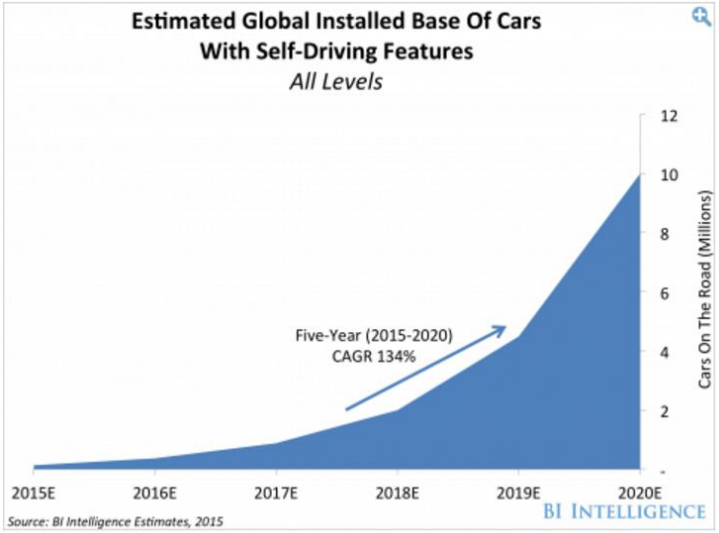
JUNHO HONG, US Corporate Research Center (CRC), 2015-11-02

IEEE SmartGridComm 2015

Cyber and Physical Security of Substations in Smart Cities

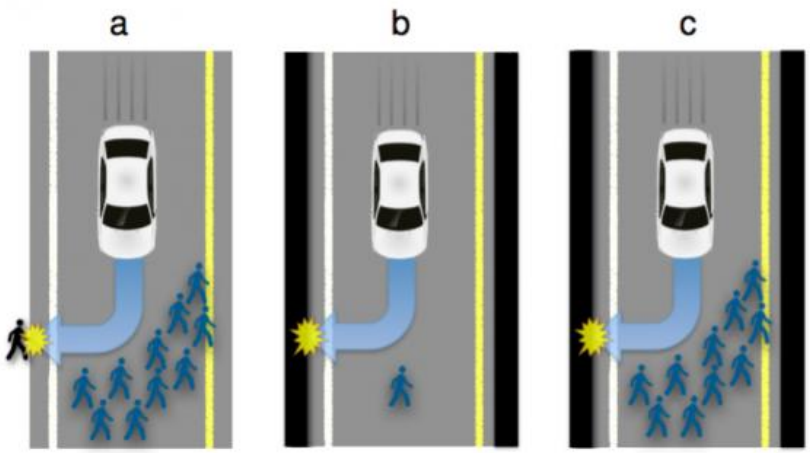
Self-driving car
Must be programmed to kill?

- **Self-driving car**



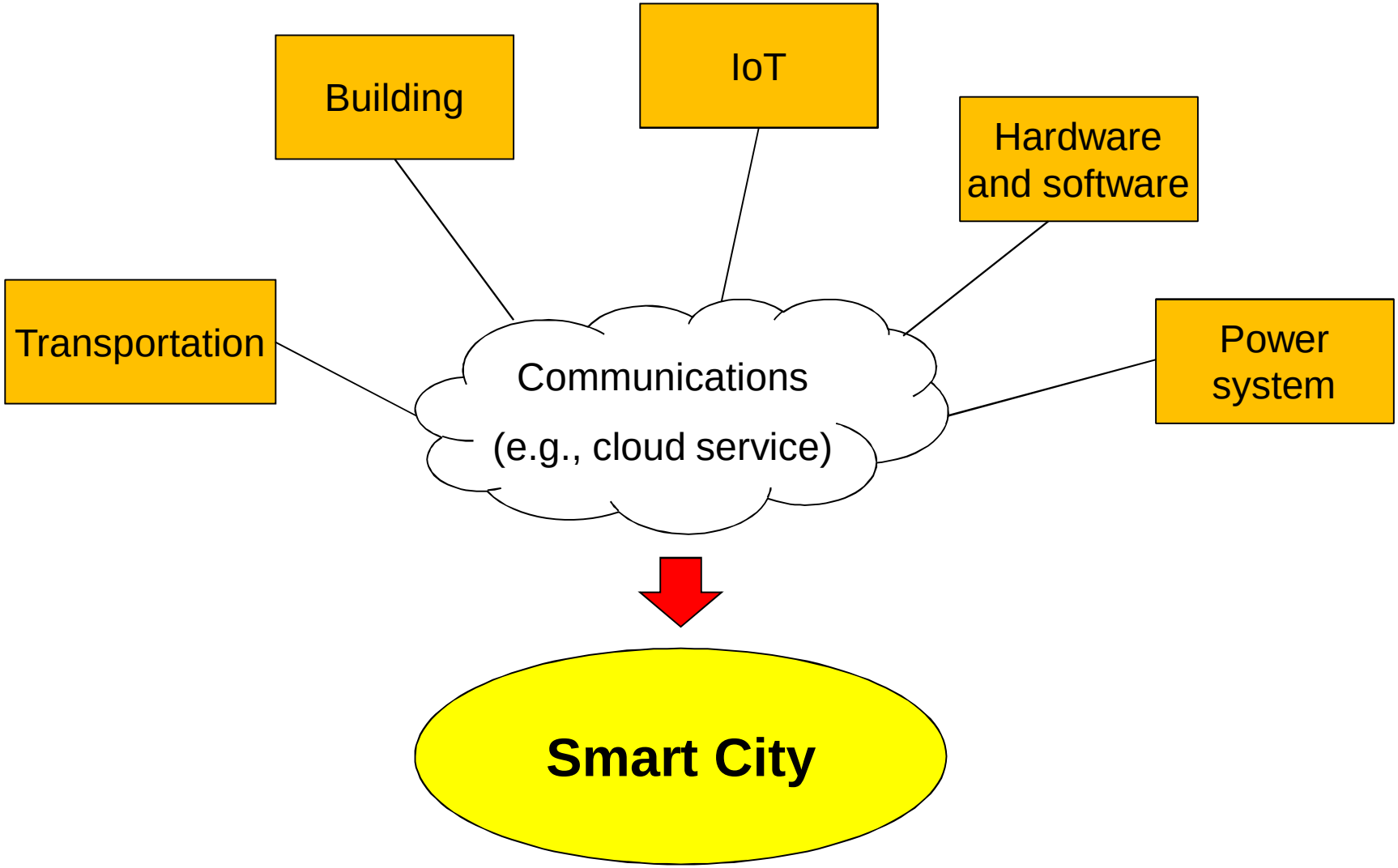
BI Intelligence

- **Why it must be programmed to kill**



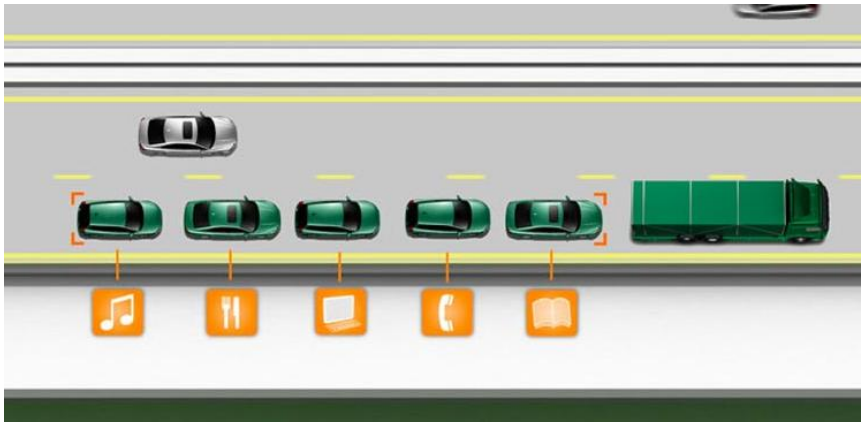
Source: google.com/selfdrivingcar, http://www.technologyreview.com/

Smart city
Technologies



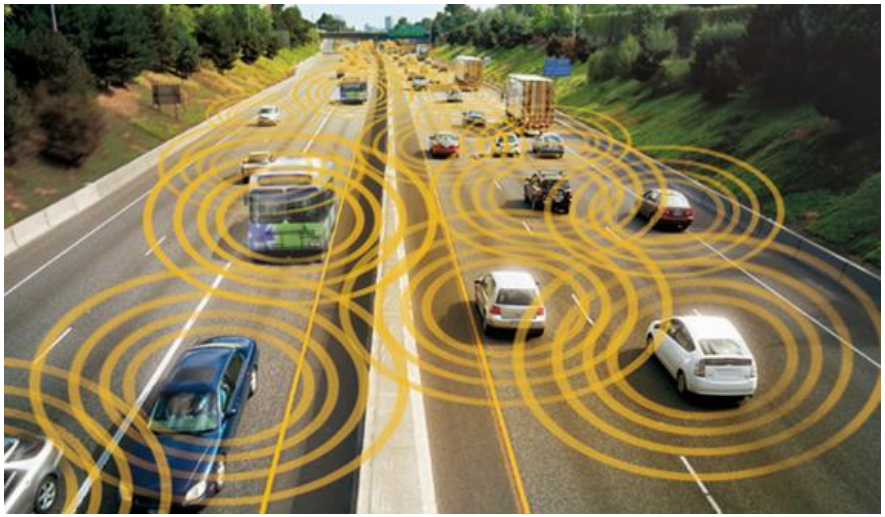
Transportation
Technologies and threats

- **Technologies**
  - V2V and V2I
  - Cloud based communication
  - Connected driving
  - Vehicle platooning



Vehicle platooning

- **Threats**
  - Car hacking
  - Change configuration
  - Sensor jamming attack
  - Change destination



Connected driving

Source: www.fhwa.dot.gov/

Building
Technologies and threats

- **Technologies**
  - Occupancy based energy use
  - IoT connected smart building
  - Connecting to the micro or smart grid
  - Physical security

- **Threats**
  - Control HVAC system
  - Control lighting system
  - Load shedding (outage)

Credit: IBM

Source: http://www.energymanagertoday.com/

IoT
Technologies and threats

- **Technologies**
  - Smart battery (roost)
  - Streetlights with gunshot detection (GE)
  - Wearable devices

Wearable devices

- **Threats**
  - Control IoT devices
  - Privacy problem
  - Security key problem
  - Security update
  - Insecure cloud interface

Smart battery

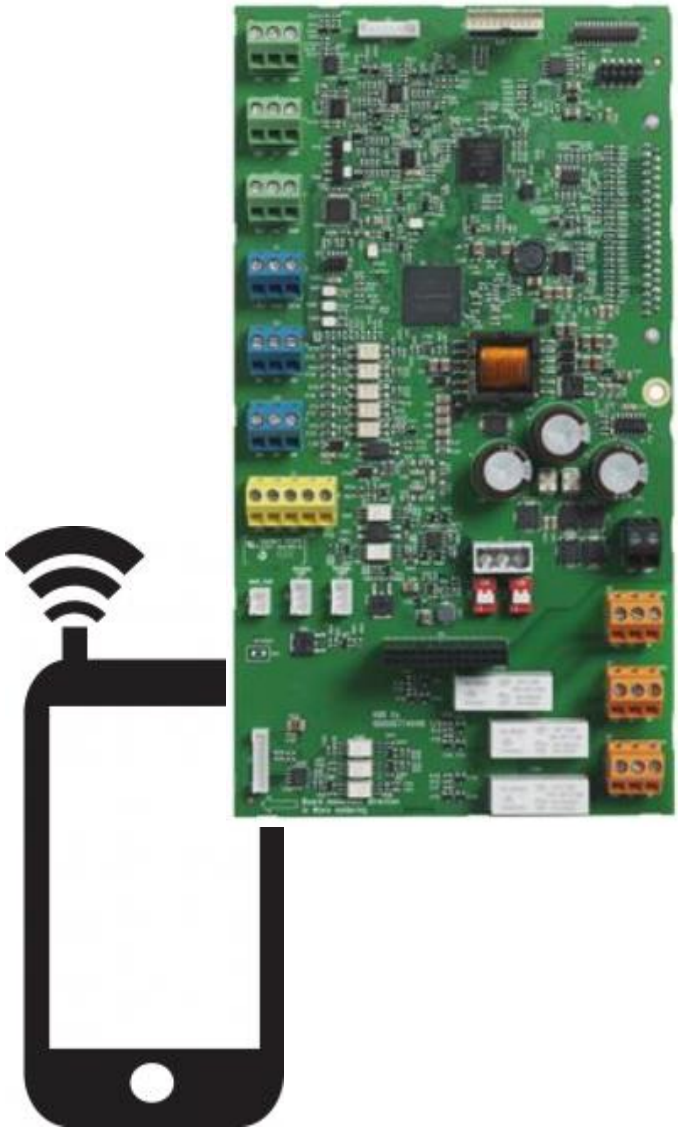
Smart home

Source: getroost.com, alarm.com, credit suisse

Hardware and software
Technologies and threats

- **Technologies**
  - IoT devices
  - Smart phones
  - Control devices

- **Threats**
  - Superuser
  - Hidden features
  - Backdoor by developers
  - Pre-installed malware



Power system
Physical and cyber attack

Shots in the Dark

A look at the April 16 attack on PG&E's Metcalf Transmission Substation

①	②	③	④	⑤	⑥	⑦
12:58 a.m., 1:07 a.m. Attackers cut telephone cables	**1:31 a.m.** Attackers open fire on substation	**1:41 a.m.** First 911 call from power plant operator	**1:45 a.m.** Transformers all over the substation start crashing	**1:50 a.m.** Attack ends and gunmen leave	**1:51 a.m.** Police arrive but can't enter the locked substation	**3:15 a.m.** Utility electrician arrives

Sources: PG&E; Santa Clara County Sheriff's Dept.; California Independent System Operator; California Public Utilities Commission; Google (image)
The Wall Street Journal

↑ Generator room at the Idaho National Laboratory was remote accessed by a hacker and a $1 Million diesel-electric generator destroyed. (U.S. Homeland Security photo)

← Two snipers attacked 17 transformers and 6 circuit breakers. Total of 52,000 gallons of oil spilled and $15.4M in estimated restoration costs.

Power system - substations
Current situation

- Attackers successfully compromised U.S. Department of Energy computer systems more than 159 cyber attacks between 2010 and 2014, a review of federal records obtained by USA TODAY finds.

- Between 2011 and 2014, there were 348 physical attacks and 14 cyber attacks on the grid that caused outrages or disturbances, according to electric utility data reported to the S. Department of Energy.

- In March 2014, the North American Electric Reliability Corporation (NERC) issued Order CIP-014-1 requiring transmission owners to assess the vulnerability of critical substations and develop and implement security plans. Once the vulnerabilities have been identified, the next step is to create a prioritized plan for addressing these vulnerabilities

- The implementation schedule for this order starts in Oct 2015 and requires completion by August 2016

Source: http://www.usatoday.com/story/news/2015/09/09/cyber-attacks-doe-energy/71929786/
http://ireport.cnn.com/docs/DOC-1249770

Power system - substations

Are we ready for this?

QUICKPOLL

What steps has your utility undertaken to comply with NERC-CIP 14 requirements for physical security?

Poll Results (multiple answers allowed):

Evaluated potential threats vulnerabilities and consequences	46%
Developed physical security plan to address vulnerabilities	39%
Engaged an independent third party to review assessments	30%
Have not yet completed any initiatives	35%

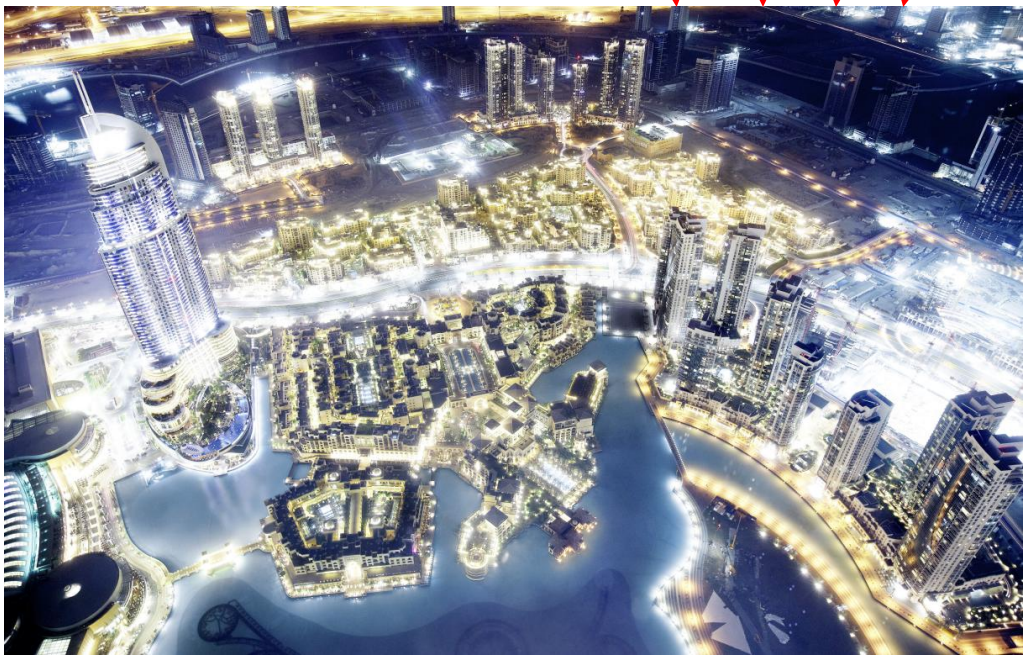
Source: How secure is your substation? Physical security (Part I) - 3 strategic elements to protect your assets, ABB

Power system - substations

Worst scenario?

- 4 substations
- 9 transformers
- A coordinated attack to multiple substations?
- No connections to reroute the power?
- Outages and then cascading events?

Substations



Smart city

Power system - substations
Mitigations – physical attack

- Underground cables to disguise location of substation
- GIS to camouflage critical substations
- Resilient bus configuration – more redundancy
- IEC 61850 based substation automation systems
- Physical separation of A & B set protection
- Perimeter fencing (bulletproof walls, cut proof fence, sensors and detection systems)
- Wireless communication for redundancy
- Physical protection of critical assets (bulletproof transformer, circuit breaker and control house)

Source: How secure is your substation? Physical security (Part I) - 3 strategic elements to protect your assets, ABB

Power system - substations

Access to data for multiple purposes

Who ?

Protection Engineers

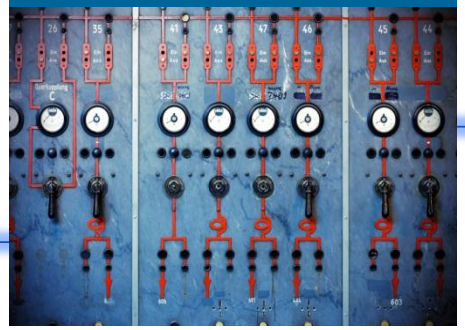
Control Center Operators

Corporate Offices

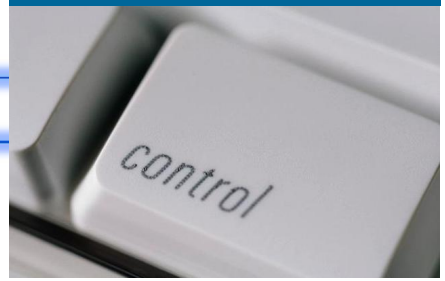
Technicians

Why ?

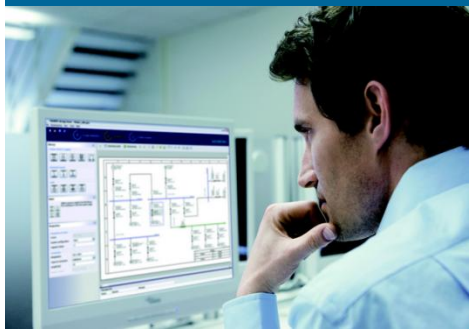
Protection



Control

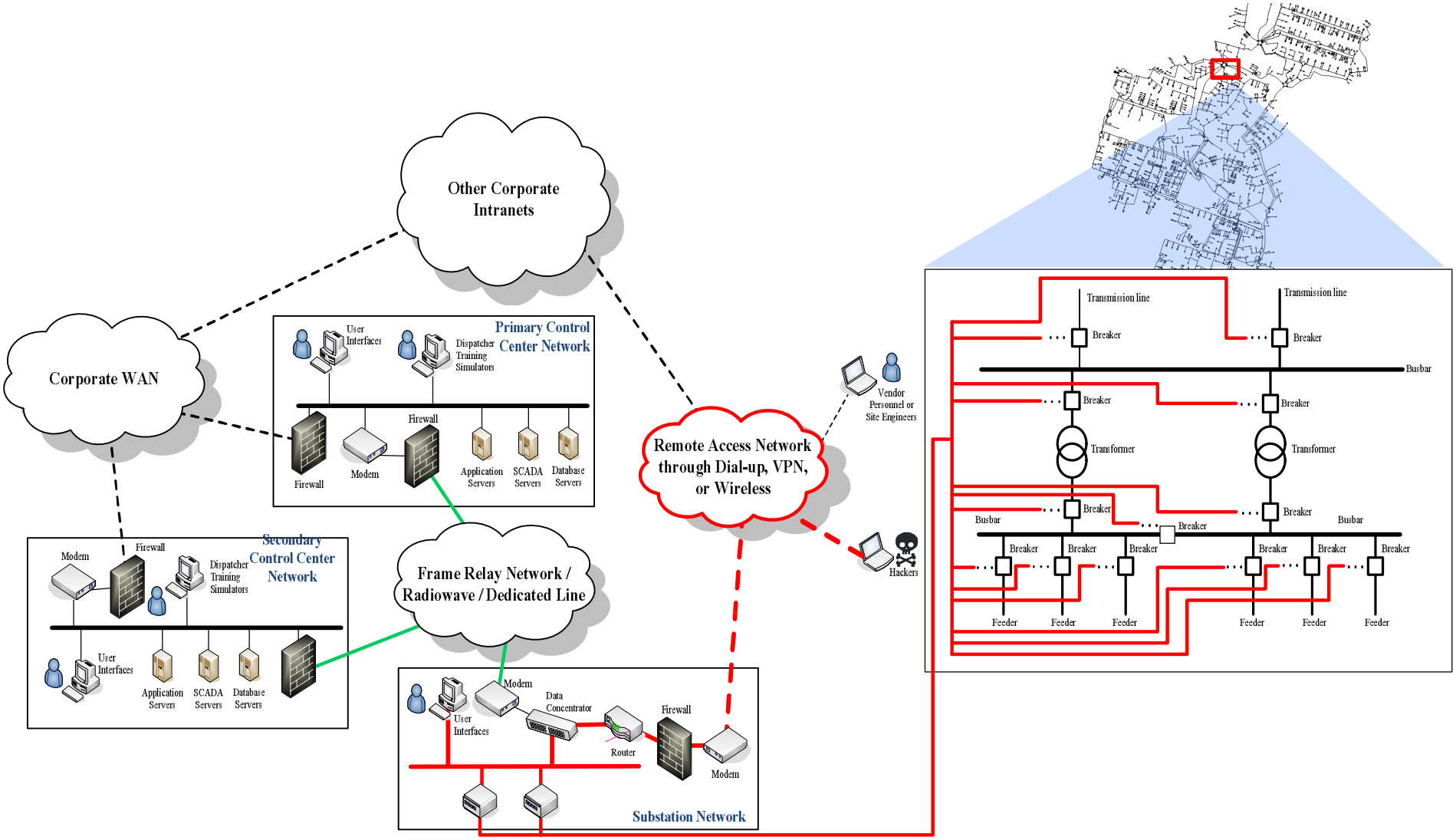


Monitoring



Power system - substations

Intrusion into a substation network



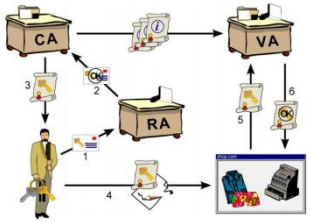
Power system - substations
Vulnerabilities of substations

- Remote access to substation user interface or IEDs for maintenance purposes
- Unsecured standard protocol, remote controllable IED and unauthorized remote access
- Some IED and user-interface have available web servers and it may provide a remote access for configuration and control with default passwords
- Well coordinated cyber attacks can compromise more than one substation – it may become a multiple, cascaded sequence of events

Power system - substations

Problems?

Confidentiality

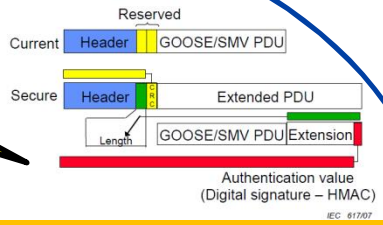


Encryption

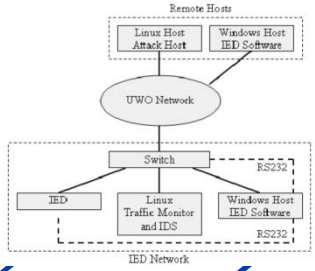
Requirement

Integrity

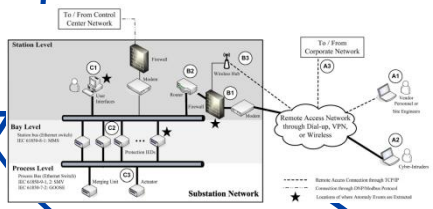
Interoperability problem



Authentication

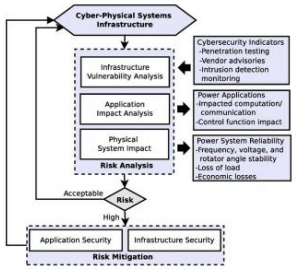


Intrusion detection system

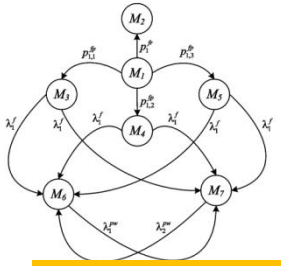


Anomaly detection system

Availability



Risk assessment

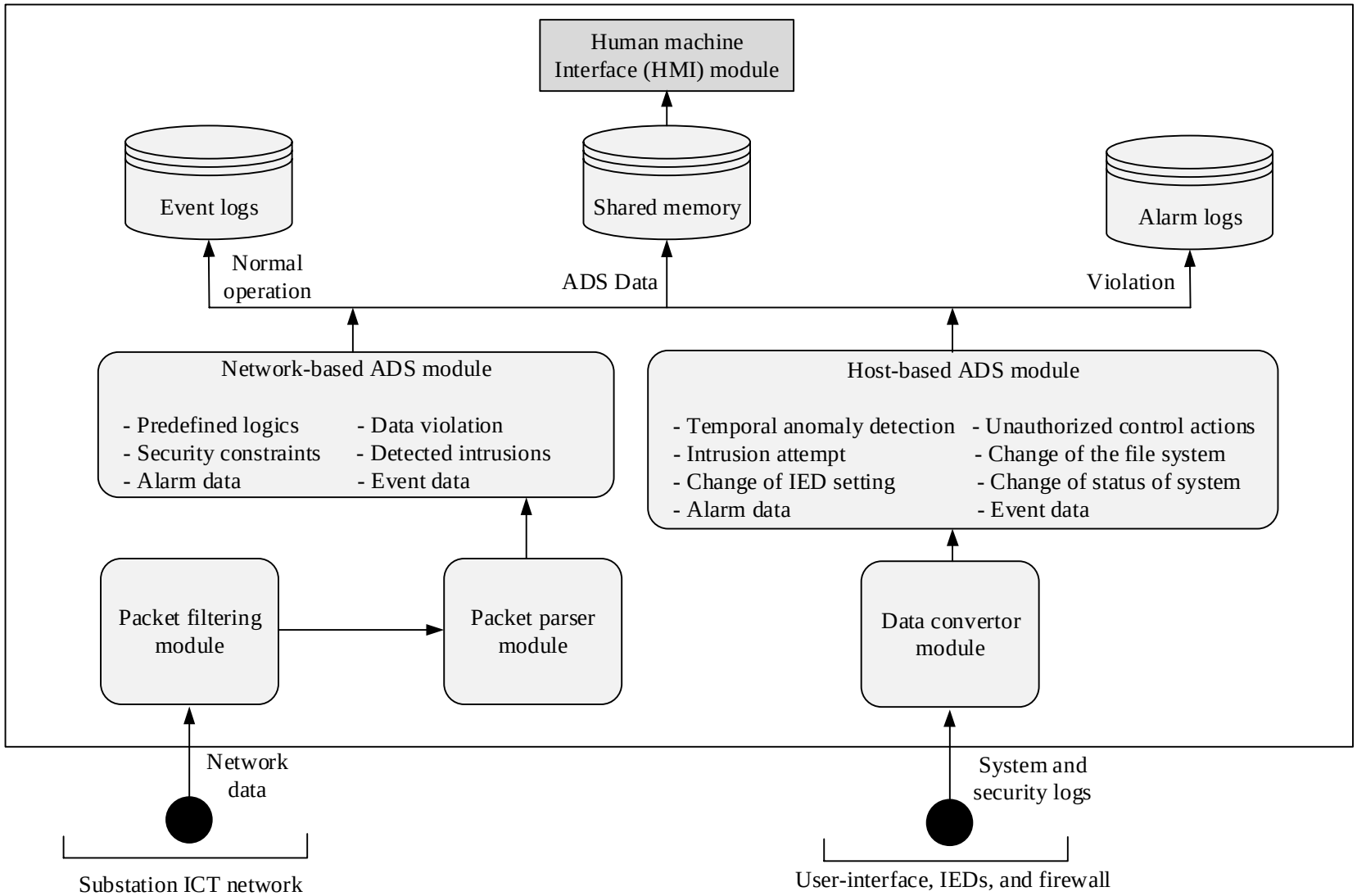


No GOOSE and SMV

Vulnerability assessment

Power system - substations

Mitigations – cyber attacks – anomaly detection system



Source: J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1643-1653, April 2014.

Power system - substations

Mitigations – cyber attacks – anomaly detection system

SMMAD Algorithm

1. $\psi^G,\ \psi^{SV},\ V_n^{GS} = 0$; // Initialize
2. capture C_{pkt}; // Capture all packets in the substation network
3. if (C_{pkt} is IEC GOOSE);
4. $\quad G_{cp} = [G_{st}, G_{sq}, G_{ge}^T, G_{re}^T]$; // Parse packet
5. $\quad$ if ($G_{cp}[G_{sm}, G_{dm}] \neq G_{cp-1}[G_{sm}, G_{dm}]$); // Find different GOOSE
6. $\quad\quad$ make $G_{at\ new}$; // Create new anomaly detection thread
7. $\quad \alpha_{Th}^G \vee \beta_S^G \vee \gamma_{Ti}^G \vee \delta_d^G \rightarrow \psi^G$; // Calculate GOOSE intrusion
8. $\quad$ if ($\psi^G = true$), set $V_n^{GS} = 1$; // Detect GOOSE intrusion
9. $\quad$ else set $V_n^{GS} = 0$; // No intrusion
10. elseif (C_{pkt} is IEC SMV);
11. $\quad S_{cp} = [S_{mc}, S_{ds}, S_{id}, S_{sm}, S_{dm}]$; // Parse packet
12. $\quad \varepsilon_{Th}^{SV} \vee \theta_{cn}^{SV} \vee \mu_d^{SV} \rightarrow \psi^{SV}$ // Calculate SMV intrusion
13. $\quad$ if ($\psi^{SV} = true$), set $V_n^{GS} = 1$; // Detect SMV intrusion
14. $\quad$ else set $V_n^{GS} = 0$; // No intrusion
15. return V_n^{GS};

Source: J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1643-1653, April 2014.

Power system - substations

Mitigations – cyber attacks – anomaly detection system

- Detection of temporal anomalies is performed by comparing consecutive row vectors representing a sequence of time instants

$$V_{h(i)}^{\mathbf{\Omega}} = \frac{\sum_{j=1}^{n} \left| \mathbf{\Omega}_{(i,j)} - \mathbf{\Omega}_{(i+1,j)} \right|}{n}, \; i = 1, \ldots, 6,$$

- If a discrepancy exists between two different periods (rows, 10 seconds), the anomaly index is a number between 0 and 1

- A value of 0 implies no discrepancy whereas 1 indicates the maximal discrepancy

Host-based anomaly indicators

- ψ^a (intrusion attempt on user interface or IED)
- ψ^cf (change of the file system)
- ψ^cs (change of IED critical settings)
- ψ^o (change of status of breakers or transformer taps
- ψ^m (measurement difference)

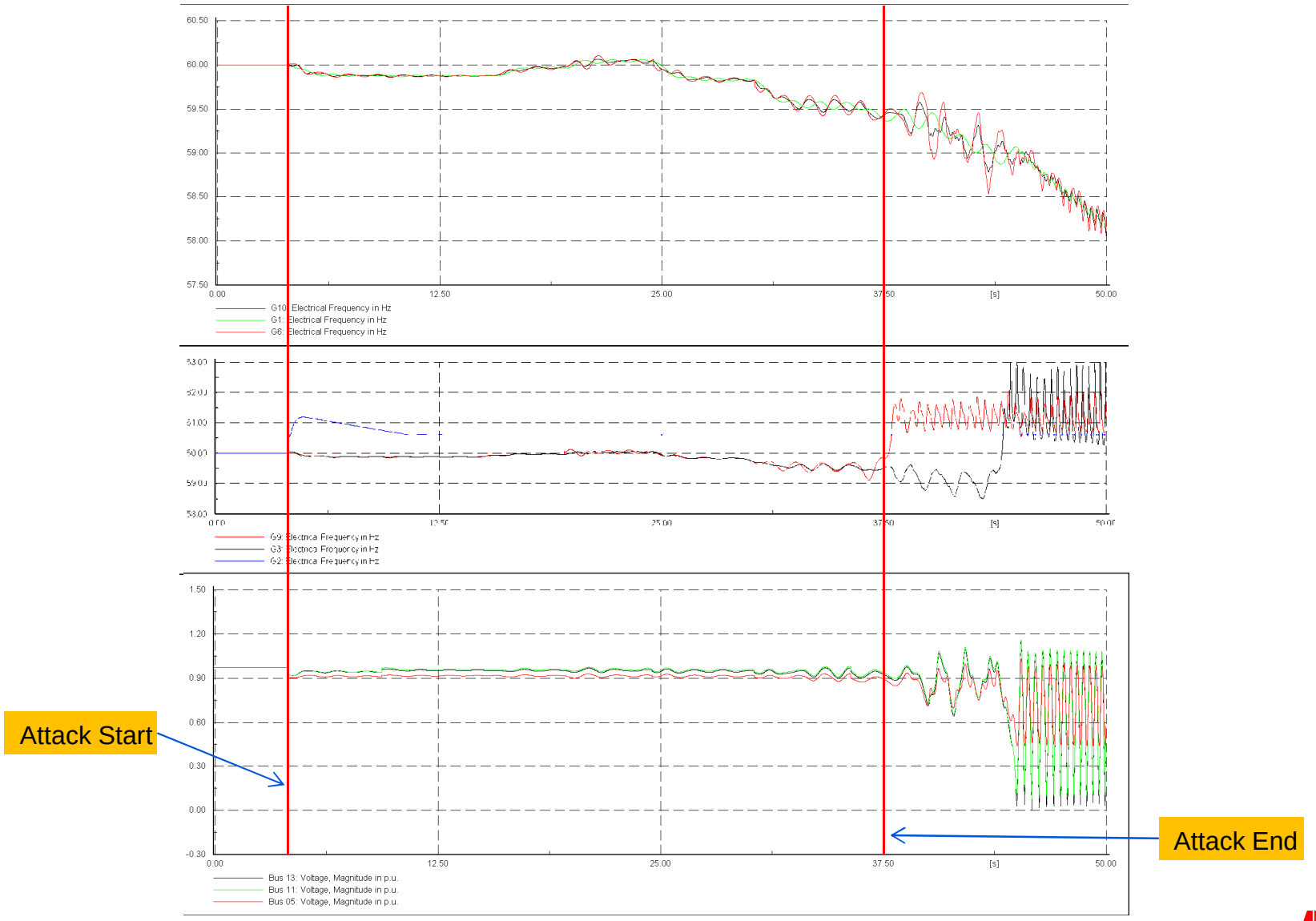
Substation A

$$\mathbf{\Omega} = \begin{array}{c} t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \\ t_7 \end{array} \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Source: J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1643-1653, April 2014.

Power system - substations

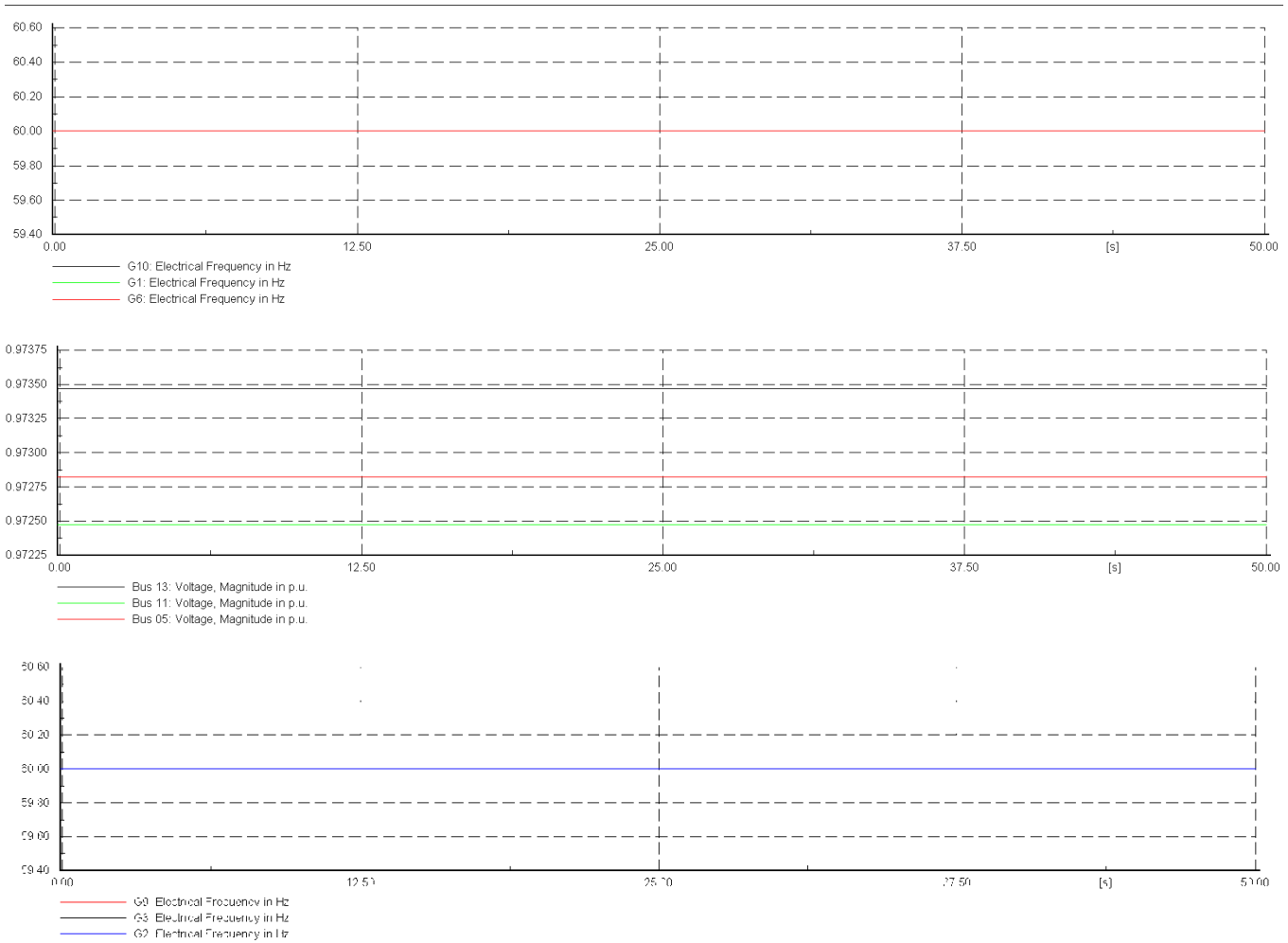
Mitigations – cyber attacks – anomaly detection system



Source: J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated Anomaly Detection for Cyber Security of the Substations," IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1643-1653, April 2014.

Power system - substations

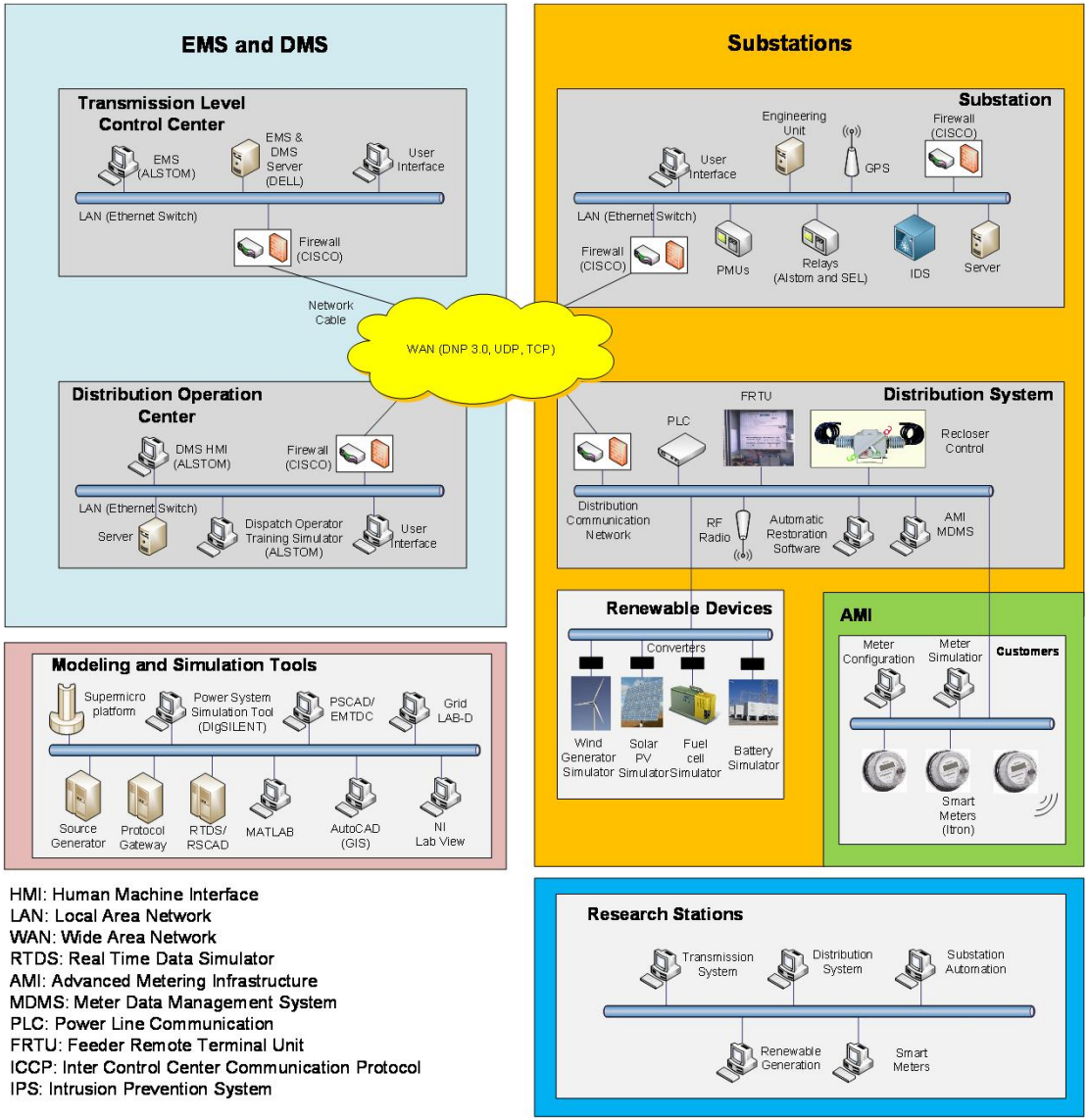
Mitigations – cyber attacks – anomaly detection system



Source: J. Hong, C.-C. Liu, and M. Govindarasu, “Integrated Anomaly Detection for Cyber Security of the Substations,” IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1643-1653, April 2014.

Power system - substations

Mitigations – cyber attacks – cyber-physical testbed

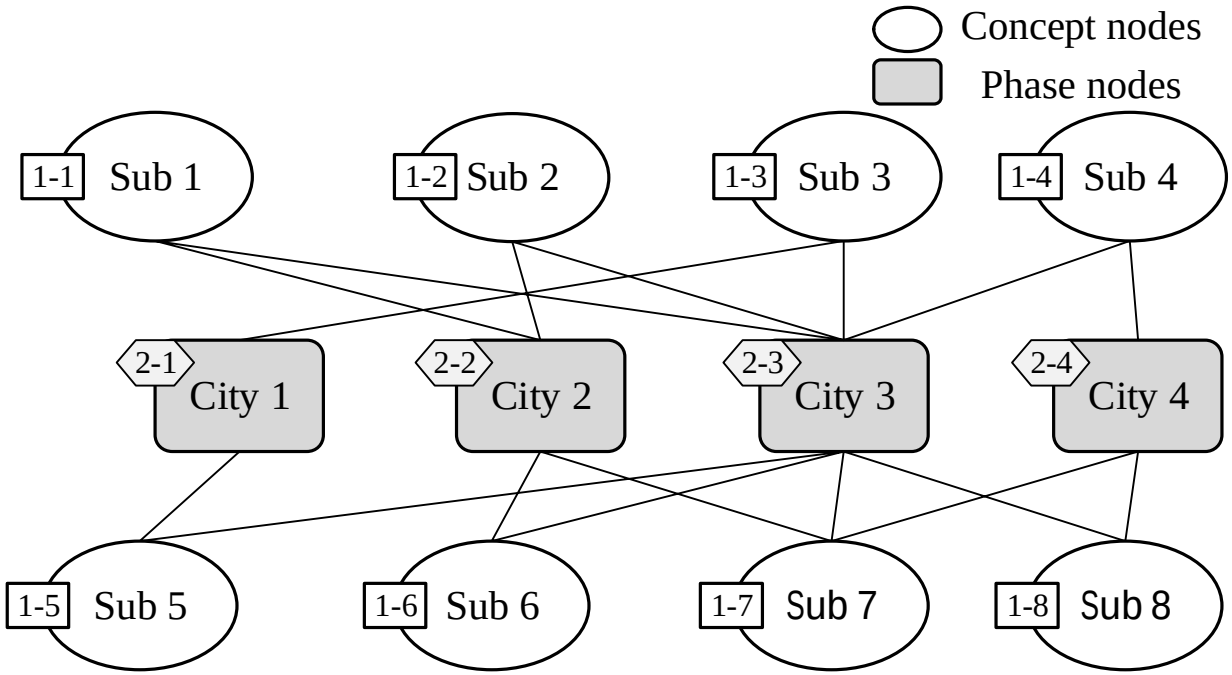


HMI: Human Machine Interface
LAN: Local Area Network
WAN: Wide Area Network
RTDS: Real Time Data Simulator
AMI: Advanced Metering Infrastructure
MDMS: Meter Data Management System
PLC: Power Line Communication
FRTU: Feeder Remote Terminal Unit
ICCP: Inter Control Center Communication Protocol
IPS: Intrusion Prevention System

Source: C. Sun, J. Hong, and C.-C. Liu, "A Co-Simulation Environment for Integrated Cyber and Power Systems," *IEEE Smartgridcomm conference*, Nov. 2015.

Power system - substations

Mitigations – cyber attacks – coordinated cyber attack detection



Big data analysis

Source: C. Sun, J. Hong, and C.-C. Liu, "A Coordinated Cyber Attack Detection System (CCADS) for Multiple Substations," *19th Power Systems Computation Conference (PSCC 2016)*, June 2016.

References

Projects

[1] **Collaborative Research: Resiliency against Coordinated Cyber Attacks on P ower Grids**, funded by National Science Foundation

[2] **Collaborative Defense of Transmission and Distribution Protection and Control Devices Against Cyber Attacks (CoDef)**, funded by Department of Energy (DoE)

Papers

[1] C.-W. Ten, J. Hong, and C.-C. Liu, "**Anomaly Detection for Cybersecurity of the Substations**," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 865-873, Dec. 2011.

[2] C.-C. Liu, A. Stefanov, J. Hong, P. Panciatici, "**Intruders in the Grid**," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58-66, Jan.-Feb. 2012.

[3] J. Hong, C.-C. Liu and M. Govindarasu, "**Integrated Anomaly Detection for Cyber security of the Substations**," *Submitted to IEEE Trans. Smart Grid*, 2013.

[4] J. Hong, C.-C. Liu, and M. Govindarasu, "**Detection of Cyber Intrusions Using Network-based Multicast Messages for Substation Automation**," *Submitted to IEEE Innovative Smart Grid Technologies (ISGT) Conference*, 2014.

[5] J. Hong, R. Nuqui, D. Ishchenko, Z. Wang, T. Cui, A. Kondabathini, D. Coats, and S. Kunsman, "**Cyber-Physical Security Test Bed: A Platform for Enabling Collaborative Cyber Defense Methods**," PAC World Americas, Sep. 2015.

Power and productivity
for a better world™

Thank you!

Junho Hong
Scientist
US Corporate Research Center (CRC), ABB Inc
Junho.hong@us.abb.com