Securing Smart Grid Cyber Infrastructure against Emerging Threats

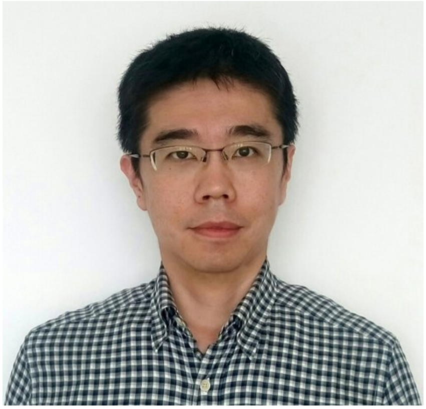
Daisuke Mashima

ADSC
ADVANCED DIGITAL SCIENCES CENTER

Version 2, WGT

Brief Bio

- Daisuke Mashima
  - PhD in Computer Science from Georgia Tech, USA
- Research Scientist at ADSC and Research affiliate at University of Illinois at Urbana Champaign since 2015
  - Smart grid security and privacy
- Formerly research scientist at Fujitsu Lab. of America
  - Smart energy and smart home IoT systems
  - Security and privacy in smart metering
  - Automated demand response and OpenADR2.0 standardization
- Award
  - Best paper award from IEEE SmartGridComm 2014
  - Silver Prize in App Contest at ACM MobiCom 2015



Advanced Digital Sciences Center

ADSC is a research center of Illinois at Singapore Pte. Ltd., an affiliate of the University of Illinois / supported by NRF's CREATE programme.

ADSC's research is led by faculty from Electrical & Computer Engineering and Computer Science

We have diverse staff of 26 full-time researchers–more than half with PhDs

We have 11 Illinois professors involved in SG

The TSCP CREATE Programme

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE
Research . Innovation . Enterprise

The Challenge

Assurance that a system is both *trustworthy* (meaning it is trusted to behave as expected, even during an accidental or intentional disruption) **and *secure*** (meaning it is hardened against malicious attacks)

CREATE Centre for a Trusted and Secure Cyber Plexus (TSCP)

Trustworthy System Architecture

Standards, Validation, Verification

Technology of Trust

Monitoring, Analysis, Interdiction and Recovery

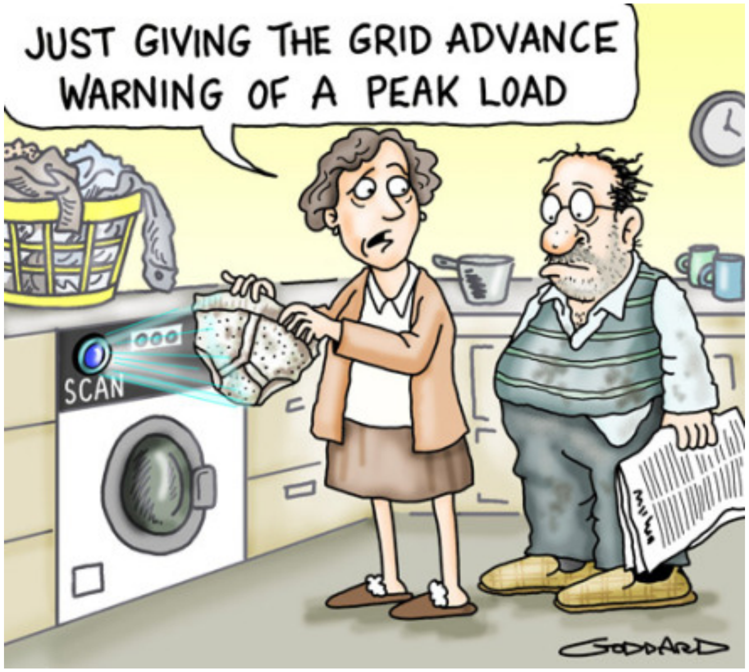
- **SUTD is Illinois' primary partner**

Outline

- About Myself and ADSC
- Smart Grid overview
- Security threats in smart grid and real-world incidents
- Introducing an additional line of defense for substation remote control
- Concluding remarks

Smart Grid

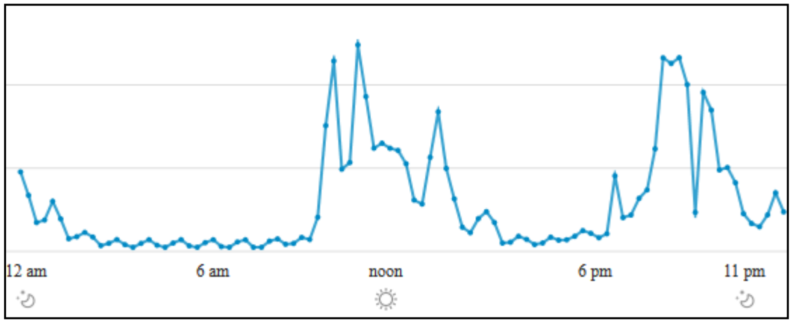
- Power grid enhanced with ICT (information and communication technologies)
  - Reliability
  - Economics
  - Efficiency
  - Environmental
  - Security
  - Safety

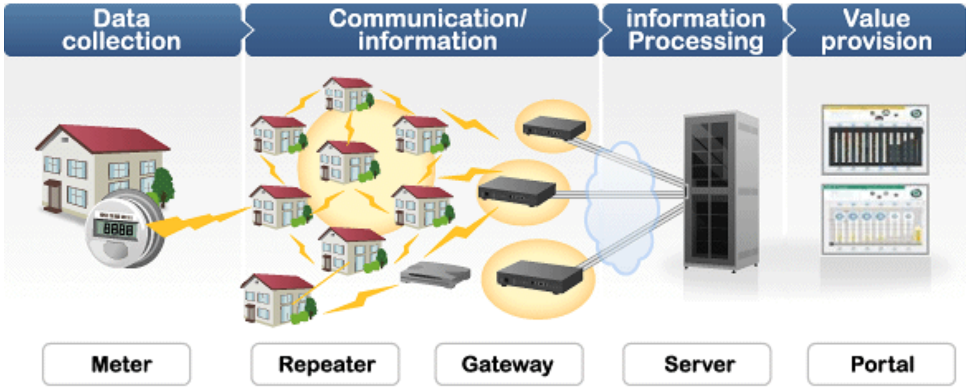


https://alittlefridaystory.com/2016/01/22/solar-power-a-new-hope/

Smart Metering

- Enable real-time electricity usage monitoring
  - Enable accurate load forecasting and further advanced services, e.g., automated demand response



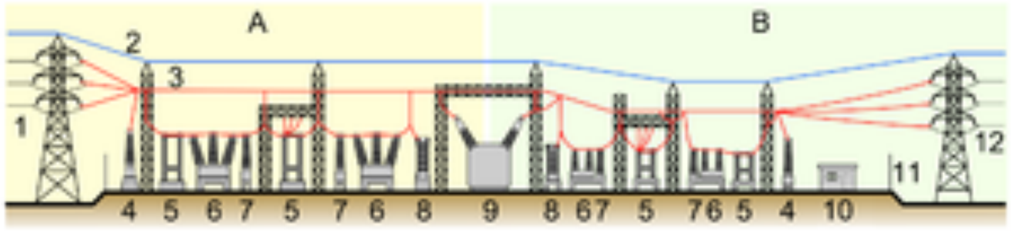


Green Button Download My Data

Green Button Connect My Data

Substation Automation and Telecontrol

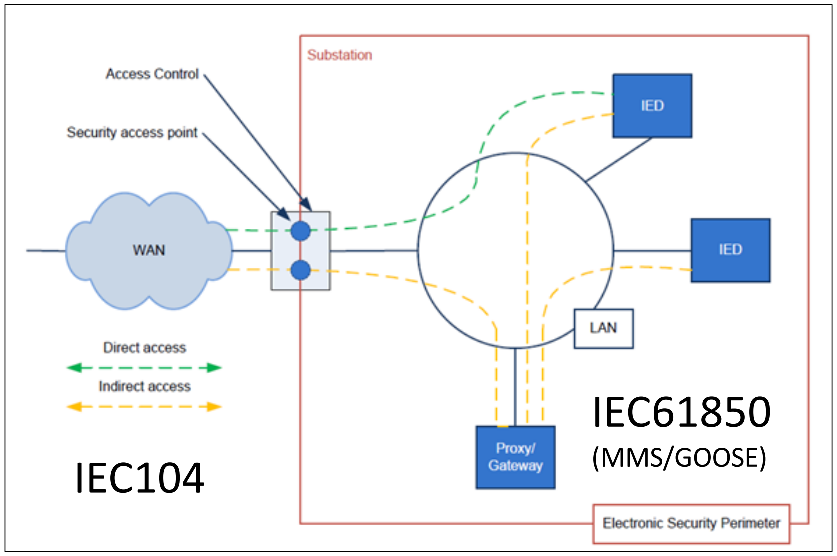
- A substation is a crucial component of an power grid system connecting generation and loads.
- Substations transform voltage from high to low, or the reverse, or perform any of several other important functions.
- Between the generating station and consumer, electric power may flow through several substations at different voltage levels.
- Over 10,000 transmission/distribution substations in Singapore



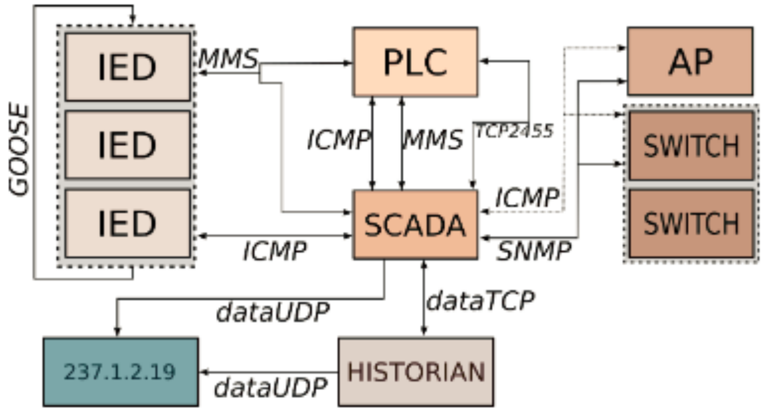
https://en.wikipedia.org/wiki/Electrical_substation

Modernization of Substations

- Adoption of standard technologies such as IEC 60870-5-104 (or IEC104) or DNP3 and IEC 61850 for remote control and automation



IEC 61850-90-2 TR: Communication networks and systems for power utility automation – Part 90-2: Using IEC 61850 for the communication between substations and control centres - Page 10



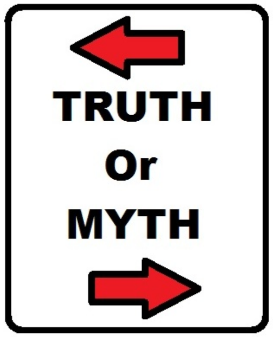
Protocols used in EPIC smart grid testbed

Ahnaf Siddiqi, Nils Ole Tippenhauer, Daisuke Mashima, and Binbin Chen, "Short Paper: On Practical Threat Scenario Testing in an Electric Power ICS Testbed." To appear at the 4th ACM Cyber-Physical System Security Workshop (ACM CPSS 2018) in June, 2018.

Remote Control Use Cases

- Load shedding
  - To handle, for instance, generator loss contingency by cutting some loads. This also could be triggered for economical purpose.
- Power shedding
  - To handle over generation from renewables, the control center controls the output from the generation and/or makes it offline
- Voltage regulation
  - Shunt reactors/capacitors are controlled (either on/off or variable setpoints) to manage voltages according to the change in loads
- Topology control
  - To optimize generation and transmission cost, power grid topology is changed.

Assumptions were…

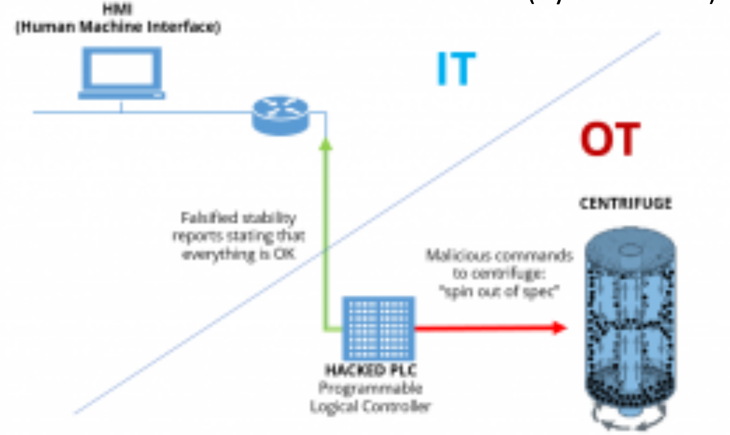


- Power grid system is secure because of “air gap”.
  - Isolation from other systems or external network eliminates possibility of cyber attacks
- Dedicated communication infrastructure
  - Network security is not considered as an issue.
  - Security for communication protocols is either not considered in the specification or optional.
    - Availability is prioritized over integrity and confidentiality

Stuxnet Worm

- First found in 2010 (“W32/Stuxnet”)
- Targeted nuclear plants in Iran
- Exploited multiple zero-day vulnerabilities on Windows
- Can infect via USB drive

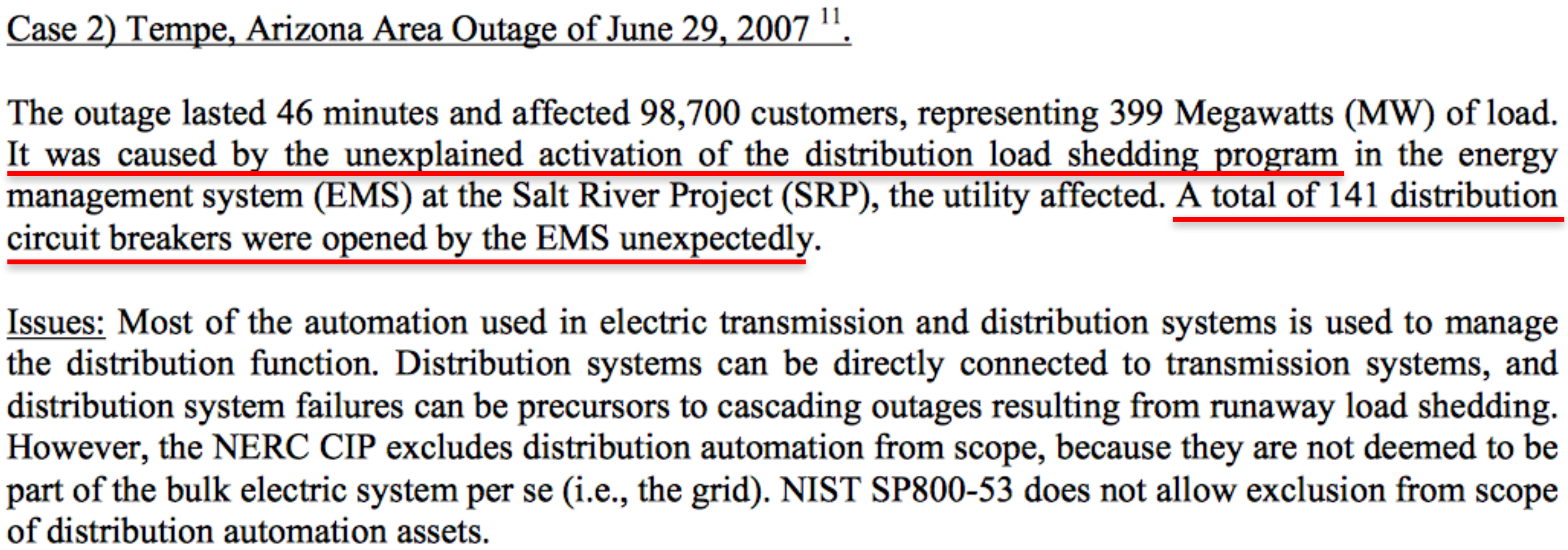
(Cyberbit.com)


HMI
(Human Machine Interface)
IT
OT
CENTRIFUGE
Falsified stability reports stating that everything is OK
Malicious commands to centrifuge: "spin out of spec"
HACKED PLC
Programmable Logical Controller

- ***Successfully bypassed the air gap and infected Siemens PLCs (programmable logic controller) that control centrifuges in nuclear plants!***

Incident in Arizona, USA

http://realtimeacs.com/wp-content/downloads/pdfs/House-Hearing-10-17-Final.pdf



Case 2) Tempe, Arizona Area Outage of June 29, 2007 [11].

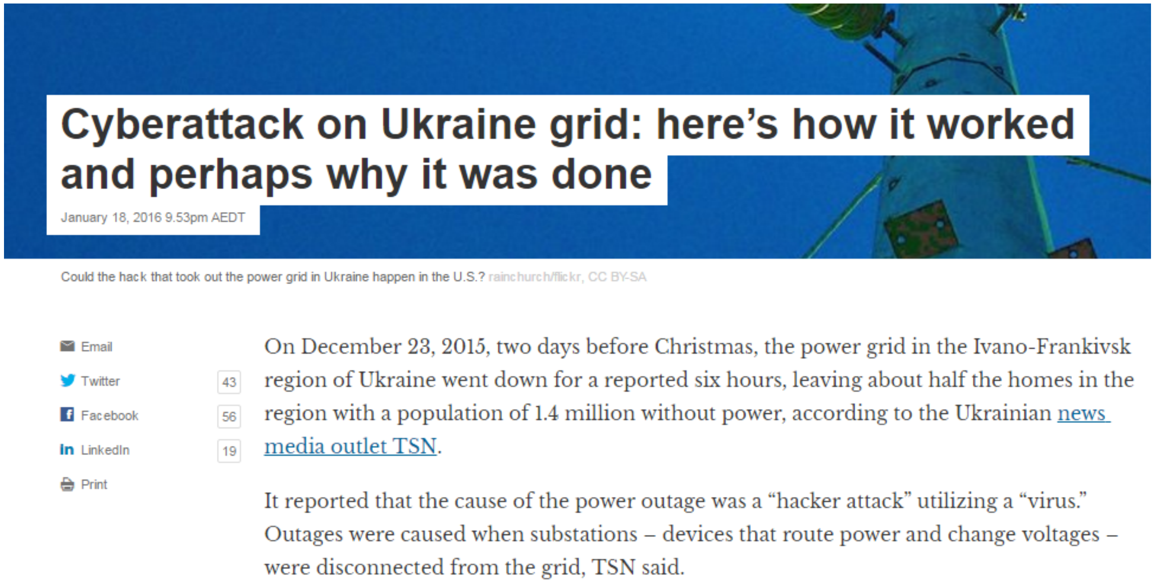
The outage lasted 46 minutes and affected 98,700 customers, representing 399 Megawatts (MW) of load. It was caused by the unexplained activation of the distribution load shedding program in the energy management system (EMS) at the Salt River Project (SRP), the utility affected. A total of 141 distribution circuit breakers were opened by the EMS unexpectedly.

Issues: Most of the automation used in electric transmission and distribution systems is used to manage the distribution function. Distribution systems can be directly connected to transmission systems, and distribution system failures can be precursors to cascading outages resulting from runaway load shedding. However, the NERC CIP excludes distribution automation from scope, because they are not deemed to be part of the bulk electric system per se (i.e., the grid). NIST SP800-53 does not allow exclusion from scope of distribution automation assets.

- **Although this was not caused by cyber attack, if the same system gets attacked, the similar consequence is expected.**

Ukraine Power Plant Attacks

- In 2015, Ukraine power grid got affected by cyberattack, which resulted in massive power outage.



Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done

January 18, 2016 9.53pm AEDT

Could the hack that took out the power grid in Ukraine happen in the U.S.? rainchurch/flickr, CC BY-SA

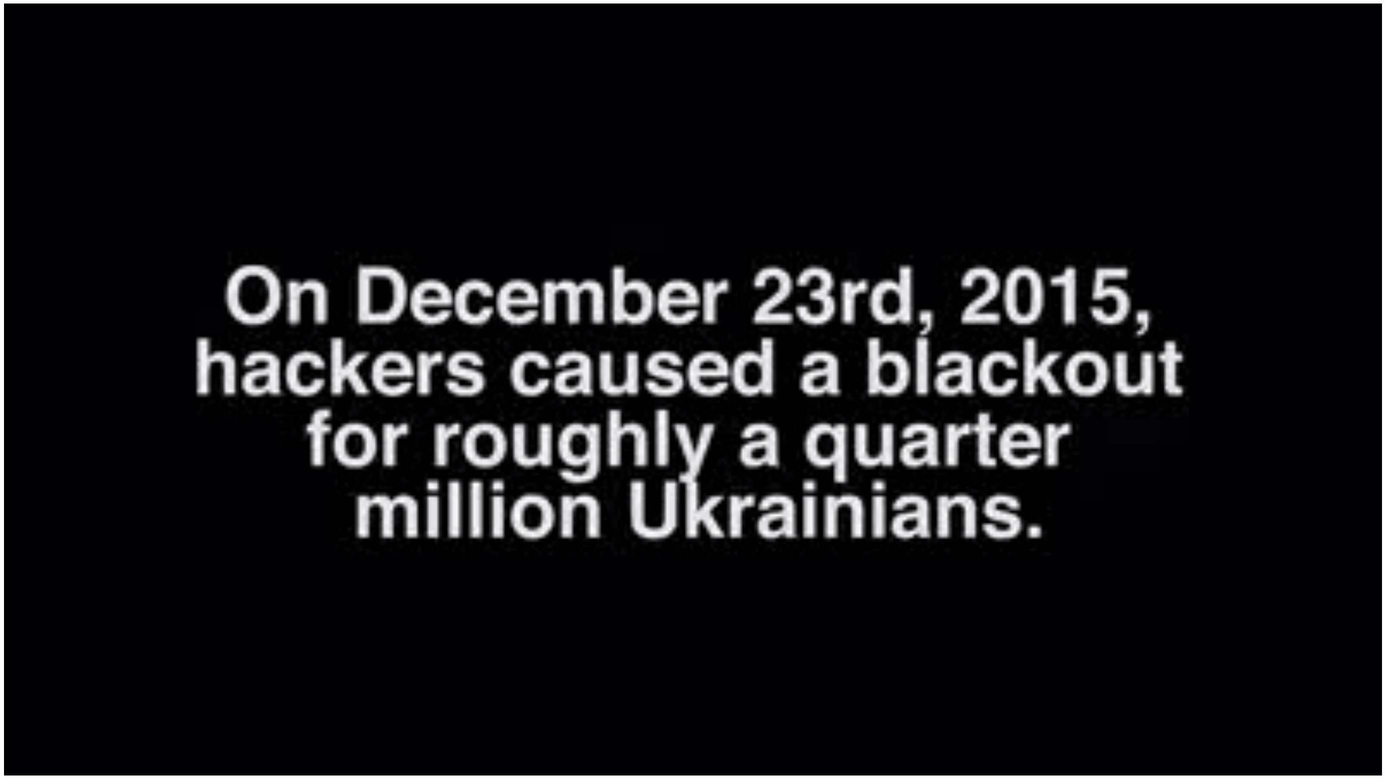
On December 23, 2015, two days before Christmas, the power grid in the Ivano-Frankivsk region of Ukraine went down for a reported six hours, leaving about half the homes in the region with a population of 1.4 million without power, according to the Ukrainian news media outlet TSN.

It reported that the cause of the power outage was a "hacker attack" utilizing a "virus." Outages were caused when substations – devices that route power and change voltages – were disconnected from the grid, TSN said.

http://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802

- **Started 6-month before the attack in December!**
- **Email with malicious files to targeted employees**
- **Malware for remotely controlling computers**
- **Malicious firmware update for slowing down recovery**
- **DoS attacks against the customer call center**

Ukraine Power Plant Attacks

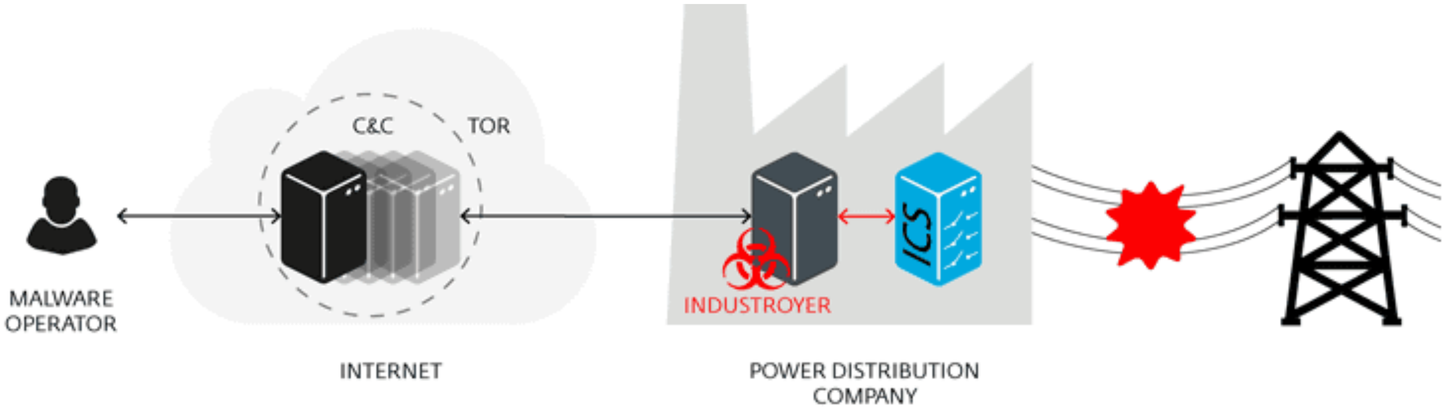


On December 23rd, 2015, hackers caused a blackout for roughly a quarter million Ukrainians.

(https://www.youtube.com/watch?v=8ThgK1WXUgk)

CrashOverride / Industroyer

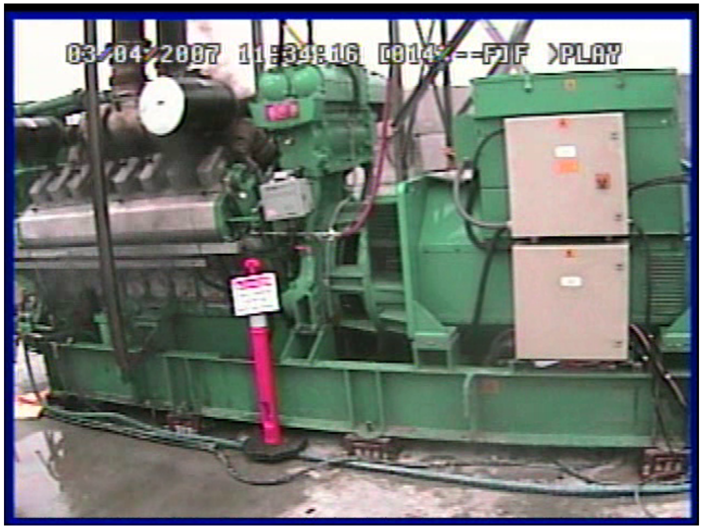
- Reported that it was used in Ukraine attack in 2016
- Abuses widely-used ICS protocols, including IEC 104 and IEC 61850
  - Capable of issuing valid commands to field devices



https://gigazine.net/news/20170613-crashoverride/

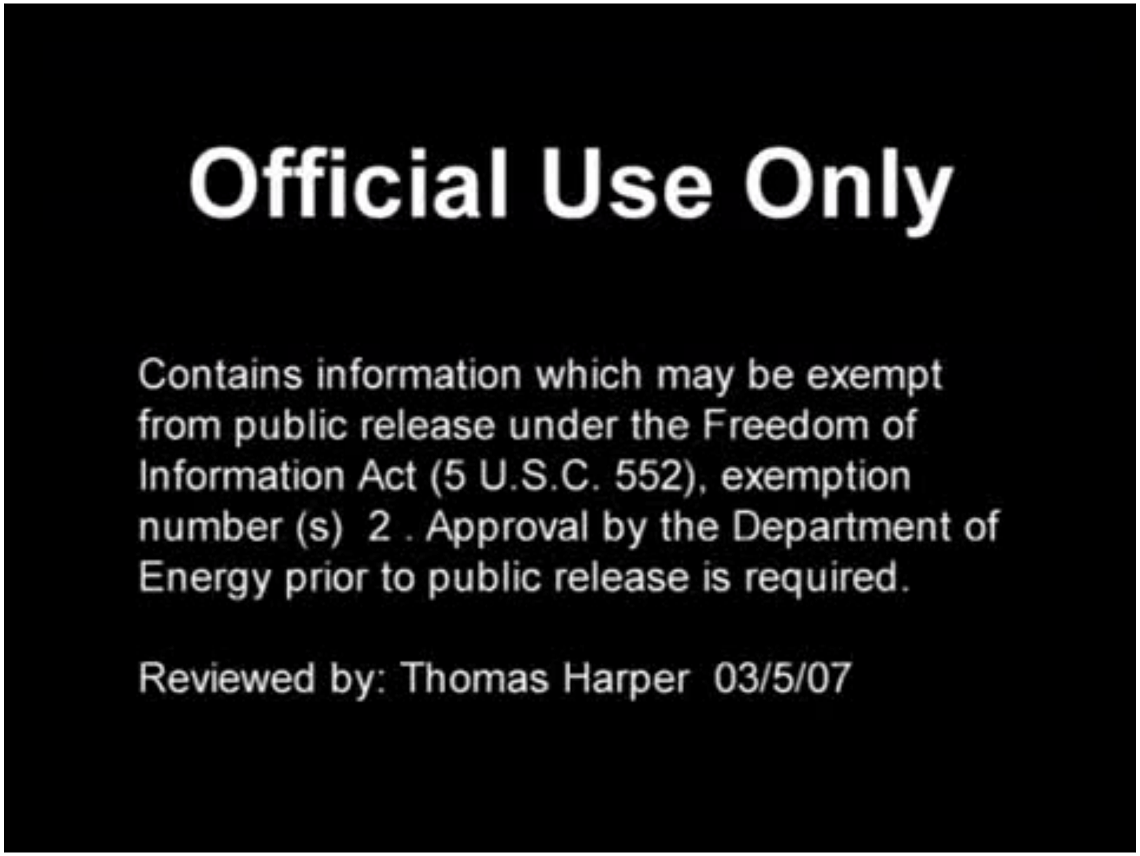
Aurora Generator Test

- Conducted by Idaho National Lab in 2007 to demonstrate how a cyber-originated attack can damage physical power grid components.
- By opening and closing circuit breakers, the attack succeeded in explode a diesel generator!



https://en.wikipedia.org/wiki/Aurora_Generator_Test

Aurora Generator Test



Official Use Only

Contains information which may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number (s) 2 . Approval by the Department of Energy prior to public release is required.

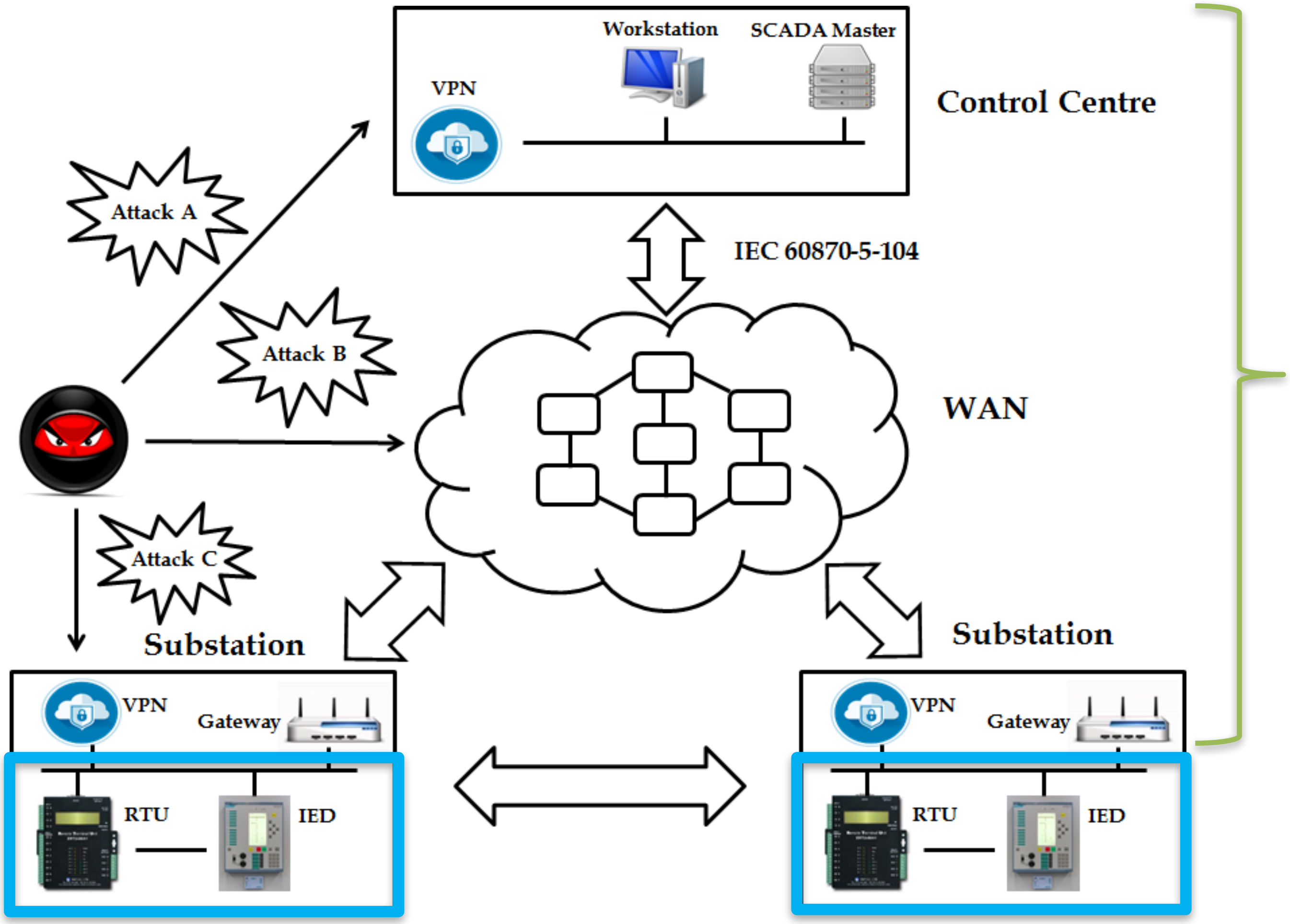
Reviewed by: Thomas Harper 03/5/07

(https://www.youtube.com/watch?v=LM8kLaJ2NDU&t=12s)

Man-in-the-middle Attacks

- Insecure deployment of IEC 60870 and 61850 is vulnerable against man-in-the-middle attacks, replay attacks, etc.
  - B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andren, C. Seitl, F. Kupzog, and T. Strasser. Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations. In Emerging Technologies & Factory Automation (ETFA), 2015 IEEE 20th Conference on, pages 1–8. IEEE, 2015.
  - P. Maynard, K. McLaughlin, and B. Haberler. Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks. In Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research 2014, pages 30–42. BCS, 2014.
- Compromise of cellular communication channel.
  - D. Perez and J. Pico. A Practical Attack against GPRS/EDGE/UMTS/HSPA Mobile Data Communication. In Blackhat DC, 2011.

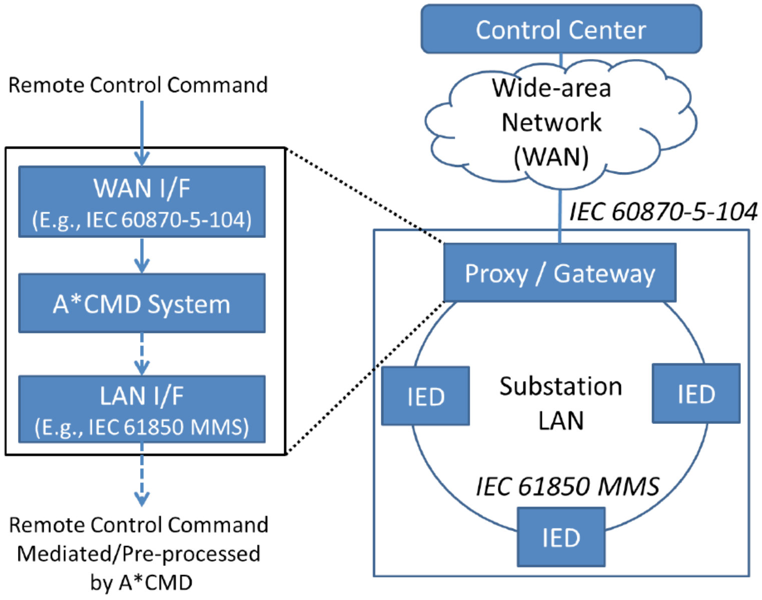
Additional Line of Defense



Authentication
Access Control
Security Patch
Anti-virus
Firewall
Intrusion Detection
IEC 62351
Etc.

Active Command Mediation

- Add additional-layer of security for securing remote control interface of substation
  - Inspect and "pre-process" incoming remote control commands
    - Should work autonomously
  - Can not be bypassed
- Practically-deployable solution
  - Require minimal change on existing infrastructure
  - Add minimal overheads and dependency on other systems



Remote Control Command

WAN I/F
(E.g., IEC 60870-5-104)

A*CMD System

LAN I/F
(E.g., IEC 61850 MMS)

Remote Control Command
Mediated/Pre-processed
by A*CMD

Control Center

Wide-area
Network
(WAN)

IEC 60870-5-104

Proxy / Gateway

IED

Substation
LAN

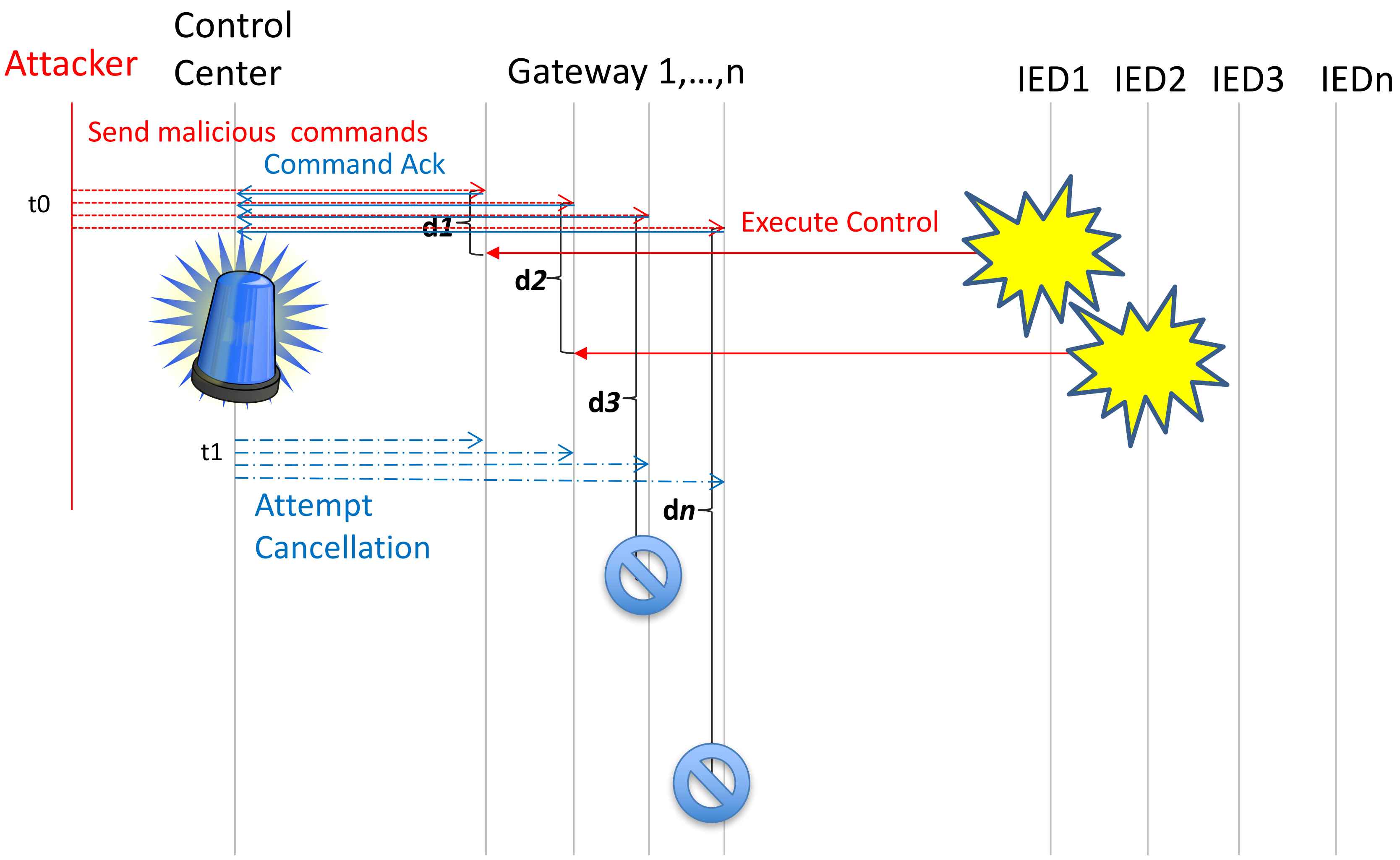
IED

IEC 61850 MMS

IED

Daisuke Mashima, Prageeth Gunathilaka, and Binbin Chen, "**An Active Command Mediation Approach for Securing Remote Control Interface of Substations**."
In Proc. of IEEE SmartGridComm 2016 in November, 2016.
Daisuke Mashima, Prageeth Gunathilaka, and Binbin Chen, **"Artificial Command-delaying for Securing Substation Remote Control: Design and Implementation."** In press for IEEE Transactions on Smart Grid.

Artificial Command-delaying



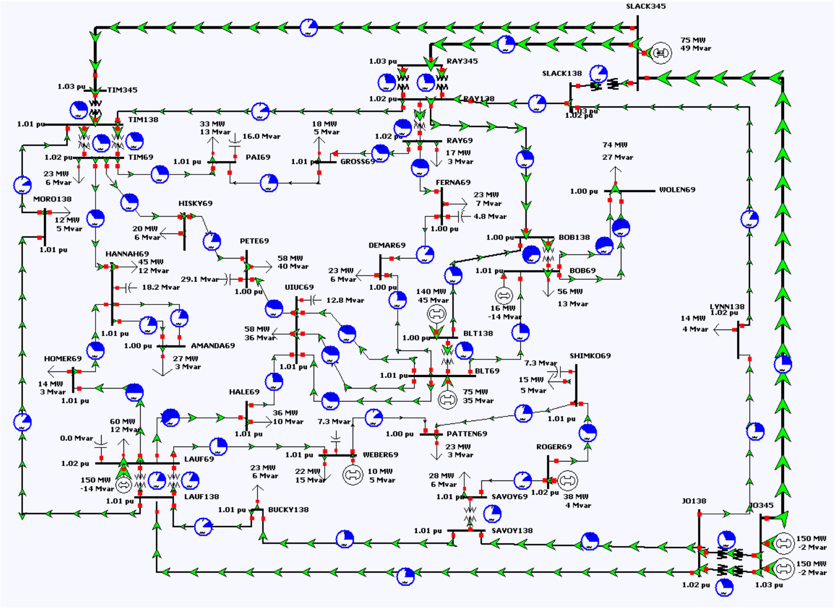
Attack Detection Mechanisms

- Deployed outside of substations (e.g., Control center)
  - Centralized semantic command analysis based on power flow simulation
    - Hui Lin, Adam Slagell, Zbigniew Kalbarczyk, Peter W. Sauer, and Ravishankar K. Iyer, "Runtime Semantic Security Analysis to Detect and Mitigate Control-related Attacks in Power Grids," in *IEEE Transactions on Smart Grid*, vol.PP, no.99, pp.1-1, doi:10.1109/TSG.2016.2547742.
    - Detection time could be up to 600ms, while offering very high detection rate and low false positive rate
  - Simple, command history-based detection
    - Detection time can be very short (less than 10ms), but has some limitations
  - Use of on-the-fly transient-state power-flow simulation for command authentication **[Work in progress]**
    - Aim at detecting attacks that could bypass detection using steady-state simulation. Processing time is around 1 second when we simulate 37-bus system on an off-the-shelf simulator

- Deployed within each substation
  - Command authentication using distributed state estimation and faster-than-real-time simulation
    - Meliopoulos, Sakis, et al. "Command authentication via faster than real time simulation." *Power and Energy Society General Meeting (PESGM), 2016*. IEEE, 2016.
  - Fully-autonomous detection based on local measurements **[Work in progress]**

Setup for Preliminary Simulation Study

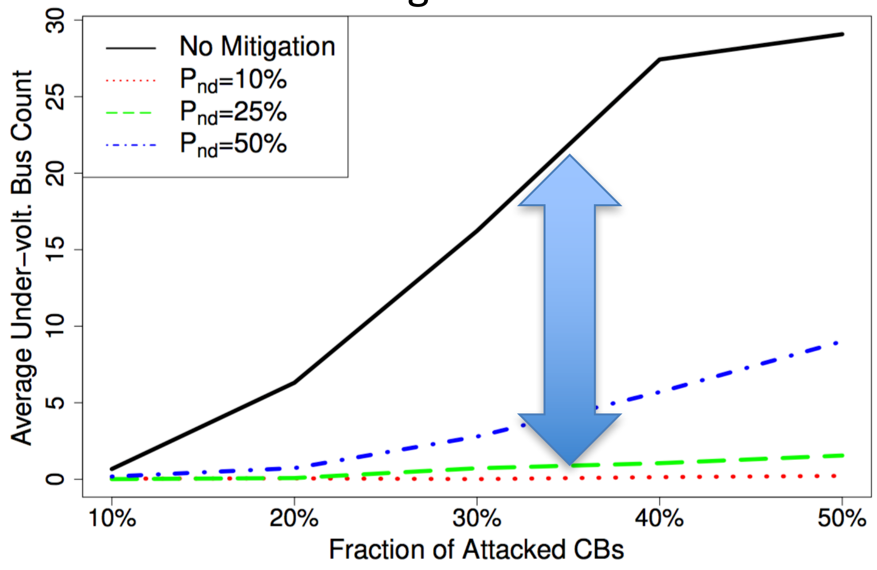
- PowerWorld Simulator
  - Transient stability analysis
  - GSO 37-bus system
    - 57 transmission lines
- Probabilistic, discrete delay
  - Constant delay is added with a certain probability
- Very accurate attack detection algorithm
  - Assume that all delayed attack commands are cancelled.
- Simulate attacks against circuit breakers
  - Issue open commands to randomly selected circuit breakers
- Metrics of attack impact on power grid
  - Voltage violation
  - Frequency violation
  - Reduction in load (Unserved Load)



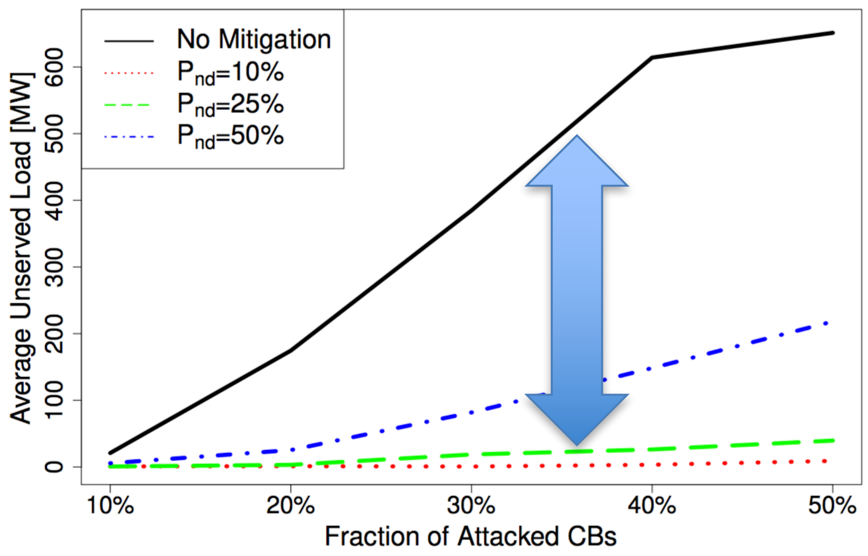
37-bus system on PowerWorld

Simulation Results

Voltage Violation



Unserved Load



- Over 90% mitigation in # of buses with voltage violation and unserved load
- Same level of mitigation is observed in frequency violation

General Guidelines for Latency

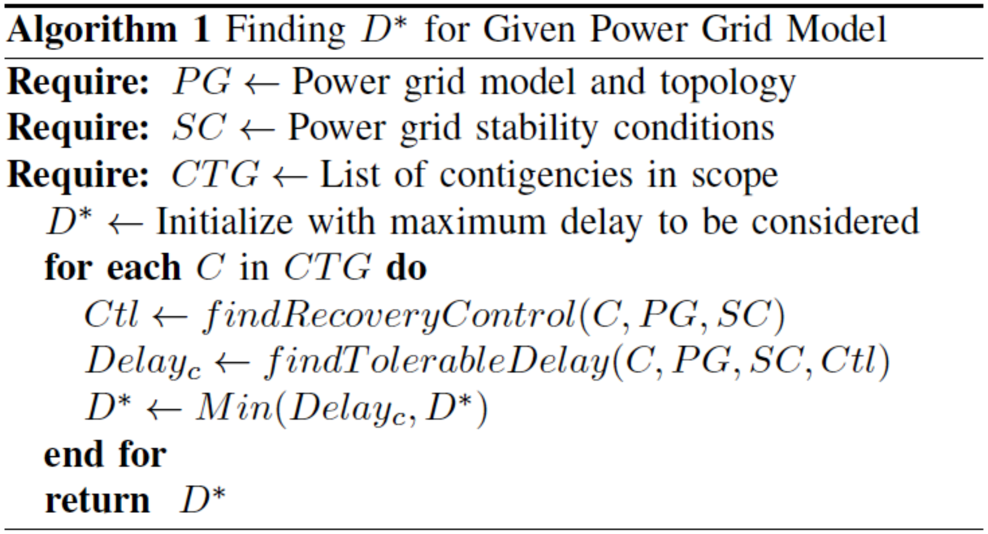
- IEEE PES Guideline
  - Communication for line sectionalizing: **5 seconds**
  - Communication for load shedding: **10 seconds**
  - Communication for transfer switching: **1 second**
- US DoE guideline
- Survey done by academia

Delaying in Remote Control Use Cases

- Topology Control?
  - Since it is triggered mainly for cost optimization purpose, delaying the operation does not cause stability issue.
- Voltage regulation?
  - Control of shunt reactors is said to be done manually twice a day (morning and evening). Again not considered very time sensitive.
- Power/load shedding may need further investigation.

Finding Delay Tolerance

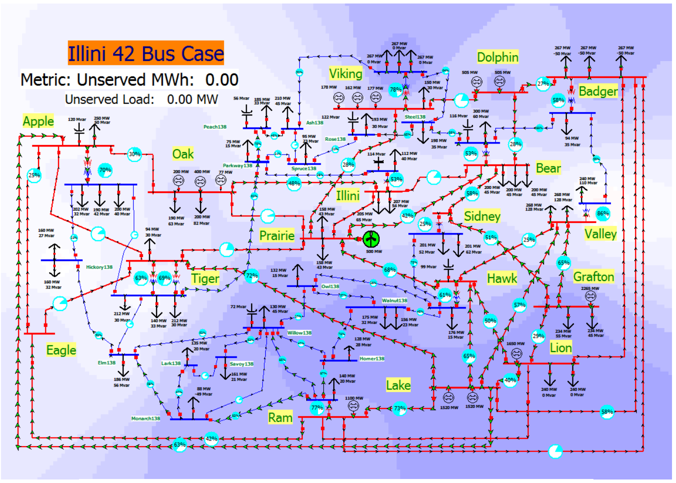
- How much artificial delay can be introduced without causing grid instability.
- Each power grid model has different delay tolerance

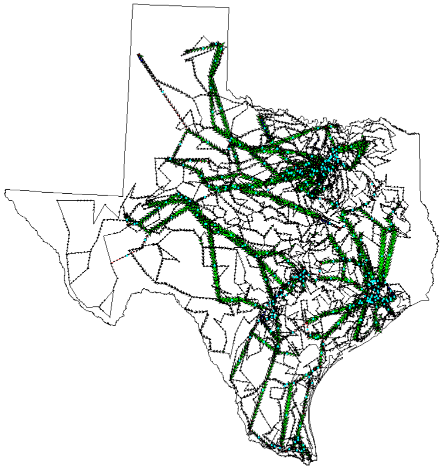


```
Algorithm 1 Finding $D^*$ for Given Power Grid Model
Require: $PG \leftarrow$ Power grid model and topology
Require: $SC \leftarrow$ Power grid stability conditions
Require: $CTG \leftarrow$ List of contigencies in scope
  $D^* \leftarrow$ Initialize with maximum delay to be considered
  for each $C$ in $CTG$ do
    $Ctl \leftarrow findRecoveryControl(C, PG, SC)$
    $Delay_c \leftarrow findTolerableDelay(C, PG, SC, Ctl)$
    $D^* \leftarrow Min(Delay_c, D^*)$
  end for
  return $D^*$
```

Delaying Load Shedding Commands

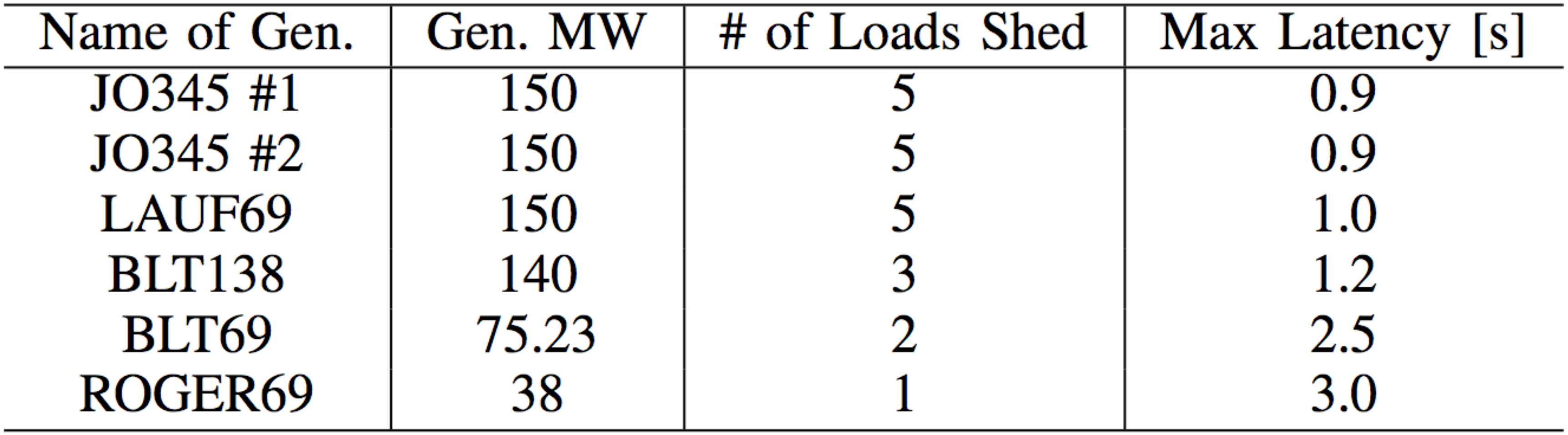
- Using three different case files (37-,42-,2000-bus systems), simulated generation loss scenarios (*CTG*)
- For each case:
  - Find a set of loads to be shed to avoid violation (*Ctl*)
  - Repeat simulation with different delay to find the maximum delay that can be added without causing violation (*findTolerableDelay*)





GSO 37-bus Experiments (1)

- Experiments corresponding to N-1 contingencies

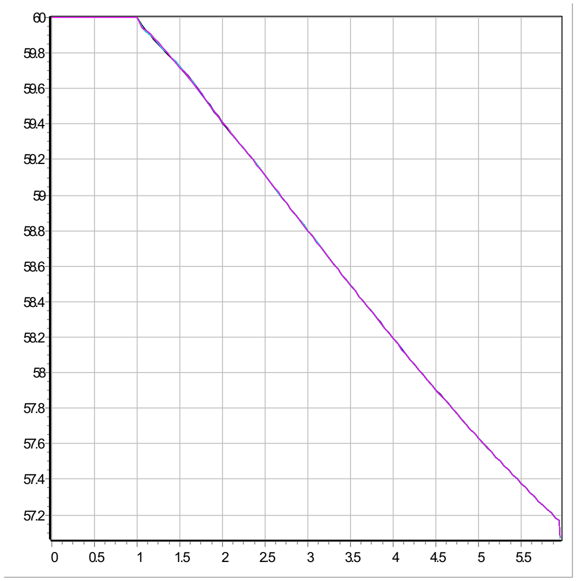


Name of Gen.	Gen. MW	# of Loads Shed	Max Latency [s]
JO345 #1	150	5	0.9
JO345 #2	150	5	0.9
LAUF69	150	5	1.0
BLT138	140	3	1.2
BLT69	75.23	2	2.5
ROGER69	38	1	3.0

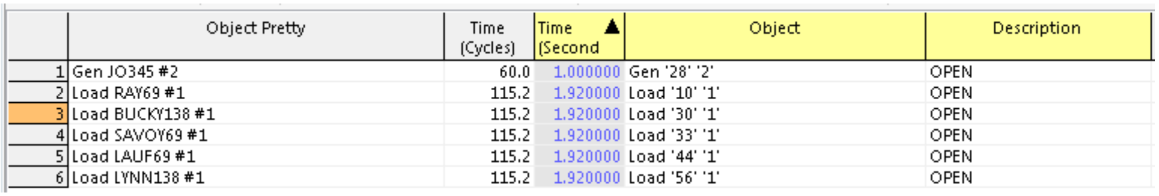
- Delaying by **0.9 second** does not cause violation for all cases

GSO 37-bus Experiments (2)

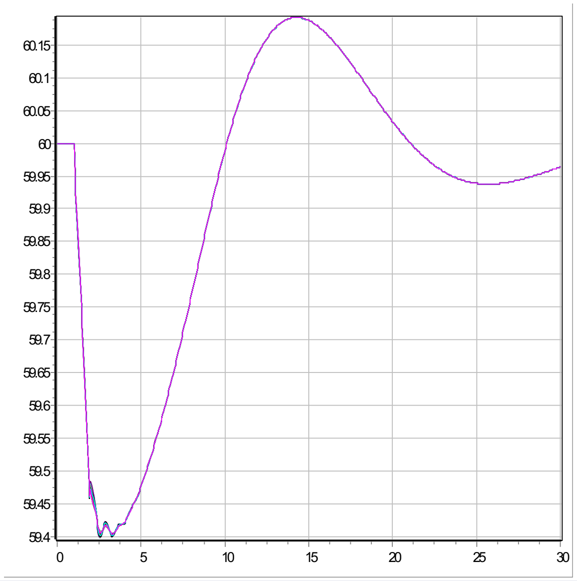
No recovery control



With recovery control



	Object Pretty	Time (Cycles)	Time ▲ (Second	Object	Description
1	Gen JO345 #2	60.0	1.000000	Gen '28' '2'	OPEN
2	Load RAY69 #1	115.2	1.920000	Load '10' '1'	OPEN
3	Load BUCKY138 #1	115.2	1.920000	Load '30' '1'	OPEN
4	Load SAVOY69 #1	115.2	1.920000	Load '33' '1'	OPEN
5	Load LAUF69 #1	115.2	1.920000	Load '44' '1'	OPEN
6	Load LYNN138 #1	115.2	1.920000	Load '56' '1'	OPEN



Delaying Power Shedding Commands

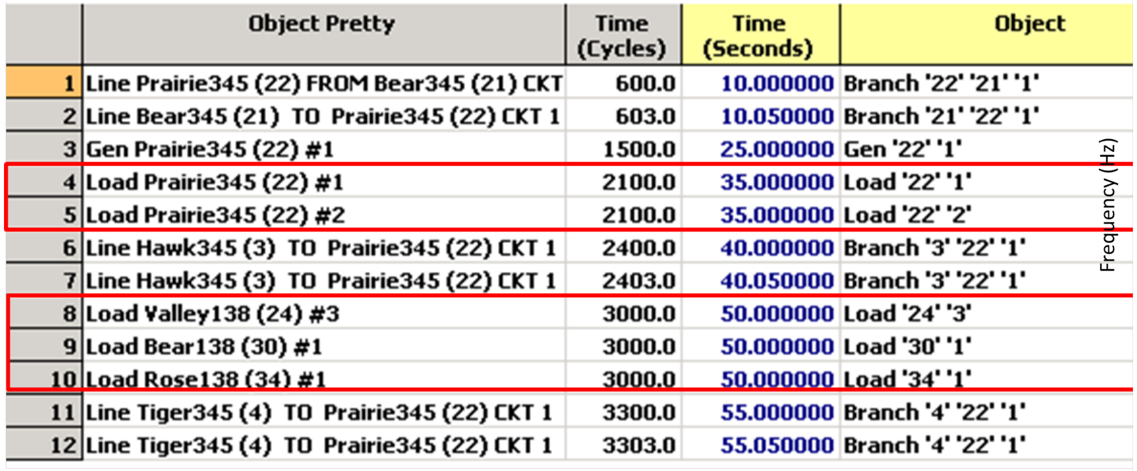
- 37-bus system on PowerWorld
  - Increased generation of generators by 100MW in total
  - Performed transient state simulation for evaluating with recovery controls at different timings
  - If recovery is done within **5.5 seconds**, no violation is observed.

Experiments with Larger Case

- Performed similar experiments with Illini 42-bus system
  - Delaying by **1 second** does not cause violation
- For Texas 2000-bus system, focused on the top-4 largest generators and simulated loss of them.
  - Used tighter stability constraints (0.4Hz deviation)
  - Delaying by **0.7 second** does not cause violation

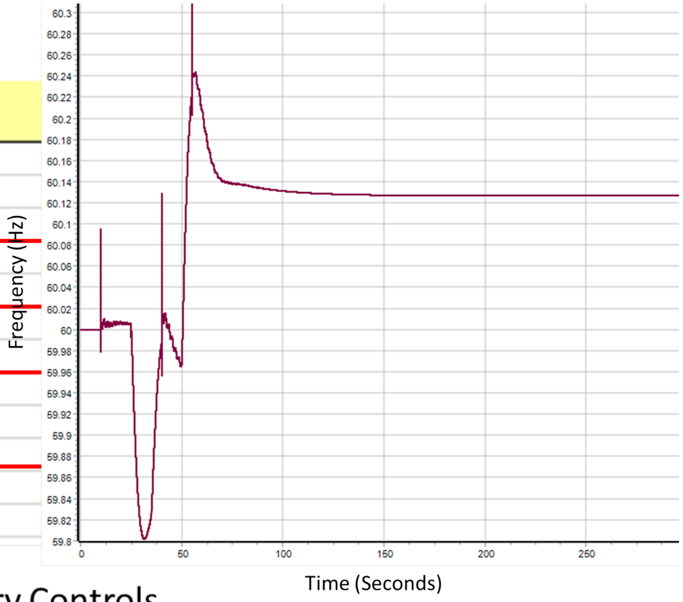
Delaying in Realistic Contingency

- Used Illini 42 Tornado Case
  - Inserted load shedding controls with varying delay and ran transient state simulation to see if blackout occurred.
  - Found that **10-second** delay was acceptable.



	Object Pretty	Time (Cycles)	Time (Seconds)	Object
1	Line Prairie345 (22) FROM Bear345 (21) CKT	600.0	10.000000	Branch '22' '21' '1'
2	Line Bear345 (21) TO Prairie345 (22) CKT 1	603.0	10.050000	Branch '21' '22' '1'
3	Gen Prairie345 (22) #1	1500.0	25.000000	Gen '22' '1'
4	Load Prairie345 (22) #1	2100.0	35.000000	Load '22' '1'
5	Load Prairie345 (22) #2	2100.0	35.000000	Load '22' '2'
6	Line Hawk345 (3) TO Prairie345 (22) CKT 1	2400.0	40.000000	Branch '3' '22' '1'
7	Line Hawk345 (3) TO Prairie345 (22) CKT 1	2403.0	40.050000	Branch '3' '22' '1'
8	Load Valley138 (24) #3	3000.0	50.000000	Load '24' '3'
9	Load Bear138 (30) #1	3000.0	50.000000	Load '30' '1'
10	Load Rose138 (34) #1	3000.0	50.000000	Load '34' '1'
11	Line Tiger345 (4) TO Prairie345 (22) CKT 1	3300.0	55.000000	Branch '4' '22' '1'
12	Line Tiger345 (4) TO Prairie345 (22) CKT 1	3303.0	55.050000	Branch '4' '22' '1'

(1) List of Pre-defined Contingencies and Added Recovery Controls

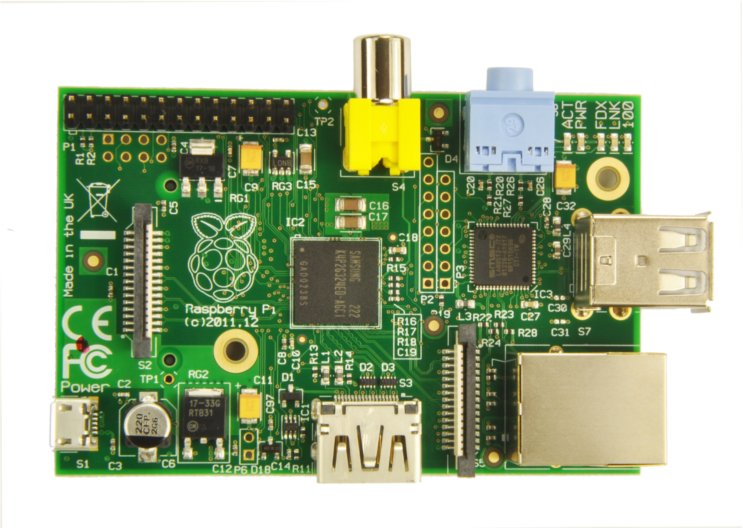


(2) Frequency Change with Load Shedding

ADSC
ADVANCED DIGITAL SCIENCES CENTER

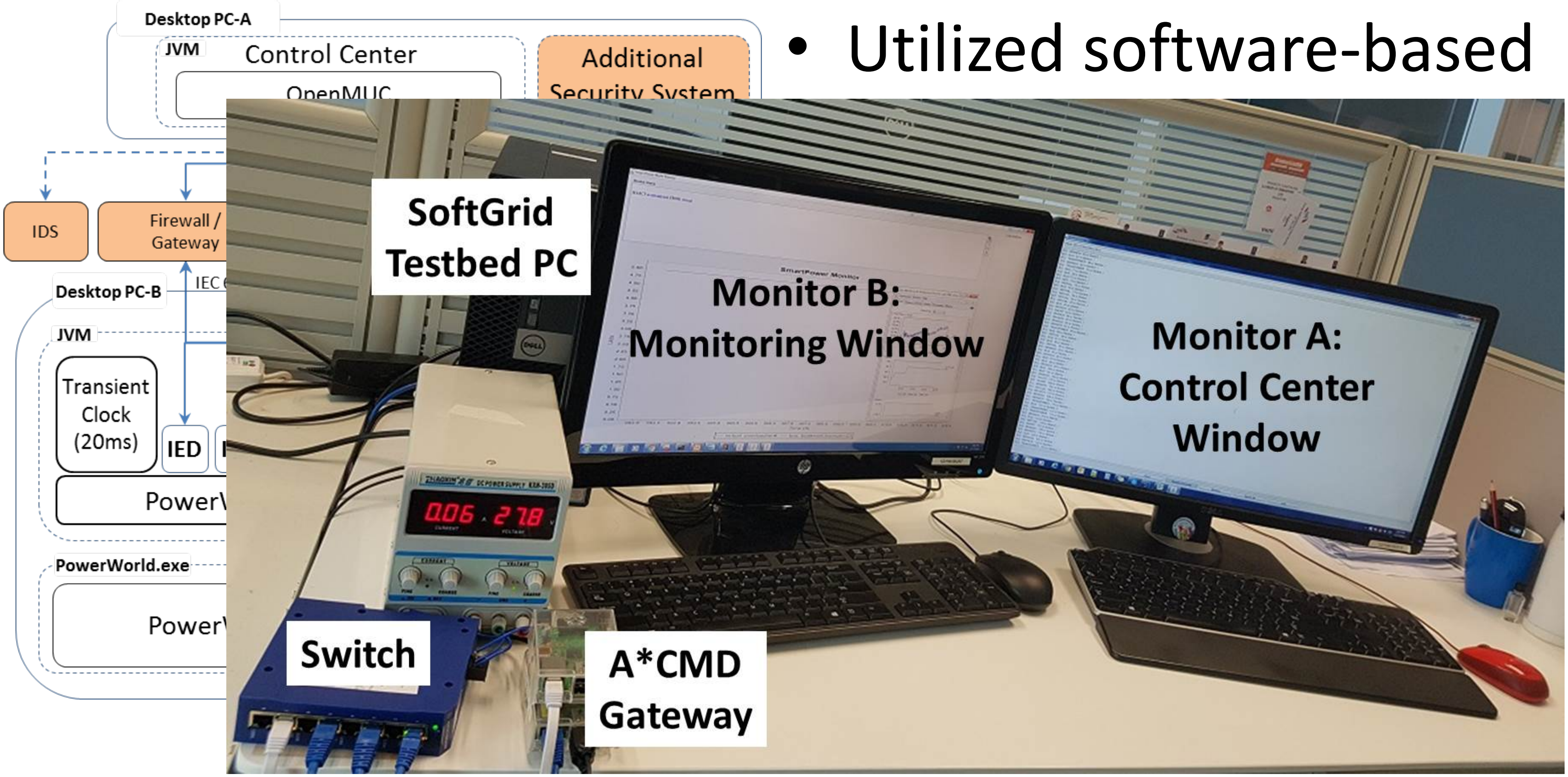
A*CMD-Pi: Prototype Implementation

- Implemented on Raspberry Pi
  - Low-cost (Available from <$10)
  - Spec/hardware similar to commercial protocol translators
    - 700MHz ARM, 512MB RAM
- Implemented in Java
- OpenMUC library
  - For IEC 60870-5-104, 61850



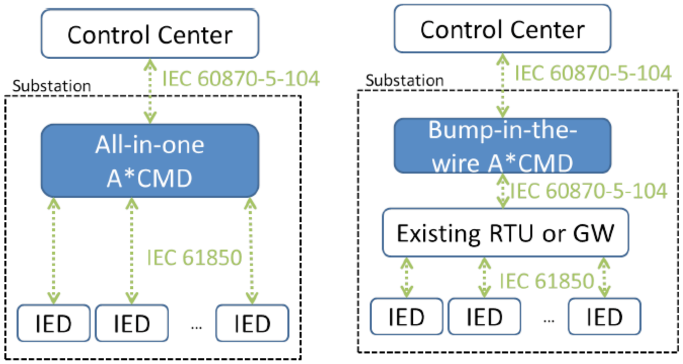
SoftGrid System Architecture

- Utilized software-based



SoftGrid project web site: http://www.illinois.adsc.com.sg/softgrid/

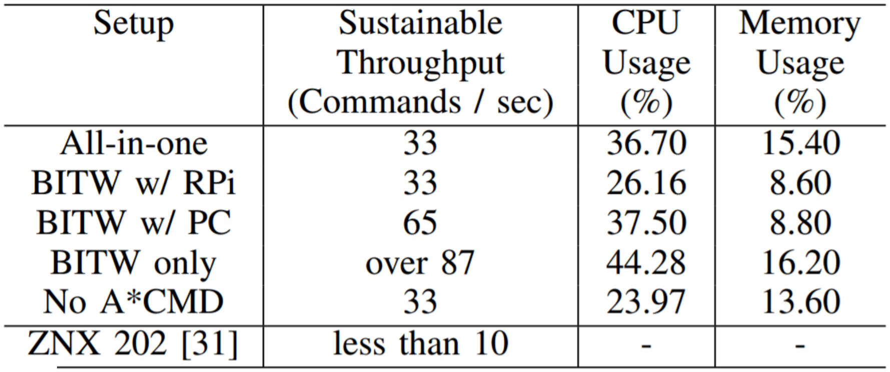
Evaluation of A*CMD-Pi



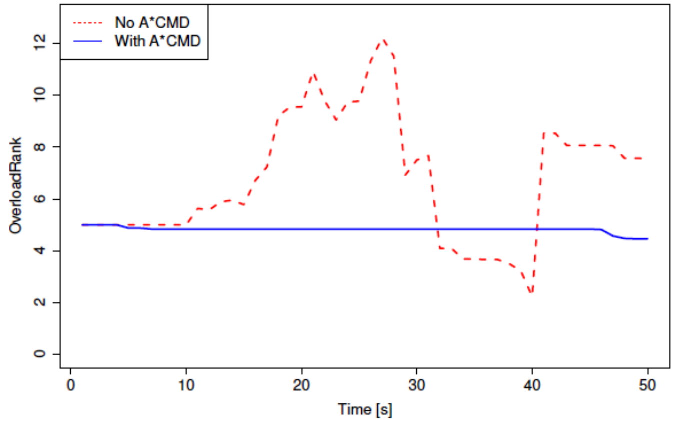
(a) All-in-one

(b) Bump-in-the-wire (BITW)

Table II
PERFORMANCE MEASUREMENTS



Setup	Sustainable Throughput (Commands / sec)	CPU Usage (%)	Memory Usage (%)
All-in-one	33	36.70	15.40
BITW w/ RPi	33	26.16	8.60
BITW w/ PC	65	37.50	8.80
BITW only	over 87	44.28	16.20
No A*CMD	33	23.97	13.60
ZNX 202 [31]	less than 10	-	-



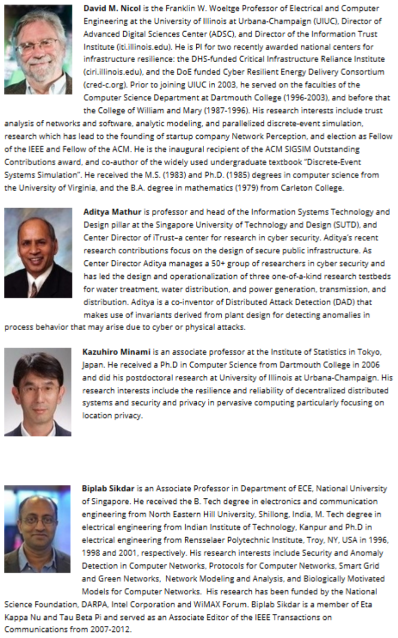
Without A*CMD in place, power flow is dramatically affected by malicious control commands. (red line)

Concluding Remarks

- Modernization of power grid has changed threat models and security assumptions.
- We observed a number of real-world incidents in the recent years.
- Given the criticality of the system, defense-in-depth is crucial.
  – Discussed an additional line of defense utilizing tolerable, artificial command-delaying

Mini-symposium on Cyber Security

- Scheduled on May 25, 2018, as part of IEEE PES ISGT Asia 2018 conference in Suntec.
  - http://sites.ieee.org/isgt-asia-2018/programs/mini-symposium/

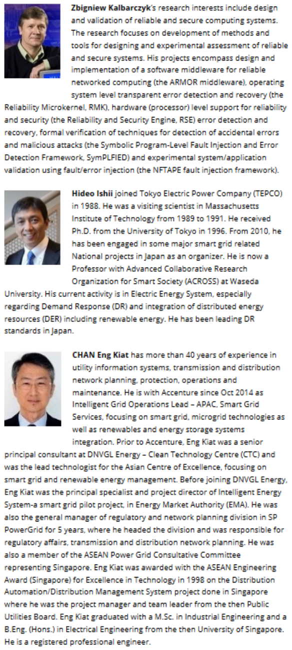


David M. Nicol is the Franklin W. Woeltge Professor of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign (UIUC), Director of Advanced Digital Sciences Center (ADSC), and Director of the Information Trust Institute (iti.illinois.edu). He is PI for two recently awarded national centers for infrastructure resilience: the DHS-funded Critical Infrastructure Reliance Institute (ciri.illinois.edu), and the DoE funded Cyber Resilient Energy Delivery Consortium (cred-c.org). Prior to joining UIUC in 2003, he served on the faculties of the Computer Science Department at Dartmouth College (1996-2003), and before that the College of William and Mary (1987-1996). His research interests include trust analysis of networks and software, analytic modeling, and parallelized discrete-event simulation, research which has lead to the founding of startup company Network Perception, and election as Fellow of the IEEE and Fellow of the ACM. He is the inaugural recipient of the ACM SIGSIM Outstanding Contributions award, and co-author of the widely used undergraduate textbook "Discrete-Event Systems Simulation". He received the M.S. (1983) and Ph.D. (1985) degrees in computer science from the University of Virginia, and the B.A. degree in mathematics (1979) from Carleton College.

Aditya Mathur is professor and head of the Information Systems Technology and Design pillar at the Singapore University of Technology and Design (SUTD), and Center Director of iTrust–a center for research in cyber security. Aditya's recent research contributions focus on the design of secure public infrastructure. As Center Director Aditya manages a 50+ group of researchers in cyber security and has led the design and operationalization of three one-of-a-kind research testbeds for water treatment, water distribution, and power generation, transmission, and distribution. Aditya is a co-inventor of Distributed Attack Detection (DAD) that makes use of invariants derived from plant design for detecting anomalies in process behavior that may arise due to cyber or physical attacks.

Kazuhiro Minami is an associate professor at the Institute of Statistics in Tokyo, Japan. He received a Ph.D in Computer Science from Dartmouth College in 2006 and did his postdoctoral research at University of Illinois at Urbana-Champaign. His research interests include the resilience and reliability of decentralized distributed systems and security and privacy in pervasive computing particularly focusing on location privacy.

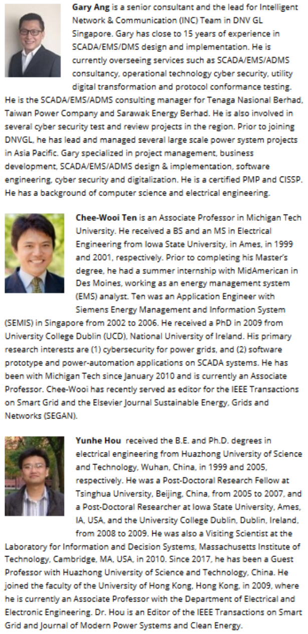
Biplab Sikdar is an Associate Professor in Department of ECE, National University of Singapore. He received the B. Tech degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, M. Tech degree in electrical engineering from Indian Institute of Technology, Kanpur and Ph.D in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA in 1996, 1998 and 2001, respectively. His research interests include Security and Anomaly Detection in Computer Networks, Protocols for Computer Networks, Smart Grid and Green Networks, Network Modeling and Analysis, and Biologically Motivated Models for Computer Networks. His research has been funded by the National Science Foundation, DARPA, Intel Corporation and WiMAX Forum. Biplab Sikdar is a member of Eta Kappa Nu and Tau Beta Pi and served as an Associate Editor of the IEEE Transactions on Communications from 2007-2012.



Zbigniew Kalbarczyk's research interests include design and validation of reliable and secure computing systems. The research focuses on development of methods and tools for designing and experimental assessment of reliable and secure systems. His projects encompass design and implementation of a software middleware for reliable networked computing (the ARMOR middleware), operating system level transparent error detection and recovery (the Reliability Microkernel, RMK), hardware (processor) level support for reliability and security (the Reliability and Security Engine, RSE) error detection and recovery, formal verification of techniques for detection of accidental errors and malicious attacks (the Symbolic Program-Level Fault Injection and Error Detection Framework, SymPLFIED) and experimental system/application validation using fault/error injection (the NFTAPE fault injection framework).

Hideo Ishii joined Tokyo Electric Power Company (TEPCO) in 1988. He was a visiting scientist in Massachusetts Institute of Technology from 1989 to 1991. He received Ph.D. from the University of Tokyo in 1996. From 2010, he has been engaged in some major smart grid related National projects in Japan as an organizer. He is now a Professor with Advanced Collaborative Research Organization for Smart Society (ACROSS) at Waseda University. His current activity is in Electric Energy System, especially regarding Demand Response (DR) and integration of distributed energy resources (DER) including renewable energy. He has been leading DR standards in Japan.

CHAN Eng Kiat has more than 40 years of experience in utility information systems, transmission and distribution network planning, protection, operations and maintenance. He is with Accenture since Oct 2014 as Intelligent Grid Operations Lead – APAC, Smart Grid Services, focusing on smart grid, microgrid technologies as well as renewables and energy storage systems integration. Prior to Accenture, Eng Kiat was a senior principal consultant at DNVGL Energy – Clean Technology Centre (CTC) and was the lead technologist for the Asian Centre of Excellence, focusing on smart grid and renewable energy management. Before joining DNVGL Energy, Eng Kiat was the principal specialist and project director of Intelligent Energy System-a smart grid pilot project, in Energy Market Authority (EMA). He was also the general manager of regulatory and network planning division in SP PowerGrid for 5 years, where he headed the division and was responsible for regulatory affairs, transmission and distribution network planning. He was also a member of the ASEAN Power Grid Consultative Committee representing Singapore. Eng Kiat was awarded with the ASEAN Engineering Award (Singapore) for Excellence in Technology in 1998 on the Distribution Automation/Distribution Management System project done in Singapore where he was the project manager and team leader from the then Public Utilities Board. Eng Kiat graduated with a M.Sc. in Industrial Engineering and a B.Eng. (Hons.) in Electrical Engineering from the then University of Singapore. He is a registered professional engineer.

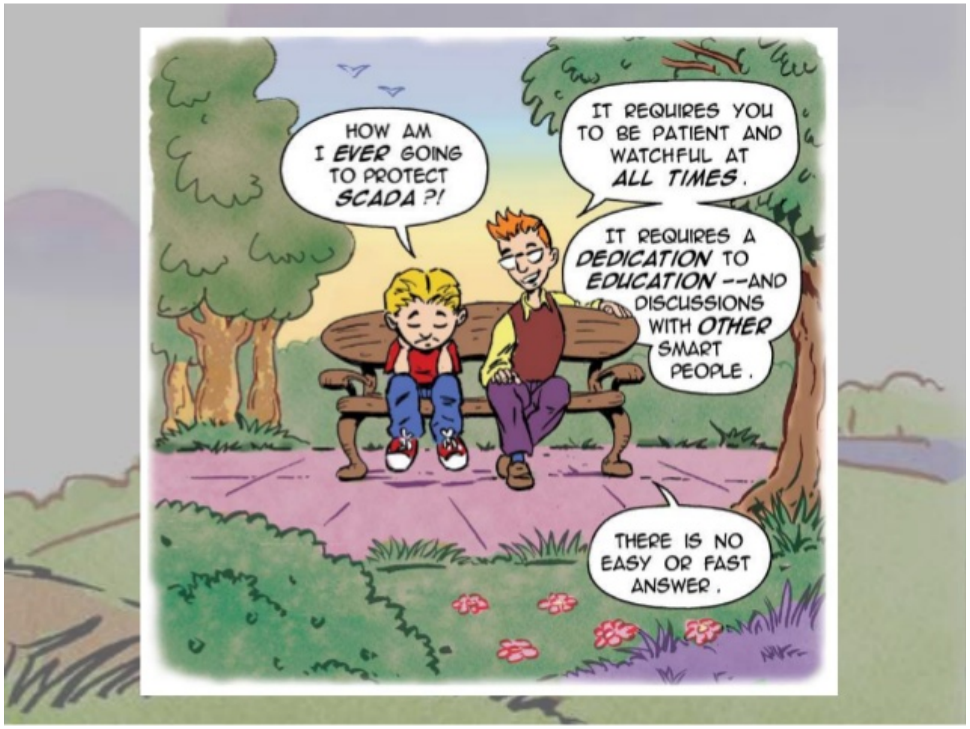


Gary Ang is a senior consultant and the lead for Intelligent Network & Communication (INC) Team in DNV GL Singapore. Gary has close to 15 years of experience in SCADA/EMS/DMS design and implementation. He is currently overseeing services such as SCADA/EMS/ADMS consultancy, operational technology cyber security, utility digital transformation and protocol conformance testing. He is the SCADA/EMS/ADMS consulting manager for Tenaga Nasional Berhad, Taiwan Power Company and Sarawak Energy Berhad. He is also involved in several cyber security test and review projects in the region. Prior to joining DNVGL, he has lead and managed several large scale power system projects in Asia Pacific. Gary specialized in project management, business development, SCADA/EMS/ADMS design & implementation, software engineering, cyber security and digitalization. He is a certified PMP and CISSP. He has a background of computer science and electrical engineering.

Chee-Wooi Ten is an Associate Professor in Michigan Tech University. He received a BS and an MS in Electrical Engineering from Iowa State University, in Ames, in 1999 and 2001, respectively. Prior to completing his Master's degree, he had a summer internship with MidAmerican in Des Moines, working as an energy management system (EMS) analyst. Ten was an Application Engineer with Siemens Energy Management and Information System (SEMIS) in Singapore from 2002 to 2006. He received a PhD in 2009 from University College Dublin (UCD), National University of Ireland. His primary research interests are (1) cybersecurity for power grids, and (2) software prototype and power-automation applications on SCADA systems. He has been with Michigan Tech since January 2010 and is currently an Associate Professor. Chee-Wooi has recently served as editor for the IEEE Transactions on Smart Grid and the Elsevier Journal Sustainable Energy, Grids and Networks (SEGAN).

Yunhe Hou received the B.E. and Ph.D. degrees in electrical engineering from Huazhong University of Science and Technology, Wuhan, China, in 1999 and 2005, respectively. He was a Post-Doctoral Research Fellow at Tsinghua University, Beijing, China, from 2005 to 2007, and a Post-Doctoral Researcher at Iowa State University, Ames, IA, USA, and the University College Dublin, Dublin, Ireland, from 2008 to 2009. He was also a Visiting Scientist at the Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA, USA, in 2010. Since 2017, he has been a Guest Professor with Huazhong University of Science and Technology, China. He joined the faculty of the University of Hong Kong, Hong Kong, in 2009, where he is currently an Associate Professor with the Department of Electrical and Electronic Engineering. Dr. Hou is an Editor of the IEEE Transactions on Smart Grid and Journal of Modern Power Systems and Clean Energy.

Thanks!


HOW AM I *EVER* GOING TO PROTECT *SCADA* ?!
IT REQUIRES YOU TO BE PATIENT AND WATCHFUL AT *ALL TIMES*.
IT REQUIRES A *DEDICATION* TO *EDUCATION* --AND DISCUSSIONS WITH *OTHER* SMART PEOPLE.
THERE IS NO EASY OR FAST ANSWER.

https://www.slideshare.net/RobertMLee1/a-child-like-approach-to-grid-cybersecurity

- Internship positions are available at ADSC. If interested, please contact me at daisuke.m@adsc-create.edu.sg