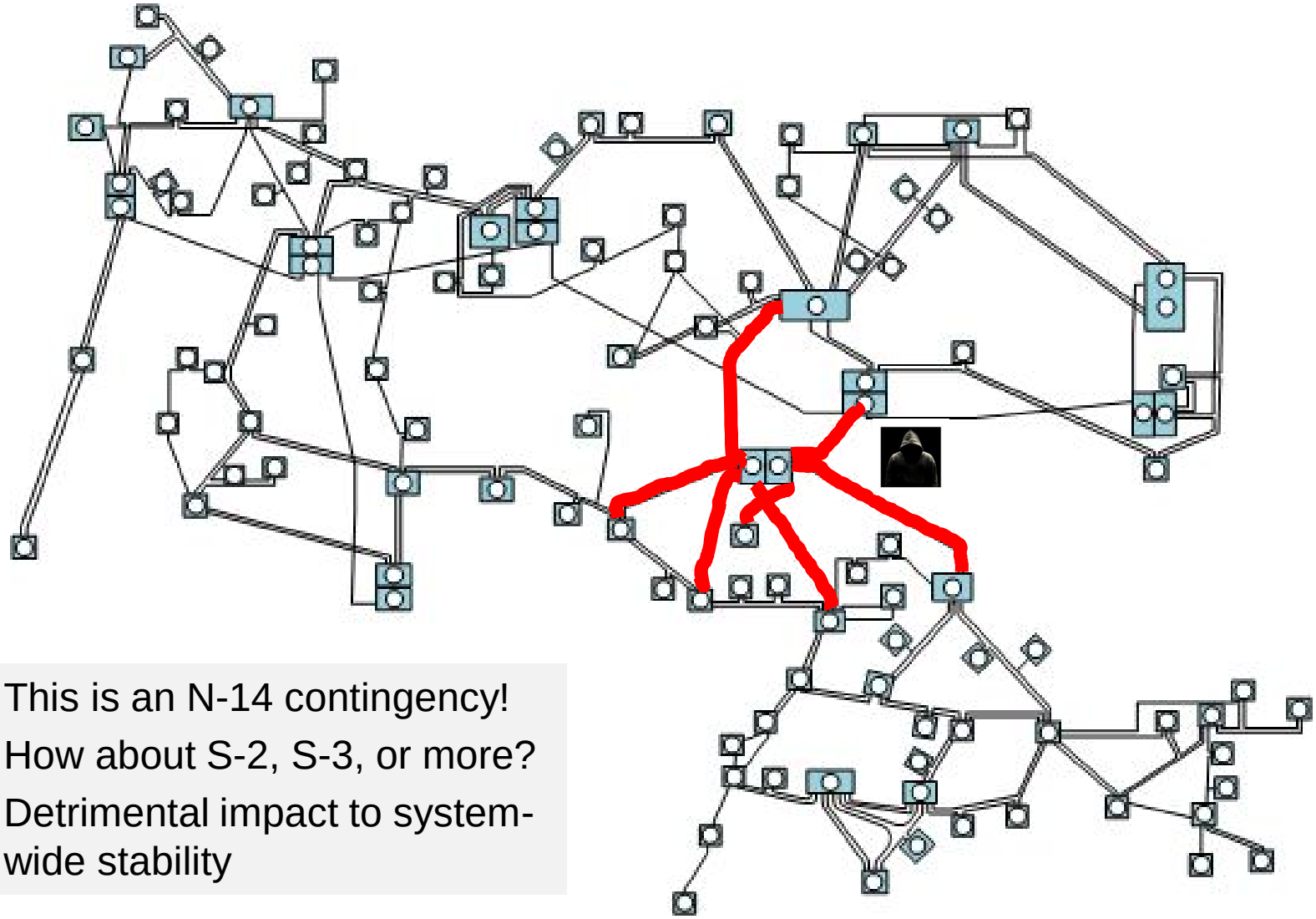
Average Load: 60GW
Max. Load: 70GW
Relative to 3GW: **5%**

Cyber-Physical Systems Security of a Power Grid



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

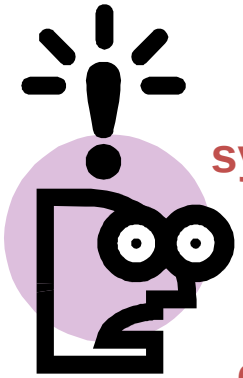
S-1 Contingency



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

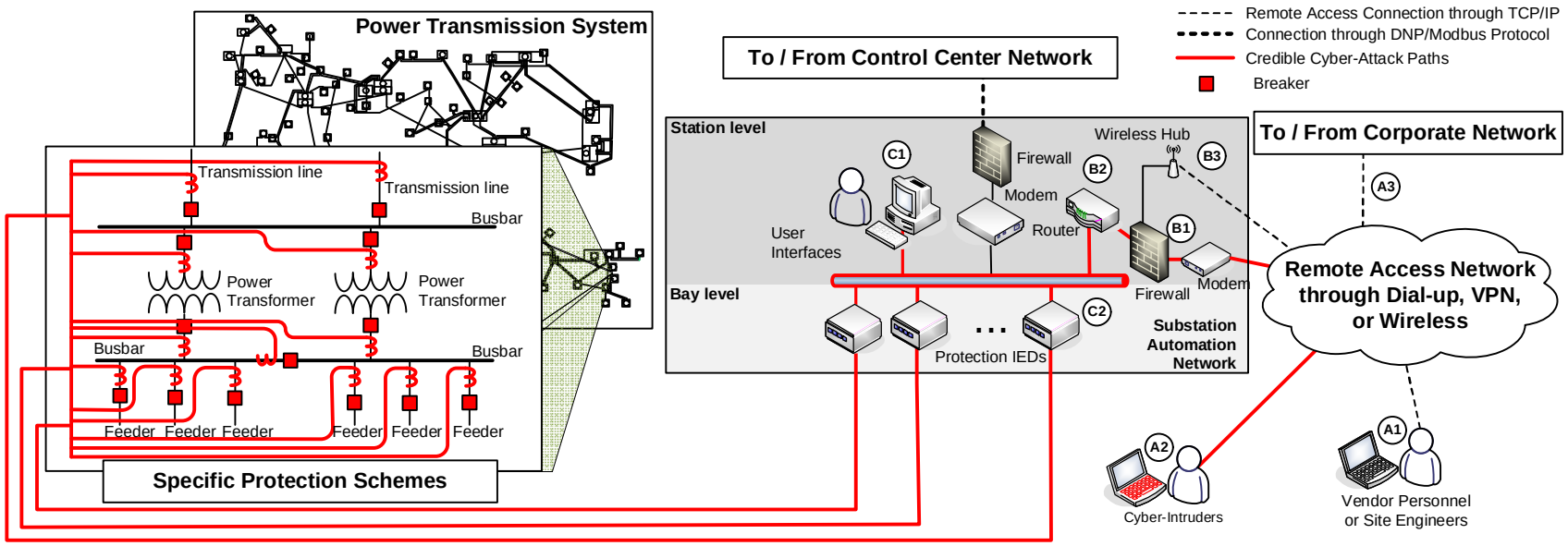
A Hypothetical Scenario

Breakers opened, what happened?



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

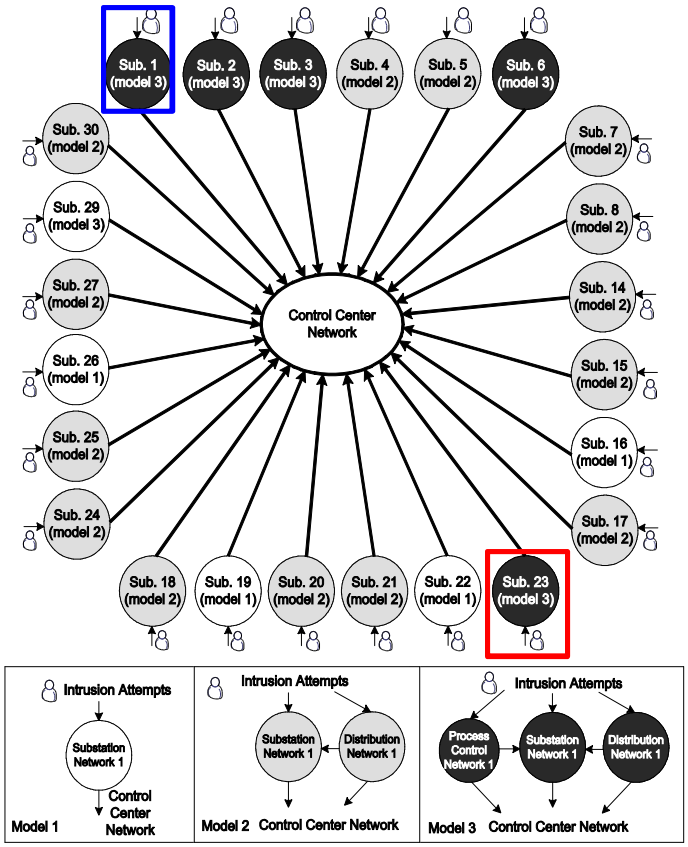
Cyber-Physical Relationship for a Substation Example



- 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**)

Hypothesized One Substation Outage

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

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

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

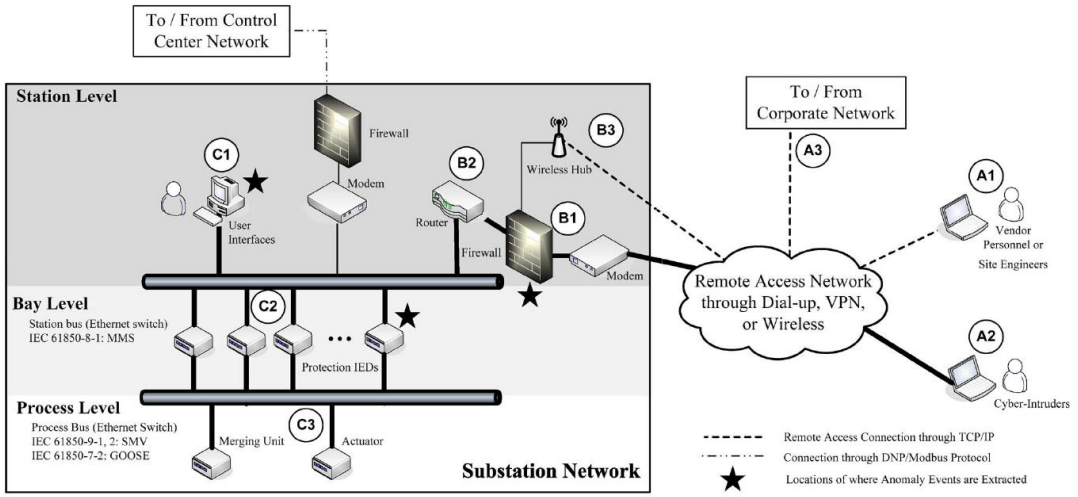
- Modeling of ***Cyber-Net*** between network entities
  - Model 1: Substation and Control Center Networks
  - Model 2: Substation, Distribution, and Control Center Networks
  - Model 3: Substation, Process Control, and Control Center Networks

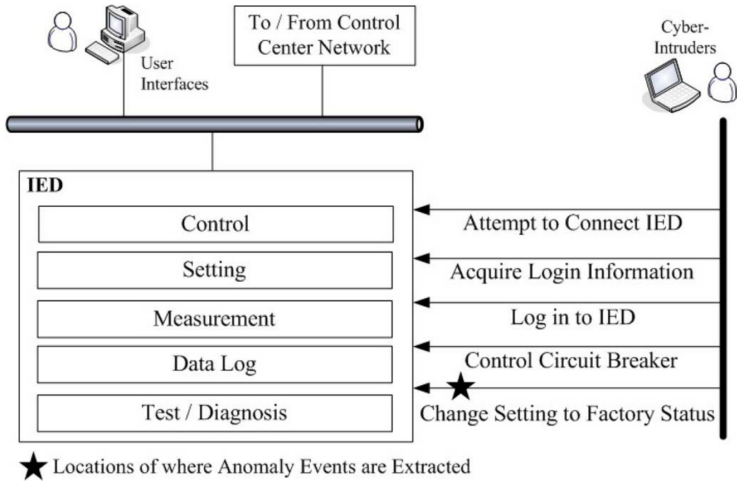
Chee-Wooi Ten, Chen-Ching Liu, and Manimaran Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836—1846, Nov. 2008. <10.1109/TPWRS.2008.2002298>

Hypothesized Outages Based on A Limited Set of Malicious Substations

$$\sum_{k=1}^{M} C_k^S$$

Anomaly Detection for Substation Cybersecurity





Outsiders

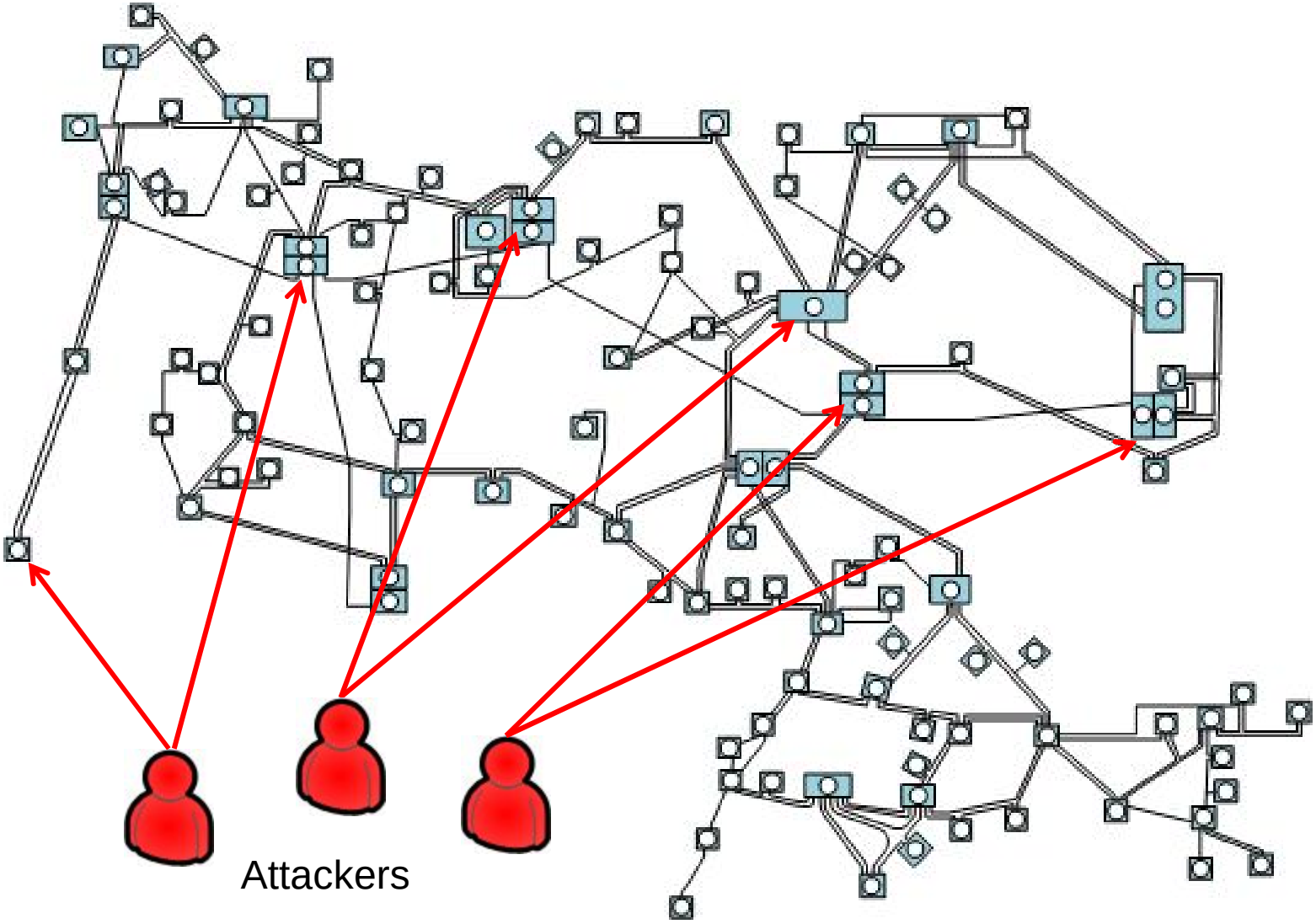
- Any point of (A1, A2, A3)-B1-B2
- Any point of (A1, A2, A3)-B3-B1-B2

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>

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



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

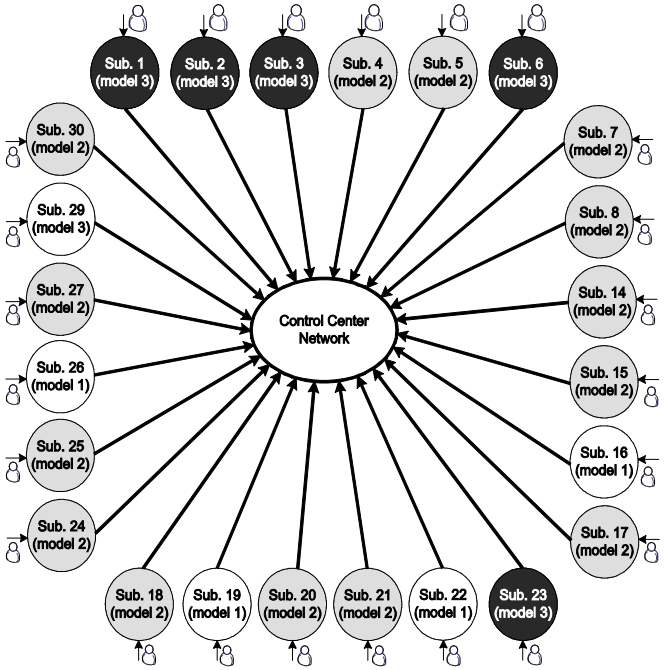
Rashiduzzaman Bulbul, Chee-Wooi Ten, and Andrew Ginter, "Cyber-Contingency Evaluation for Multiple Hypothesized Substation Outages," *Proc. 5th IEEE-PES Conference on Innovative Smart Grid Technologies*, Feb. 19-22, 2014, Washington, DC, USA.

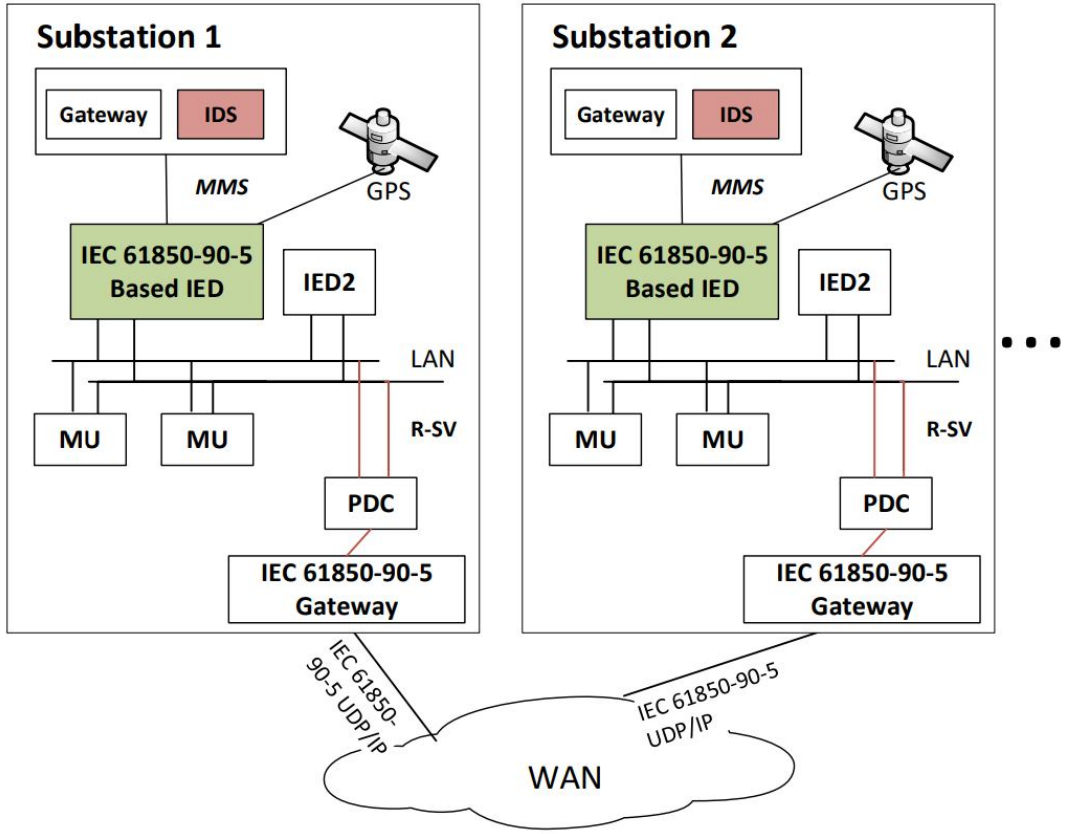
We **MAY NOT have all successful/failures cases**, but we **could simulate all plausible outcomes**!

Hypothesized Outages for All Substations

$$\sum_{k=1}^{S} C_k^S$$

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



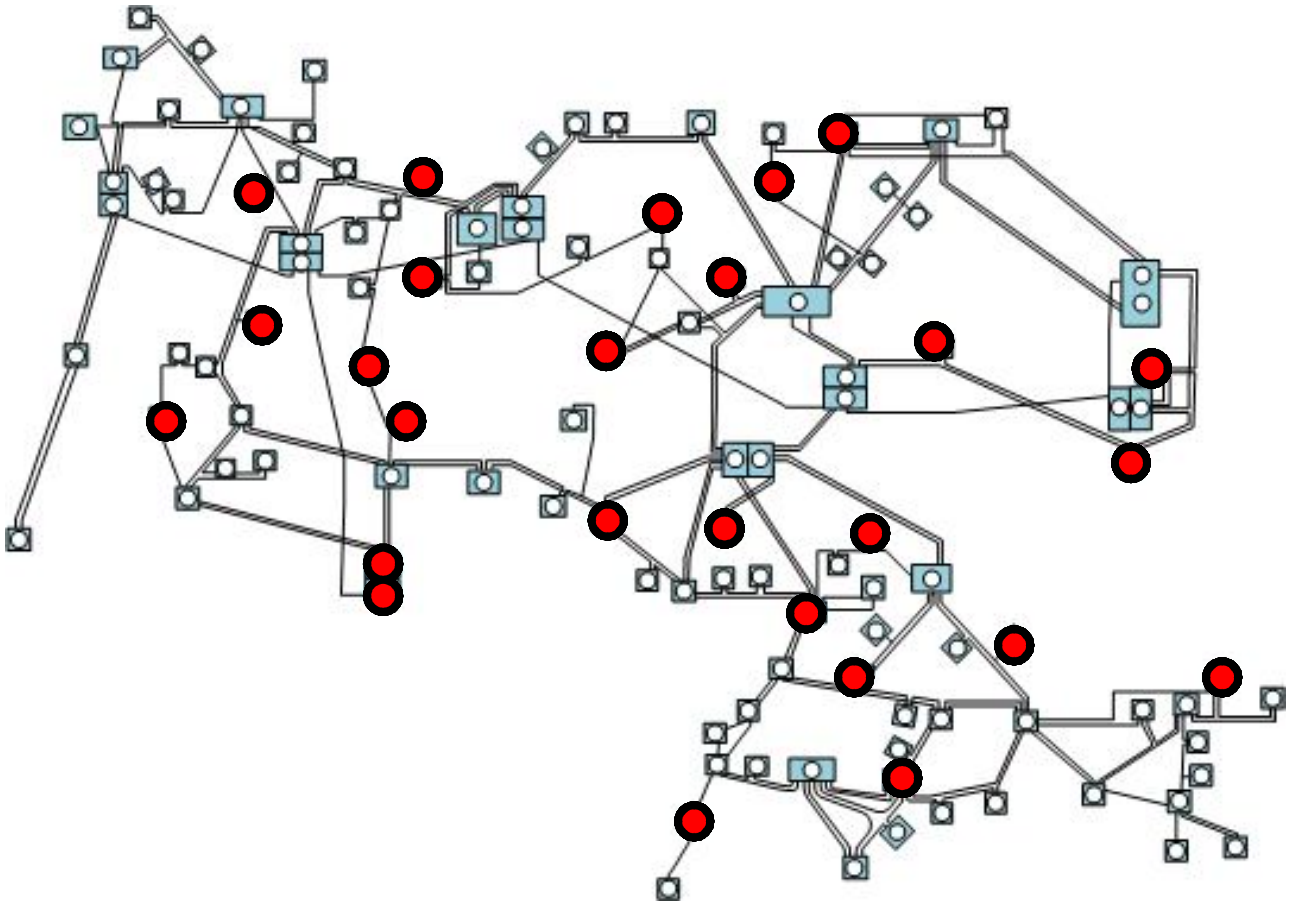


Chee-Wooi Ten, Chen-Ching Liu, and Manimaran Govindarasu, "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Transactions on Power Systems, vol. 23, no. 4, pp. 1836—1846, Nov. 2008. <10.1109/TPWRS.2008.2002298>

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.

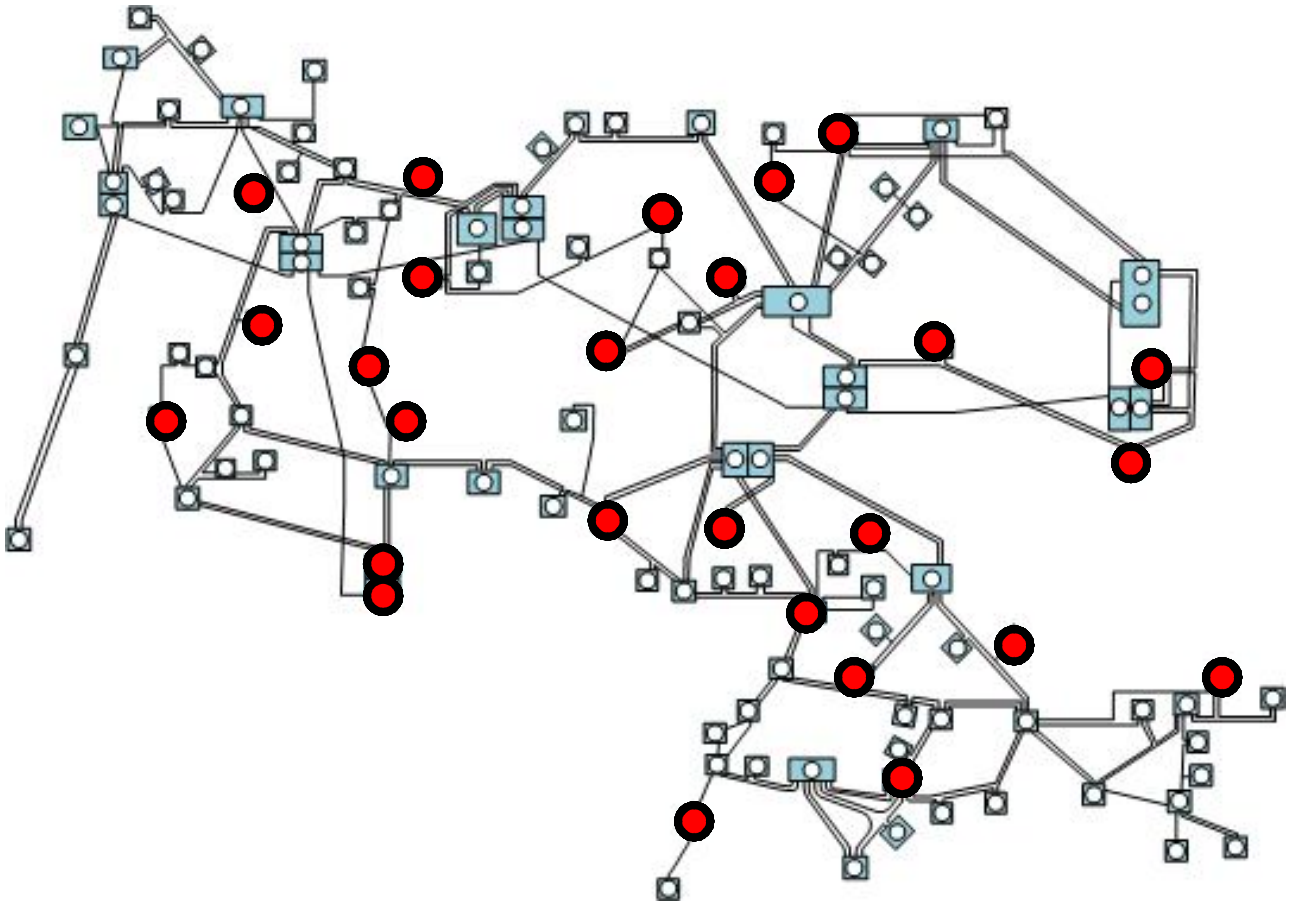
Coordinated Cyber-Physical Attacks

- 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!

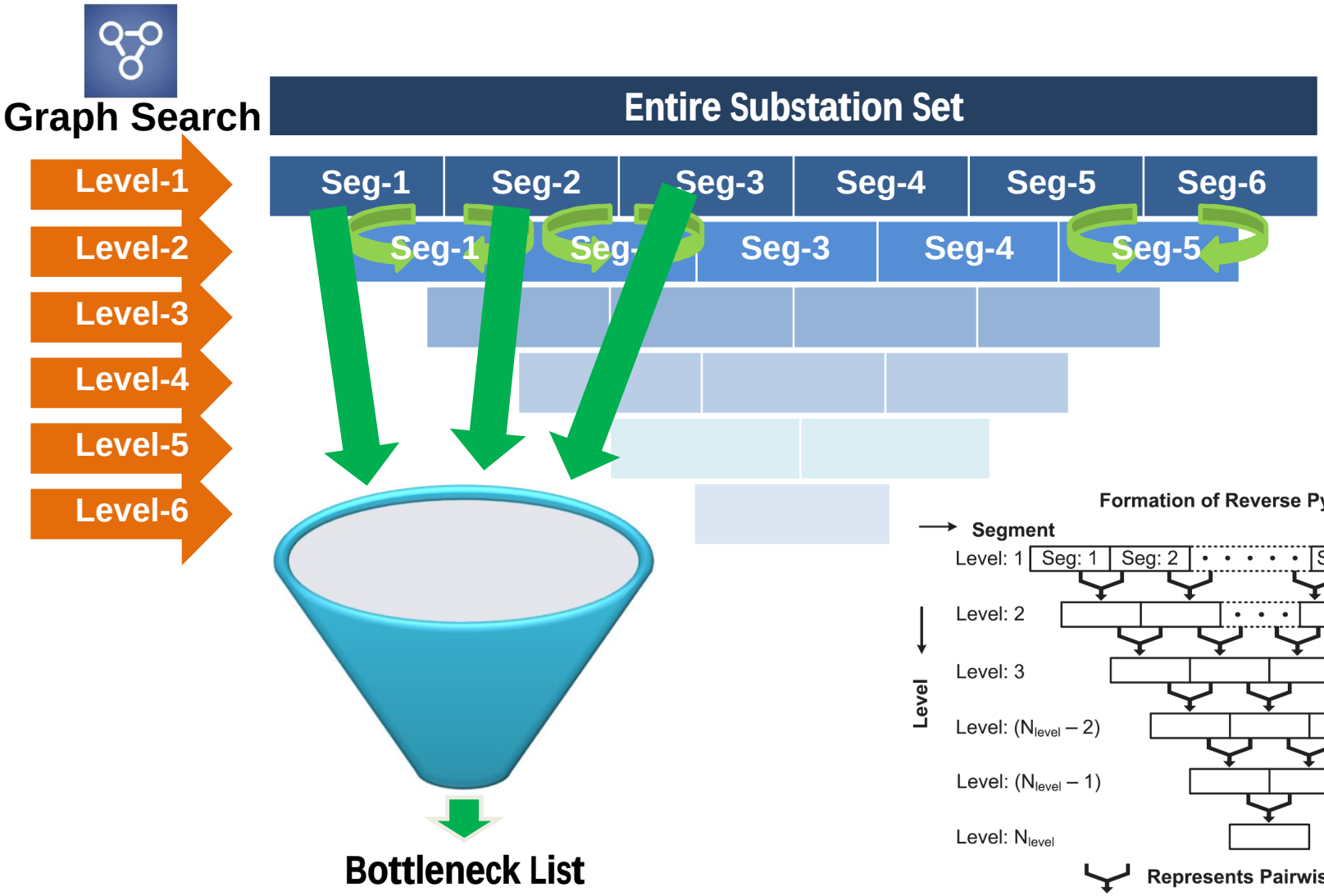


Coordinated Cyber-Physical Attacks

- 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!

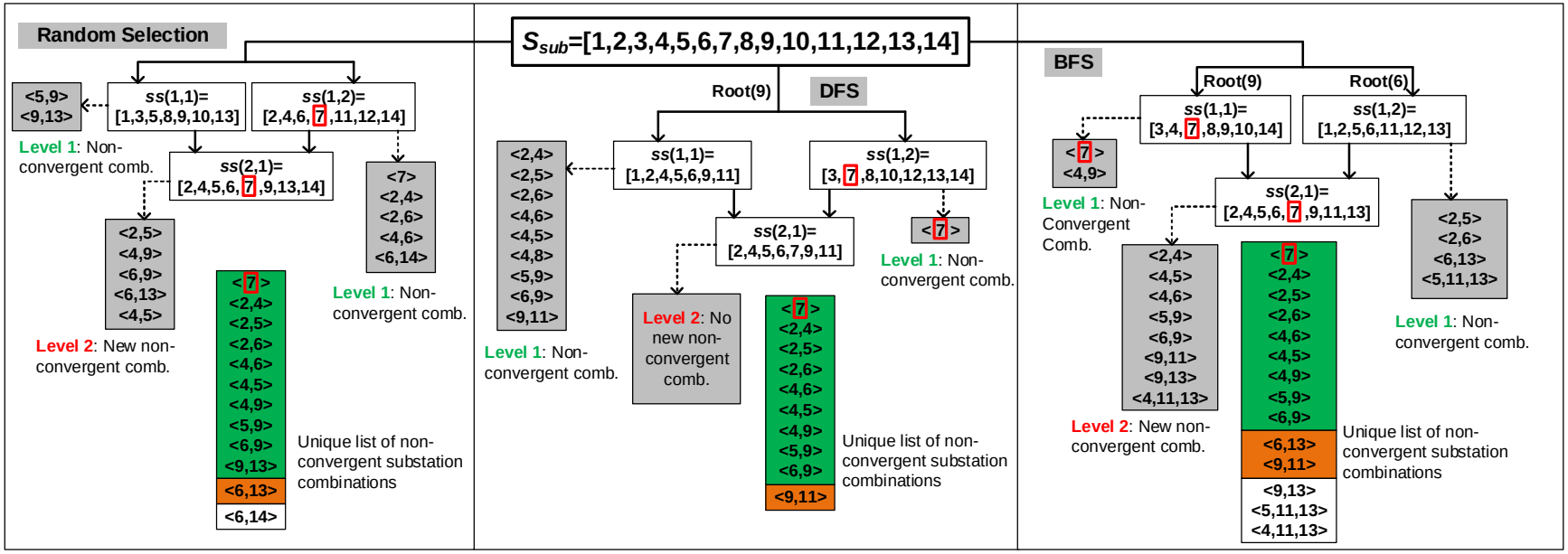


Formation of Reverse Pyramid Model (RPM)



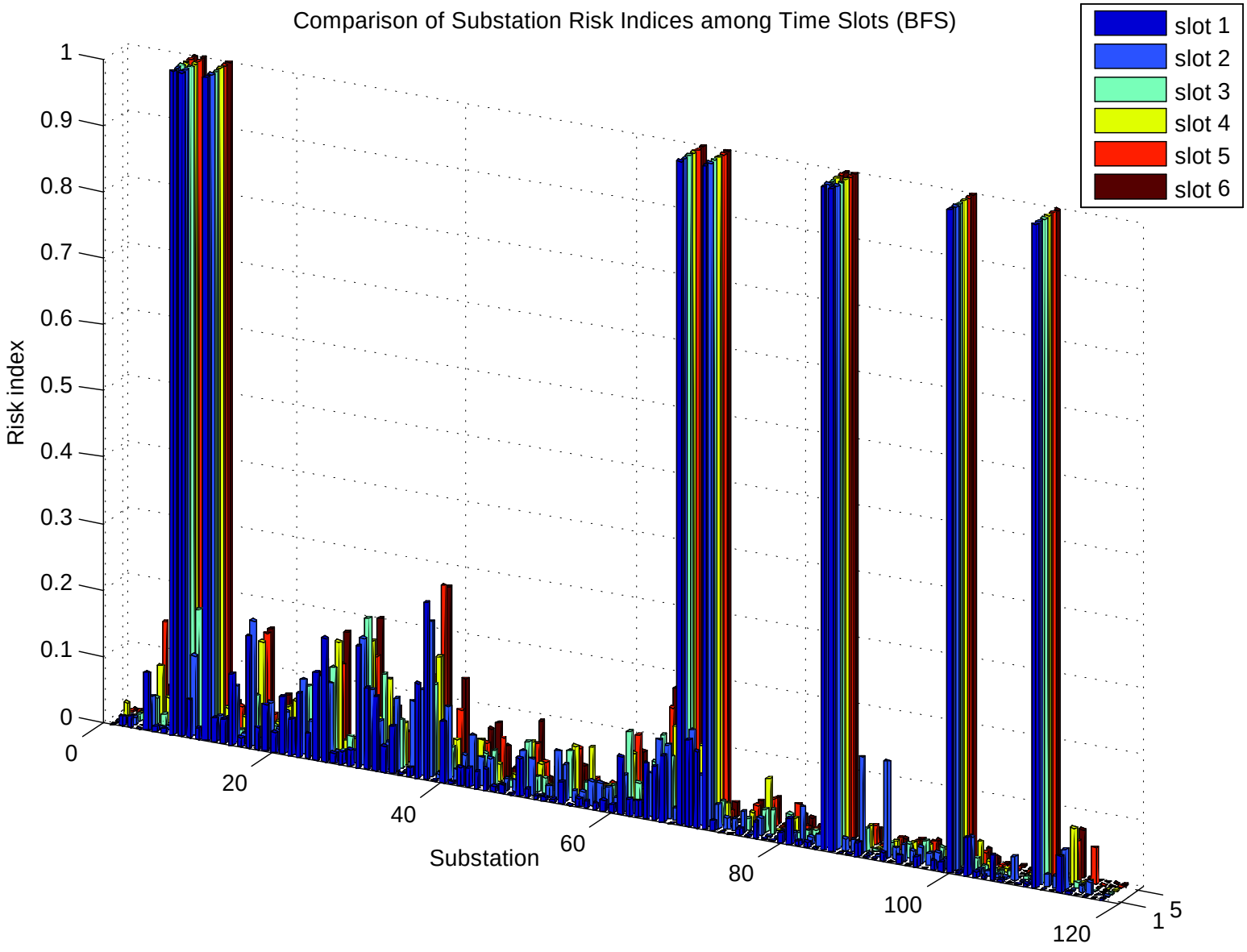
Chee-Wooi Ten, Andrew Ginter, and Rashiduzzaman Bulbul, “Cyber-Based Contingency Analysis,” IEEE Transactions on Power Systems, vol. 31, no. 4, pp. 3040—3050, Sep. 2015. <10.1109/TPWRS.2015.2482364>

Segmentation Approaches on IEEE 14-Bus System

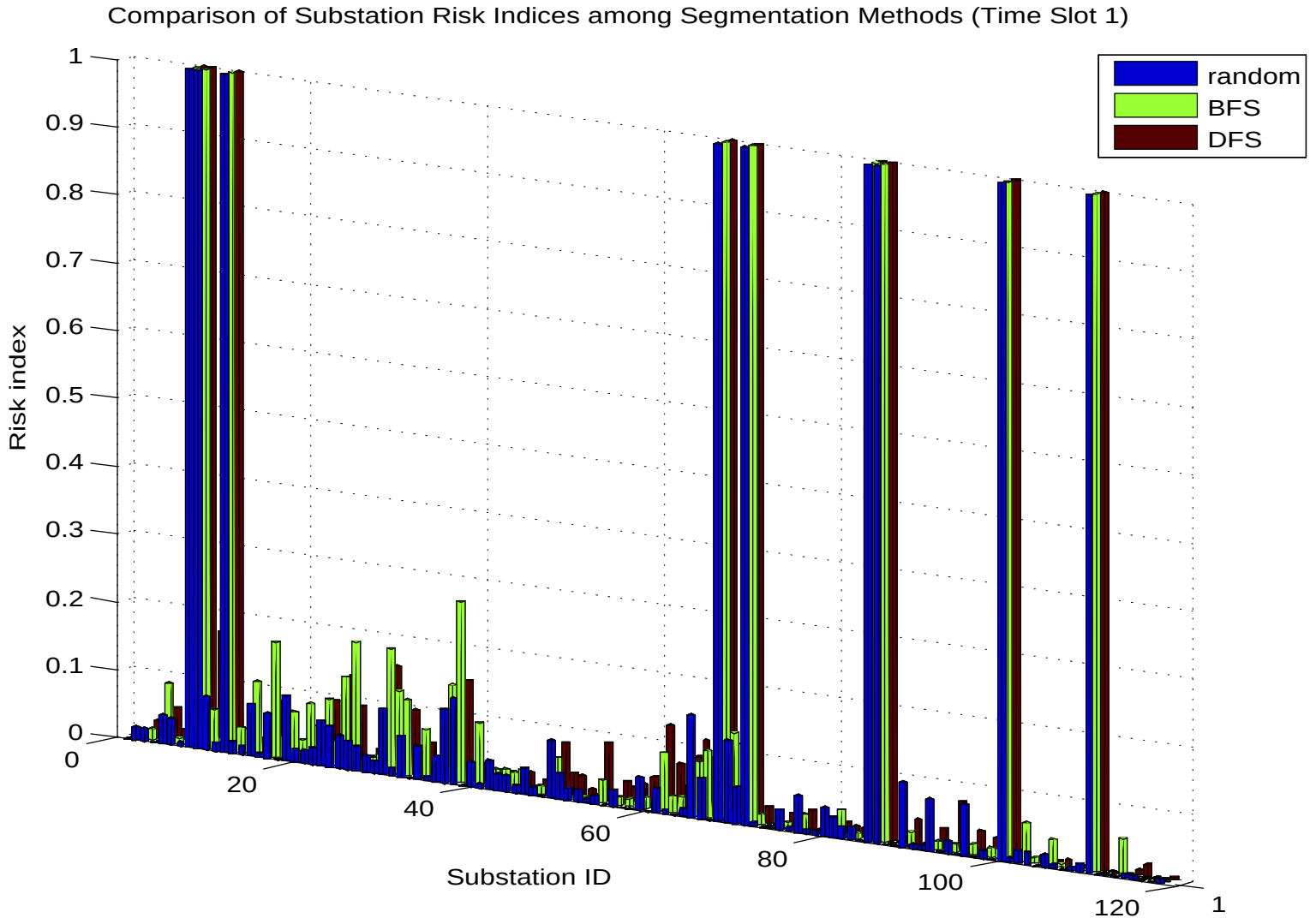


- Graph-based heuristic approaches
- 9 combinations are common (green zones)
- 1 or 2 combinations are common in two methods (orange zones)

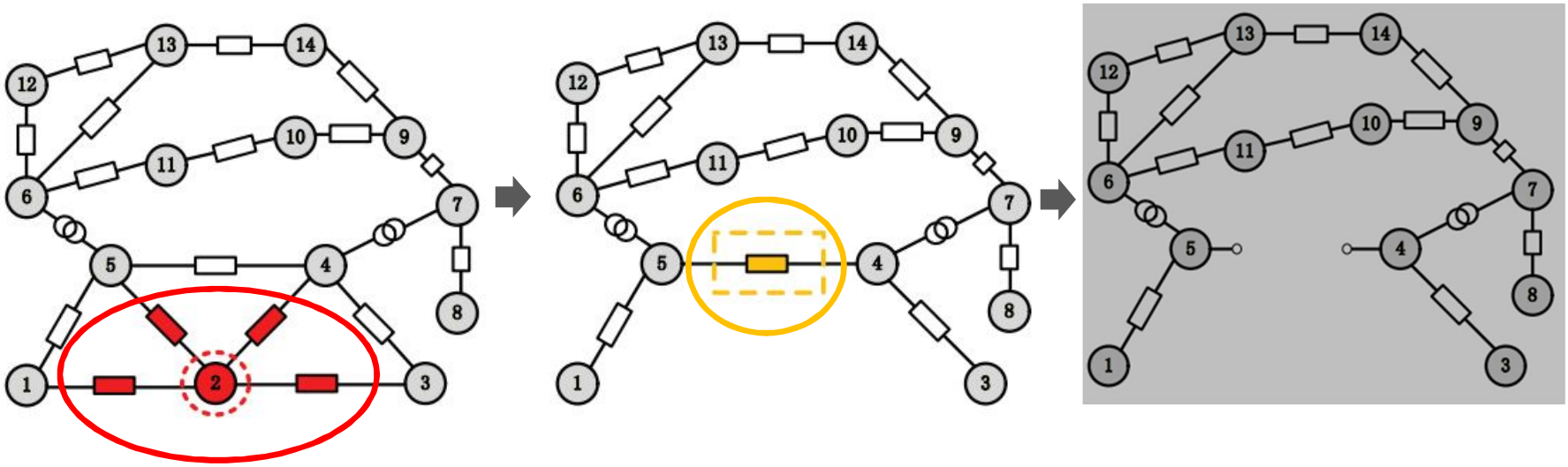
Risk Index on IEEE-118 Bus System



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'')

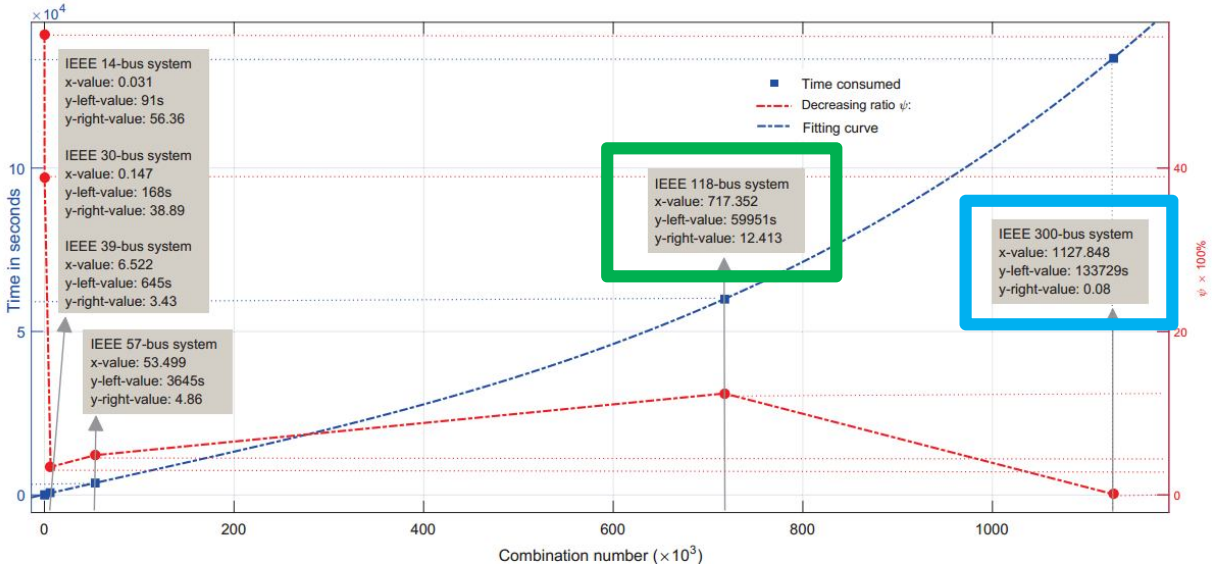
$$\underbrace{G(V,E)}_{\text{(a) Original } G} \xrightarrow[\text{cyberattack}]{\text{Switching}} \underbrace{V'(G') = V(G) \setminus V_k \subset S_{sub}}_{\text{(b) Hypothesized substations outages}} \xrightarrow[\text{overloading}]{\text{Potential}} \underbrace{E'(G'') = E(G') \setminus E_k \subset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

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>

Simulation Results

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

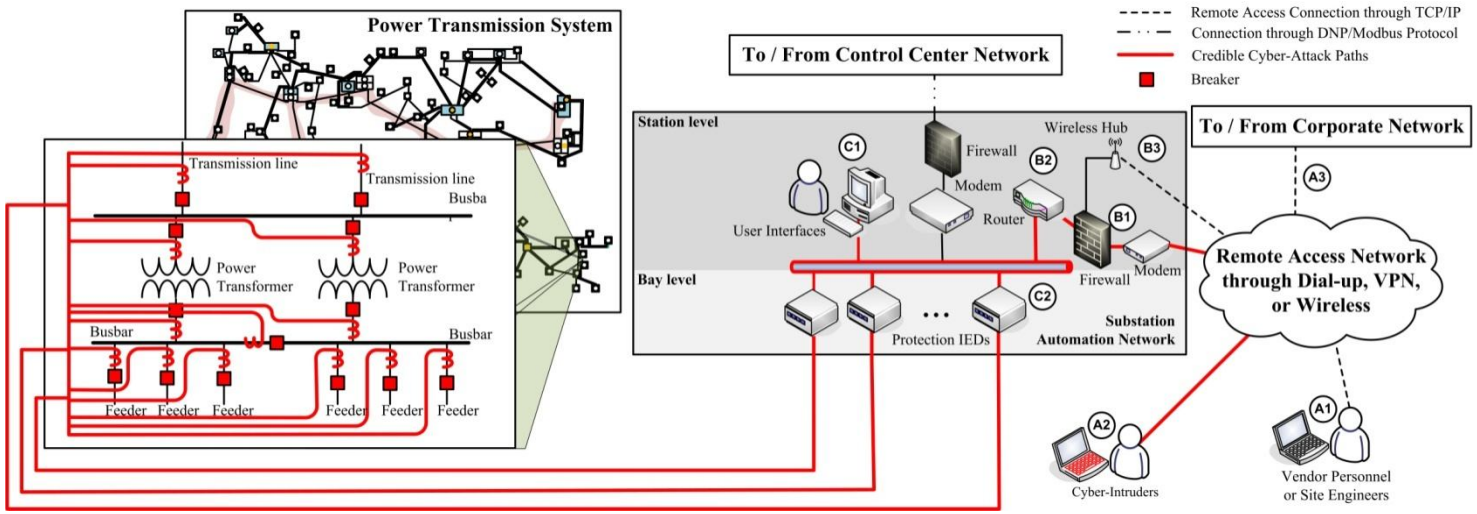
Cases #	k	# Total Comb. s_k	# Reduction χ	# New $s_{new,k}$	$\mathbf{PF}_{failed}$ = 1
14-bus	1	10	-	10	3
	2	45	24	25	1
30-bus	1	24	-	24	8
	2	276	156	120	5
	3	2,024	1,593	493	15
	4	10,626	9,354	1,272	17
	5	42,504	40,315	2,189	39
	6	134,596	132,172	2,424	59
39-bus	1	27	-	27	11
	2	351	231	120	30
57-bus	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

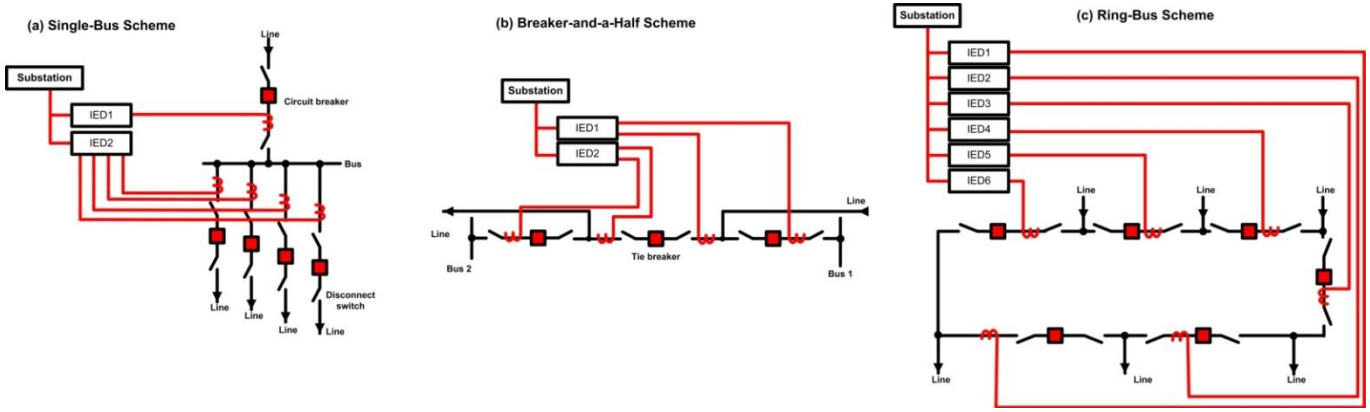


For IEEE 118-bus system, 717,353 cases are evaluated, which takes approximate 16 hours to complete calculation

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

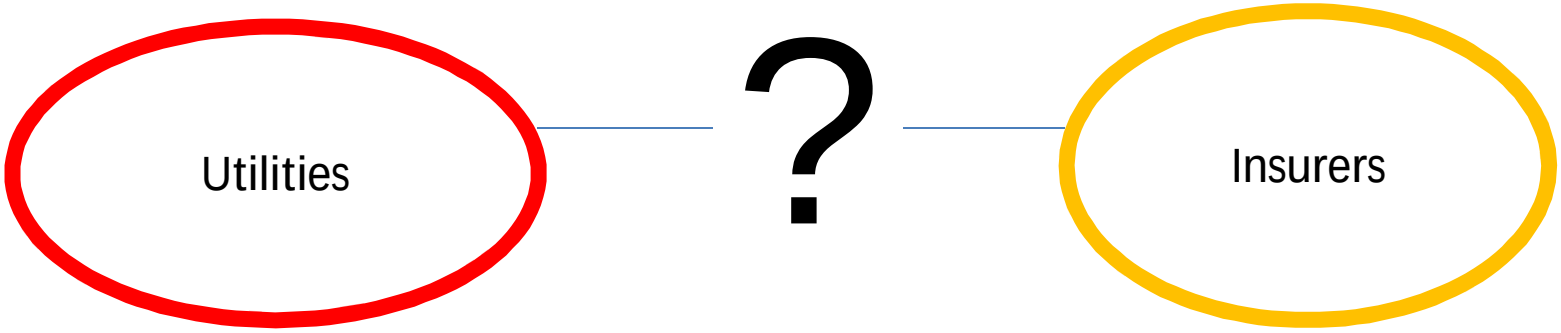
Exploring the Details of Substation Topology



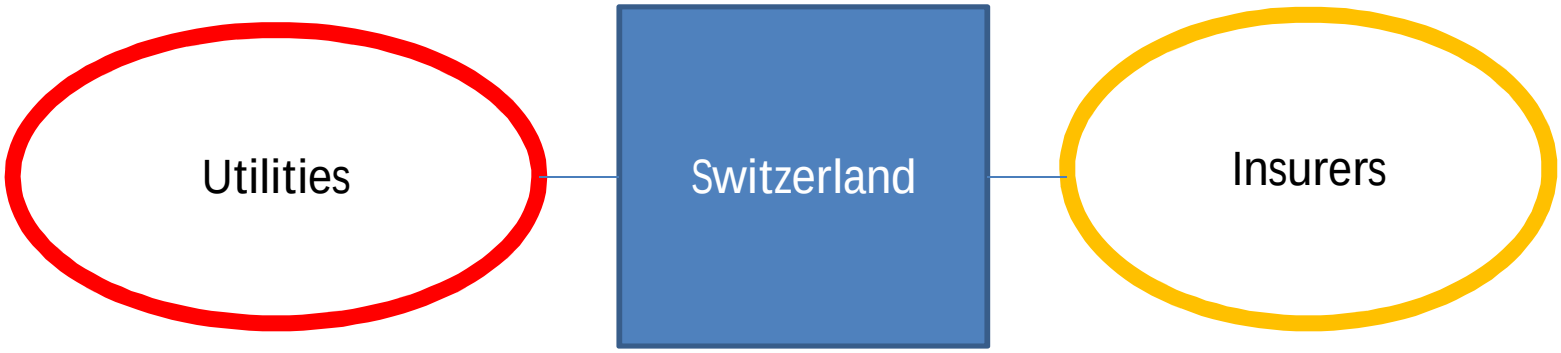


- Permutations of switching sequence that will cause maximum damage to system instability.

How does cybersecurity actuarial science inform risk hedging between utilities and insurers?



We need an independent, neutral party



Concluding Remarks

- What can we do to prevent switching/tap changing attack when IEDs and local computer systems are compromised?
- Longevity of system upgrade and how we could improve the lifecycle coordination and perhaps transition the electronic evidence into quantity of risks
- What oversight system and architecture can we do to enhance the circuit breaker operation?
- Physical security is as equal as cyber on manufacturing and operational standpoints