TCIPG

TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG

FROM SECURITY TO RESILIENCY: OPPORTUNITIES AND CHALLENGES FOR THE SMART GRID'S CYBER INFRASTRUCTURE

APRIL 20, 2015

BILL SANDERS

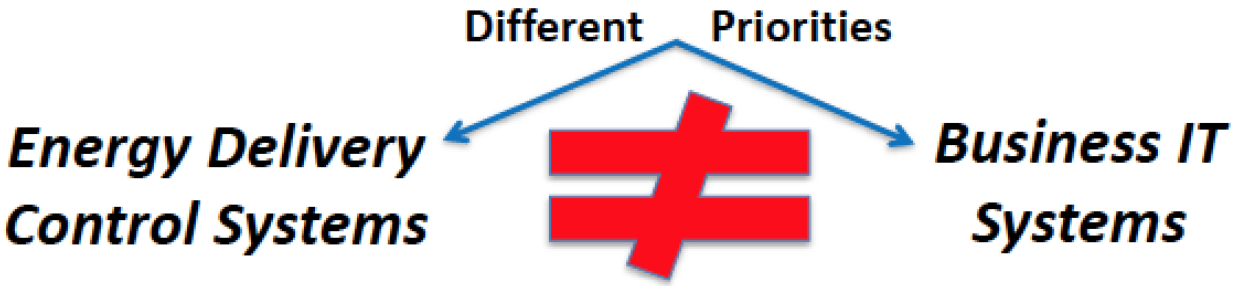
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

THE CHALLENGE: PROVIDING TRUSTWORTHY GRID OPERATION IN POSSIBLY HOSTILE ENVIRONMENTS

- Trustworthy
  - A system which does what it is supposed to do, and nothing else
  - Safety, Availability, Integrity, Confidentiality …
- Hostile Environment
  - Accidental Failures
  - Design Flaws
  - Malicious Attacks
- Cyber Physical
  - Must make the whole system trustworthy, including both physical & cyber components, and their interaction.

BACKGROUND.

Energy Sector Cybersecurity



- Energy delivery control systems (EDS) must be able to survive a cyber incident while sustaining critical functions
- Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades
- The modern grid contains a mixture of legacy and modernized components and controls
- EDS components may not have enough computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities that are not tailored to the energy delivery system operational environment
- EDS components are widely dispersed over wide geographical regions, and located in publicly accessible areas where they are subject to physical tampering
- Real-time operations are imperative, latency is unacceptable
- Real-time emergency response capability is mandatory

SOURCE: CAROL HAWK, CEDS OVERVIEW PRESENTATION

- Multiparty interactions with partial & changing trust requirements
- Regulatory limits on information sharing

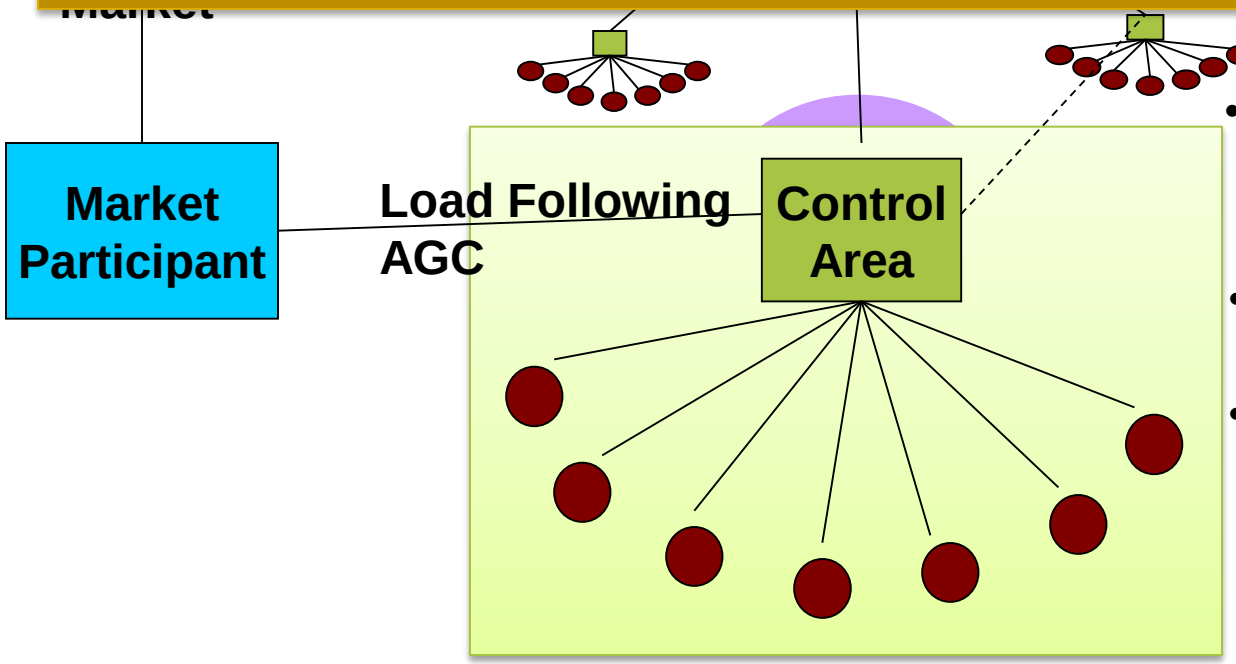
Other Coordinators

Market

Coordinator

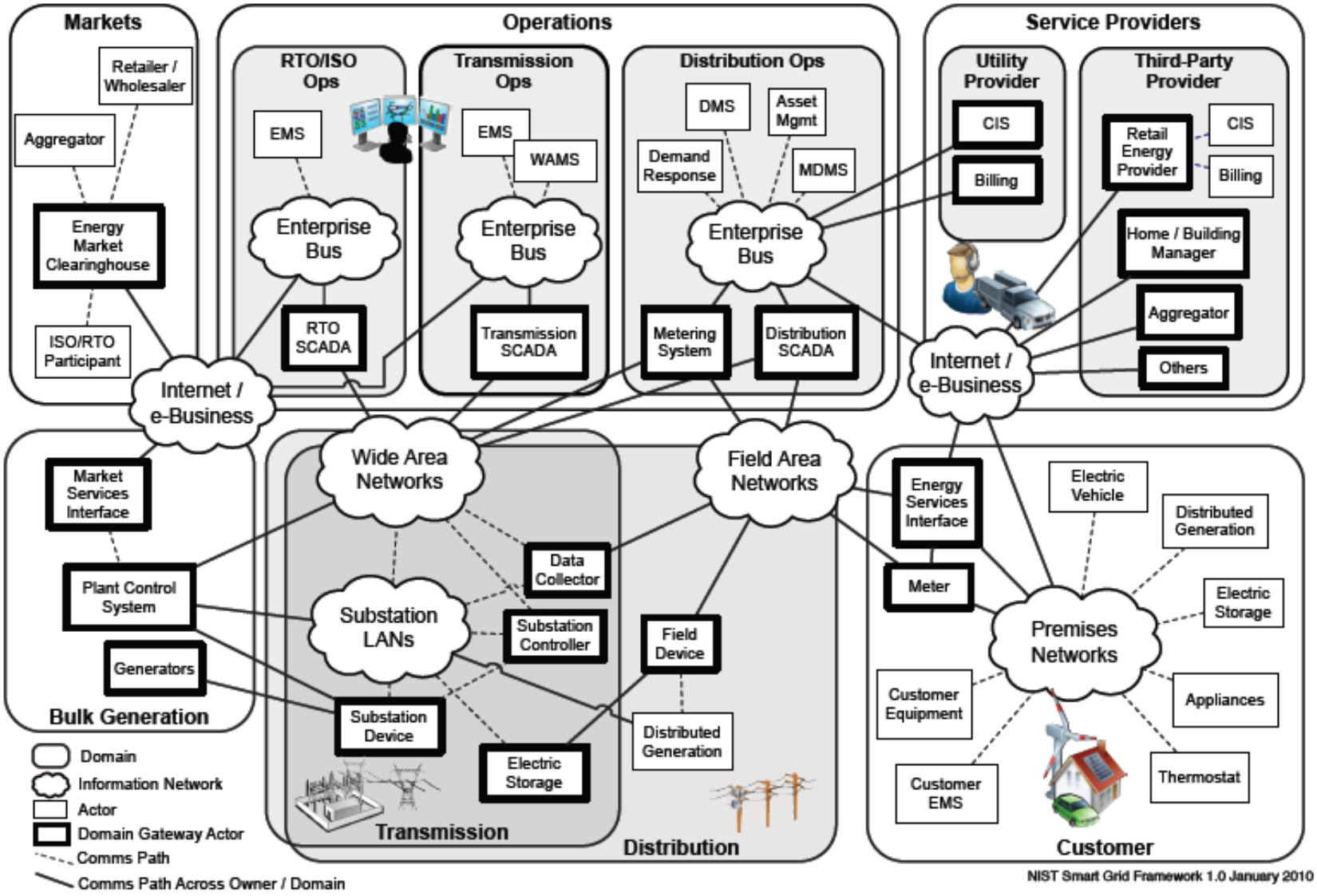
Cross Cutting Issues

- Large-scale, rapid propagation of effects
- Need for adaptive operation
- Need to have confidence in trustworthiness of resulting approach



- Need to create secure and reliable computing base
- Support large # of devices
- Timeliness, security, and reliability required of data and control information

CONCEPTUAL REFERENCE DIAGRAM FOR SMART GRID INFORMATION NETWORKS



NIST Smart Grid Framework 1.0 January 2010

DISRUPTIVE TRENDS IN THE SMART GRID: *TRANSFORMATION OF THE SMART GRID INFRASTRUCTURE*

- Large numbers of intelligent devices in the substation and the field
- Smart meters deployed as part of AMI
- Larger-scale wide-area measurement systems
- Mixed legacy environment with older components that cannot support modern security mechanisms

DISRUPTIVE TRENDS IN THE SMART GRID: *ENERGY "INTERNET OF THINGS" AND UTILITY CLOUDS*

- Radical changes coming in the way ICS will be managed, owing to network virtualization and increased connectivity
- Increased availability of data and analysis
- Many events will become manageable in the cloud as "wide-area system event"
- Virtualization will blue the notion of the control parameter and make security more difficult
- Increased dependence on computation and communication could increase attack surface

DISRUPTIVE TRENDS IN THE SMART GRID: *RENEWABLES*

- Wind and solar are both subject to short-term fluctuations that can potentially destabilize a grid
- Resiliency requires technology that can sense fluctuations quickly and respond to dynamic variation in generation
- Requirement for high system “self-awareness” as well as advanced analytics
- Distributed generation ownership complicates issue

DISRUPTIVE TRENDS IN THE SMART GRID: *ELECTRIC VEHICLES*

- "EV Everywhere" will require a new grid infrastructure, with new security and resiliency requirements
- Control of infrastructure must deal with rapid changes of volume and location of loads
- Billing is likely to follow vehicle
- Will result in complex mobile and human-based cyber-physical system which will create new reliability and security issues

HUMBLE CYBER SECURITY BEGININGS, CIRCA 2000.

RAPID ADVANCE TO ADOLESCENCE.

CLASSICAL (PHYSICAL) ATTACK APPROACHES

- Physical attacks on lines, buses and other equipment can be locally effective:
  - "low tech" attacks may be easy, and are also difficult to defend against
  - Requires physical proximity of attacker
  - Particularly effective if multiple facilities are attacked in a coordinated manner
- But coordination may be much easier in a cyber attack

J.D. Konopka (a.k.a. Dr. Chaos) Alleged to have caused $800K in damage in disrupting power in 13 Wisconsin counties, directing teenaged accomplices to throw barbed wire into power stations. (From Milwaukee Journal Sentinel)
http://www.jsonline.com/news/Metro/may02/41693.asp

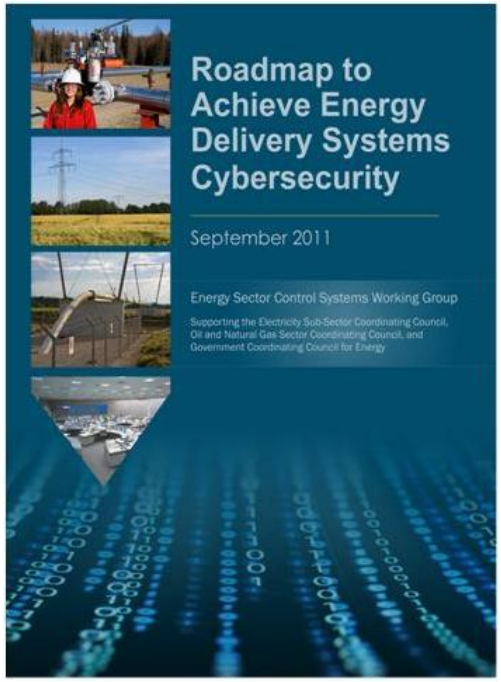
POTENTIAL TRANSMISSION-SIDE CYBER ATTACK STRATEGIES

- Tripping breakers
- Changing values breaker settings
  - Lower settings can destabilize a system by inducing a large number of false trips
  - Lowering trip settings can cause extraneous other breakers, causing overloading of other transmission lines and/or loss of system stability
- Malicious fuzzing of power system components
- Life cycle attacks
- Insider threats
- Physical damage by cyber means
- Combined physical and cyber attacks

POWER GRID CYBER SECURITY GUIDANCE

- Roadmap to Achieve Energy Delivery Systems Cybersecurity – 2006, 2011
- FERC/NERC: Cybersecurity Standards – 2008 to present
- NISTIR 7628: Guidelines for Smart Grid Cybersecurity, 2009 to present
- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) – 2012 to present

INDUSTRY ROADMAP – A FRAMEWORK FOR PUBLIC-PRIVATE COLLABORATION



- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in control systems security

Roadmap Vision

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

FERC/NERC CYBER SECURITY STANDARDS FOR THE BULK ELECTRIC POWER GRID

- Energy Policy Act of 2005 created an Electric Reliability Organization (ERO) to develop and enforce mandatory cybersecurity standards
- FERC designated NERC as the ERO in 2006
- NERC worked with electric power industry experts to develop the NERC Critical Infrastructure Protection (CIP) standards CIP-002 through CIP-009
- Standards approved by FERC in 2008, making them mandatory for owners and operators of the bulk electric system
- NERC standards continue to evolve, as the threat environment evolves, and more is known about critical infrastructure protection

REAL FINANCIAL PENALTIES


NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

October 31, 2012

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100957	CIP-002-1	R1	Medium[5]	$725,000
Reliability*First* Corporation	URE1	1448	RFC201100958	CIP-002-1	R2	High[6]	

http://www.nerc.com/filez/enforcement/Public_FinalFiled_NOP_NOC-1448.pdf

TODAY'S CYBER RESILENCEY CHALLENGES AND GAPS.

CHALLENGES TO GRID RESILIENCY: **DEPENDENCY ON CYBER INFRASTRUCTURE RESILIENCE**

- Resiliency may be impacted by the grid's increased dependence on cyber technology
- Adverse cyber events may arise from cyber attack, or from software/hardware malfunction, or through error in configuration or operation
- Cyber assets might be compromised with no direct attack on the physical grid system, or a blended attack could impact both cyber and physical assets
- The event may affect measurement, communications, or control systems

CHALLENGES TO GRID RESILIENCY: **DEPENDENCY ON OTHER INFRASTRUCTURES**

- Hydroelectric power depends on the correct function of dam controls
- Smart grid communication depends on the telecommunication infrastructure
- The grid features multiple interdependencies with transportation for fuel delivery
- The emerging electric vehicle system will introduce multiple interfaces, including some tightly coupled ones, to transportation
- Smart grid market mechanisms will necessitate interfaces to the financial infrastructure, particularly in the case of demand response stimulated by rapid real-time price fluctuations

GRID RESILIENCY:
THE RESILIENCY CHAIN

- System Analysis
- Detection of adverse events
- Identification of affected assets and potential system consequences
- Automated or semi-automated response
- Remediation of the effects of the event
- Hardening of the affected components and modification of design
- Full system restoration

RESEARCH AND TECHNOLOGY GAPS: **SUPPORTING AN EMERGING INTECONNECTED SYSTEM**

- Significant expansion of interconnection with third-party systems
- Security and resiliency for an energy “internet of things”

RESEARCH AND TECHNOLOGY GAPS: **ADVANCED SENSING, ANALTYICS, AND CONTROL**

- Advanced analytics to leverage the wide-area measurement systems being deployed in the smart grid
- Cyber-physical contingency analysis in support of grid resilience
- Advanced controls for intelligent autonomous or semi-autonomous islanding to achieve resiliency
- Adaptive cybersecurity and resiliency for ICS and power applications

RESEARCH AND TECHNOLOGY GAPS: **ADDRESSING NON-TECHNICAL ISSUES**

- Smart grid components being deployed today will be in the field for a decade or more
- Social, cultural, and human factors

TCIPG VISION AND RESEARCH FOCUS (TCIPG.ORG)

Vision: Create technologies which improve the design of a resilient and trustworthy cyber infrastructure for today's and tomorrow's power grid, so that it operates through attacks

Research focus: Making smart grid systems resilient to malicious attack

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications and architectures
- Quantifying security and resilience

2015 TCIPG SUMMER SCHOOL

- Leverage the emerging Smart Grid Cybersecurity Curriculum
- Will include hands-on training
- Scheduled for June 15-19, 2015, reception June 14
- Venue will be the Q Center near Chicago, IL

2015 Summer School
June 15-19, 2015
Reception: June 14

- www.tcipg.org
- Bill Sanders whs@illinois.edu
- Request to be on our mailing list
- Attend Monthly Public Webinars
- Attend our TCIPG Summer School June 2015