COORDINATED SCIENCE LABORATORY

ILLINOIS

ENGINEERING AT ILLINOIS

Setting the Stage: Computing, Communications, and Cyber Resilience in the Grid

Bill Sanders

ITI.ILLINOIS.EDU

NAS Workshop

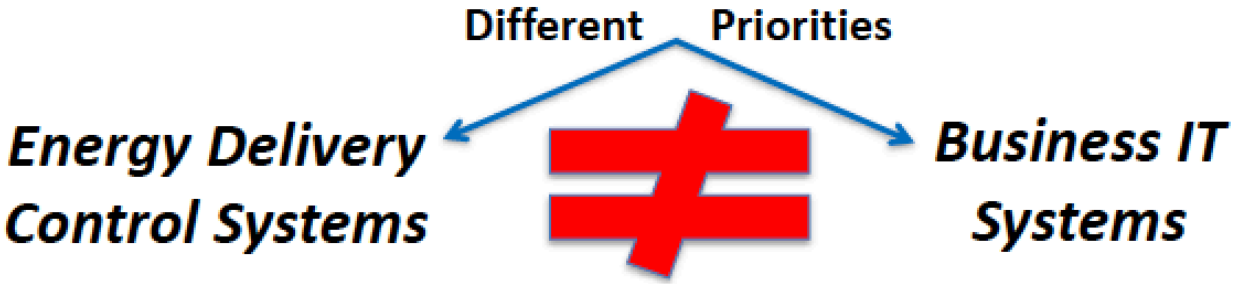
November 1, 2019

INFORMATION TRUST INSTITUTE

The Challenge: Providing Trustworthy Grid Operation in 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.

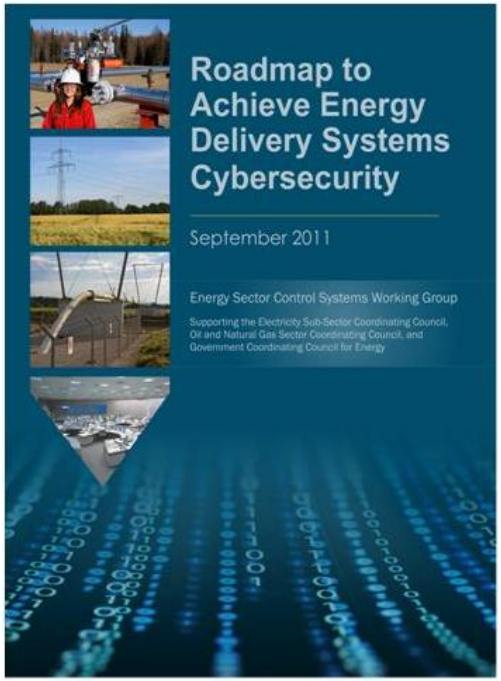
Energy Sector Cybersecurity



- 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, DOE CEDS OVERVIEW PRESENTATION

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 cyber security 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

A Decade of Energy Cyber Infrastructure Attack Malware

- **2010: Stuxnet:** Targeted Siemens industrial control systems in Iran. Was first discovered malware that spies on and subverts industrial systems and the first to include a programmable logic controller (PLC) rootkit.
- **2014: Dragonfly/Havex:** Focus was to collect ICS network and access control information. Evidence suggests this was provided to a well organized and funded group outside countries from which the data was collected.
- **2015: Black Energy 3:** Used in attack on the Ukraine power grid. Considered to be the first known power grid cyberattack. Hackers were able to successfully compromise information systems of three energy distribution companies and temporarily disrupt electricity supply to the end consumers.
- **2016: CRASHOVERRIDE:** Second known attack in Ukraine. Impacted a single transmission level substation. Significant increase in sophistication of attack code relative to past attacks.
- **2017: TRISIS/TRITON:** Incident at a critical infrastructure organization which targeted Schneider Electric's Triconex safety instrumented system (SIS) and where an attacker deployed malware which targeted systems provided emergency shutdown capability for industrial processes. Deployed against at least one victim in the Middle East.

Potential Power-System-Specific 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
- Corrupting Control Information: Smart Meters, SCADA Data, PMU Data, Dispatch Information, etc.
- Sophisticated lateral movement attacks
- Life cycle attacks
- Insider threats
- Physical damage by cyber means
- Combined physical and cyber attacks

TODAY'S CYBER RESILENCY TRENDS, CHALLENGES, AND GAPS.

Disruptive Trends
Challenges
Research and Technology Gaps

Disruptive Trends in the Smart Grid (1/4): *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 (2/4):
Energy "Internet of Things" and Utility Clouds

- Radical changes in the way industrial control systems 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 events"
- Increased dependence on computation and communication will increase the attack surface

Disruptive Trends (3/4): *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 (4/4): *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

Challenges (1/2):
Grid resiliency tied to Cyber Infrastructure Resiliency

- Grid 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

Challenges (2/2): *Grid 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 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

Research and Technology Gaps (1/4): *Advanced Sensing, Analytics and Control*

- Advanced analytics needed to leverage the wide-area measurement systems being deployed in the smart grid
- Cyber-physical contingency analysis must be developed to support grid resilience
- Advanced controls needed for intelligent autonomous or semi-autonomous islanding to achieve resiliency

Research and Technology Gaps (2/4): *Building a Detection and Response Mechanism*

- Detection of suspicious events
  - Profusion of potential attack points
  - Direct detection via cyber traffic analysis
  - Detection informed by physical system state
- Making sense of potential “event avalanche”
  - Situational awareness
  - Comprehend the joint cyber and physical state
- Response
  - Carefully consider consequence of response
  - Ultimately, operate through cyber attack or failure

Research and Technology Gaps (3/4): *Resiliency Assessment*

- Define appropriate security metrics
  - Integrated at multiple levels
  - Applied throughout system lifecycle
  - Be both “process” and “product” oriented
- Determine methods for estimating metrics
  - To choose appropriate architectural configuration
  - To test implementation flaws, e.g., fuzzing, firewall rule analysis
  - Can be applied in cost effective manner *before* an audit
- Link metrics to technical and business concerns

Research and Technology Gaps (4/4): 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

Today's Panels

- Electric Sector Cyber Security: Perspectives on Current Status and Future Concerns
- EMP & GMD: Perspectives on Current Status and Future Concerns
- Where and how should digital technologies be used to improve security and resiliency
- Strategies for moving from a culture of compliance to a culture of security
- How to reconcile the timescales of innovation with standards and regulation
- Boundaries and interactions between utilities and national security efforts

Final Thoughts

- It's critical that we act now; and the basic work has been done to permit quick progress
- Must break out of the current "pierce and patch" mentality
- Solutions require thinking short term and long term at the same time
- Must deeply engage academia, industry, and government
- **For this workshop: Help us understand how to build a modernized grid while improving, not compromising, resiliency and cyber security**