GIAN Short course

Cyber-Physical Security for the Smart Grid

Indian Institute of Technology, Bombay, India

Coordinator: Prof. R. K. Shyamasundar

Manimaran Govindarasu

Dept. of Electrical and Computer Engineering

Iowa State University

Email: gmani@iastate.edu

http://powercyber.ece.iastate.edu

March 5-16, 2018

Course Agenda

Day 01	• Module 1: Cyber Threats, Attacks, and Security concepts
Day 02	• Module 2: Risk Assessment and Mitigation & • Overview of Indian Power Grid
Day 03	• Module 3: Attack-resilient Wide-Monitoring, Protection, Control
Day 04	• Module 4: SCADA, Synchrophasor, and AMI Networks & Security
Day 05	• Module 5: Attack Surface Analysis and Reduction Techniques
Day 06	• Module 6: CPS Security Testbeds & Case Studies
Day 07	• Module 7: Cybersecurity Standards & Industry Best Practices
Day 08	• Module 8: Cybersecurity Tools & Vulnerability Disclosure
Day 09	• Module 9 : Review of materials, revisit case studies, assessments
Day 10	• Module 10: Research directions, education and training

Cyber and Control Systems Security Standards for Electric Power Systems

Organizations for Cyber Security Standards

- **IEEE** **–** Institute of Electrical and Electronics Engineers
- **IEC** – International Electro-technical Commission
- **NERC** – North American Electric Reliability Council
- **CIGRE** – International Council on Large Energy Systems
- **FERC** – Federal Energy Regulatory Commission
- **PSRC** – Power Systems Reliability Committee

Protocol	Scope
IEEE 1402	Electric Power Substation Physical and Electronic Security
IEC 62351	Data and Communication Security
NERC CIP	Cyber Security Standards (CIP Standards) [www.nerc.com]
FERC SSEMP	Security Standards for Electric Market Participants
NISTIR 7628	Smart Grid Cyber Security

Outline of **Module 7**

- **US NERC CIP Compliance & NERC GridEx**
- US NISTIR 7628
- US DHS ICS Best Practices
- US DOE Cybersecurity Capability Maturity Model (C2M2) & DOE CEDS Roadmap

NERC – Critical Infrastructure Protection (CIP)

Objective: Physical, cyber and operational security for bulk power system

Identify vulnerabilities and countermeasures

Vulnerability and risk assessment

Cyber and physical countermeasures

Threat response

Communications

Support operation and protection

Facility and field equipment

Physical security

IT/Cyber security

Deterrence, prevention, detection and correction

Protecting sensitive data

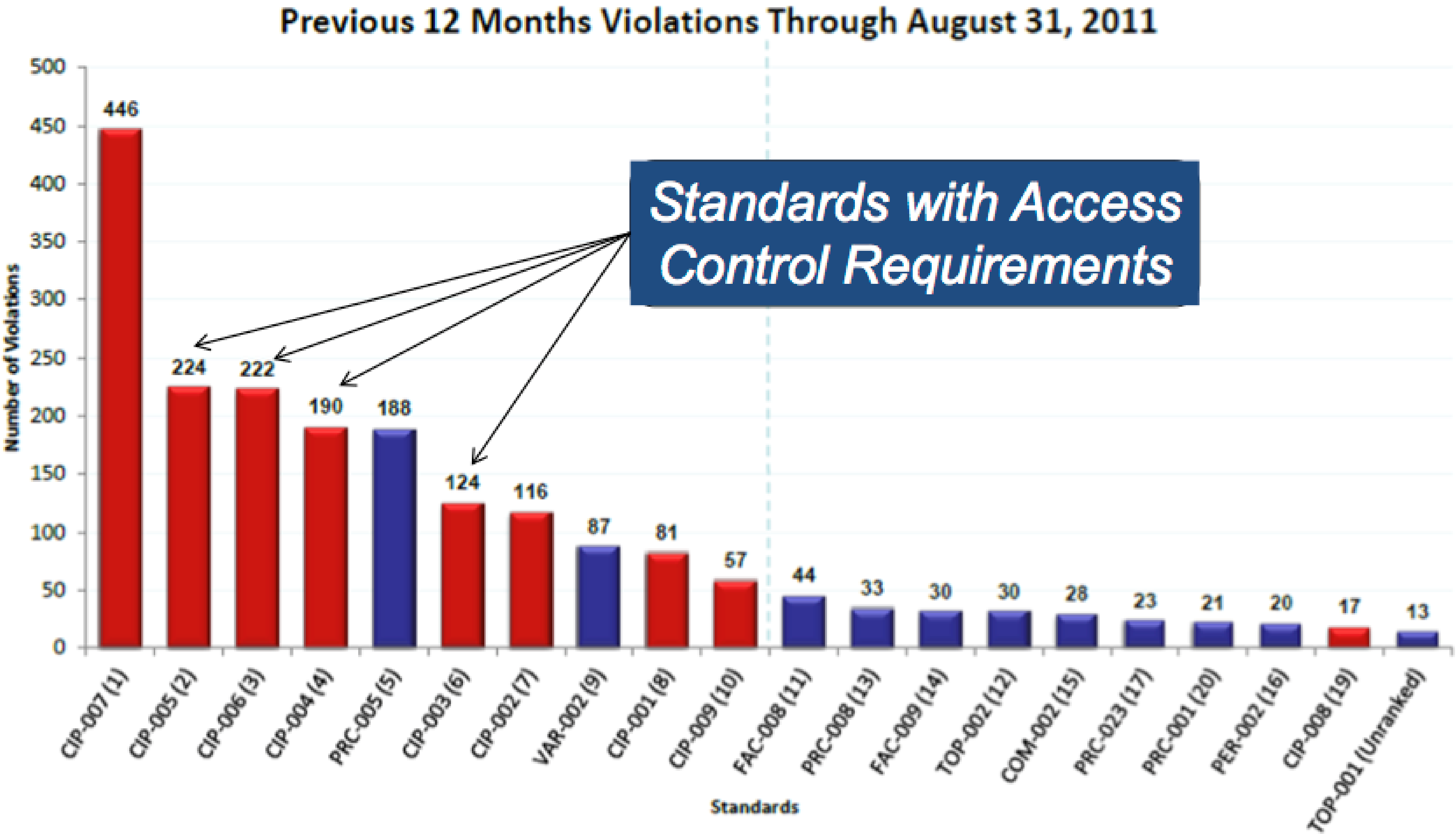
Production, storage, transmission and disposal

CIP compliance penalties - example

- Enforced by FERC
- Non-compliance attracts high penalties

	Violation Severity Level							
Violation Risk Factor	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
Medium	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
High	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

CIP compliance violations during early years



NERC – CIP Standards (ver. 5), current version: 6

CIP - 002	Critical Cyber Asset Identification
CIP - 003	Security Management Controls
CIP - 004	Personnel & Training
CIP - 005	Electronic Security Parameters
CIP - 006	Physical Security
CIP - 007	Systems Security Management
CIP - 008	Incident Reporting and Response
CIP - 009	Recovery Plans
CIP - 010	Configuration Change Management and Vulnerability Assessments
CIP - 011	Information Protection

CIP 002-5: Cyber Security —BES Cyber System Categorization

- To identify and categorize **Bulk Electric System (BES) Cyber Systems** and their associated BES Cyber Assets
- Defining cyber security requirements commensurate with the adverse impact could have on the reliable operation of the BES.
- Identification and categorization of BES Cyber Systems impacting the Bulk Electric System as having a high, medium, or low impact.

Critical Cyber Assets

- Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
  - The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter
  - The Cyber Asset uses a routable protocol within a control center
  - The Cyber Asset is dial-up accessible
  - The Cyber Asset participates in, or is capable of, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset.
  - The Cyber Asset displays, transfers, or contains information relied on to make Real-time operational decisions that are essential to the reliable operation of a Critical Asset.
  - The Cyber Asset fulfils another function essential to the reliable operation of the associated Critical Asset and its Loss, Degradation, or Compromise would affect the reliability or operability of the BPS.

CIP 002-5: Criteria for Impact Ratings

High Impact:

- Control centers of a Reliability Coordinator
- Balancing Authorities (for gen > 3000MW in a single interconnection)
- Transmission Operators
- Generation Operators

Medium Impact:

- Generating units (gen < 1500 MW in a single interconnection)
- Reactive resources (gen <= 1000 MVAR)
- Transmission facilities (voltage > 500kV)
- Transmission facilities (200kV<=voltage<=499kV, aggregate weighted value>3000)
- Generating station (identified by Reliability Coordinator as '*critical*')
- Remedial Action Schemes
- Automatic Load Shedding (load>300MW)
- Control centers (gen<1500MW)

Low Impact:

All others outside Medium and High Impact categories

CIP 003-5: Cyber Security – Security Management Controls

Requires that each Responsible Entity review and obtain **CIP Senior Manager** approval at least once every **15 months** of documented cyber security policies for its **High and Medium** Impact BES Cyber Systems that address:

- Personnel & training
- Electronic Security Perimeters, including Interactive Remote Access
- Physical security of BES Cyber Systems
- System security management
- Incident reporting and response planning
- Recovery plans for BES Cyber Systems
- Configuration change management and vulnerability assessments
- Information protection
- Declaring and responding to CIP Exceptional Circumstances.

For Low Impact BES Cyber Systems, the standard requires that the Responsible Entity implement "in a manner that identifies, assesses, and corrects deficiencies." - possible refinement of this requirement …

CIP 004-5: Cyber Security- Personnel and Training

- Requires documented processes or programs for protecting High and Medium Impact BES Cyber systems
  - Security awareness
  - Cyber security training
  - Personnel risk assessment
  - Access management

CIP 006-5 Cyber Security – Physical Security of BES Cyber Systems

- Manage physical access to BES Cyber Systems through a specified physical security plan in support of protecting High and Medium Impact BES Cyber Systems

- Requirements categories
  - Physical Security plan
  - Monitoring Unauthorized Access
  - Visitor Control
  - Physical Access Control System Maintenance and Testing

CIP 007-5 Cyber Security – Systems Security Management

- Manage system security by specifying select technical, operational, and procedural requirements in support of protecting High and Medium Impact BES Cyber Systems against compromise.

- Requirements Categories
  - Ports and Services
  - Security Patch Management
  - Malware Prevention
  - Security Event Monitoring
  - System Access Control

CIP 008-5 Cyber Security – Incident Reporting and Response Planning

- Mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements.
- Measures to follow includes Cyber Security Incident response processes or procedures that define roles and responsibilities for
  - Monitoring
  - Reporting
  - Initiating
  - Documenting of the incident.
- Requires testing of plans at least once every **15 months.**

CIP 009-5 Cyber Security – Recovery Plans for BES Cyber Systems

- Recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability, and reliability of the BES.
- Requirements categories
  - Conditions for recovery plan activation
  - Roles and responsibilities of responders
  - Documented process for backup and restoration
  - Documented process for data preservation
- Requires testing of recovery plans once every **15 months.**

CIP 010-1 Cyber Security – Configuration Change Management and Vulnerability Assessments

- Prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment
- Requirements categories
  - Developing and documenting baseline configurations
  - Verifying changes to baseline before implementation
  - Testing changes in a test environment for High Impact BES Cyber system
- Requires active Vulnerability Assessments once every **15 months.**

CIP 011 -1 Cyber Security – Information Protection

- Prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise

- Requirements

  – Procedures for protecting and securely handling BES Cyber System information, including storage, transit, and use.

  – Procedures for reuse and disposal of BES Cyber assets.

NERC CIP and Synchrophasors

- NERC CIP 002-4 standard requires the identification and documentation of all **BES Cyber Systems** impacting the BES as **high, medium and low impact** assets.
- Is Synchrophasor a '**High or Medium Impact**' BES Cyber asset?
    - Is it used in a key control algorithm?
    - Does it support Bulk Electric System reliability?

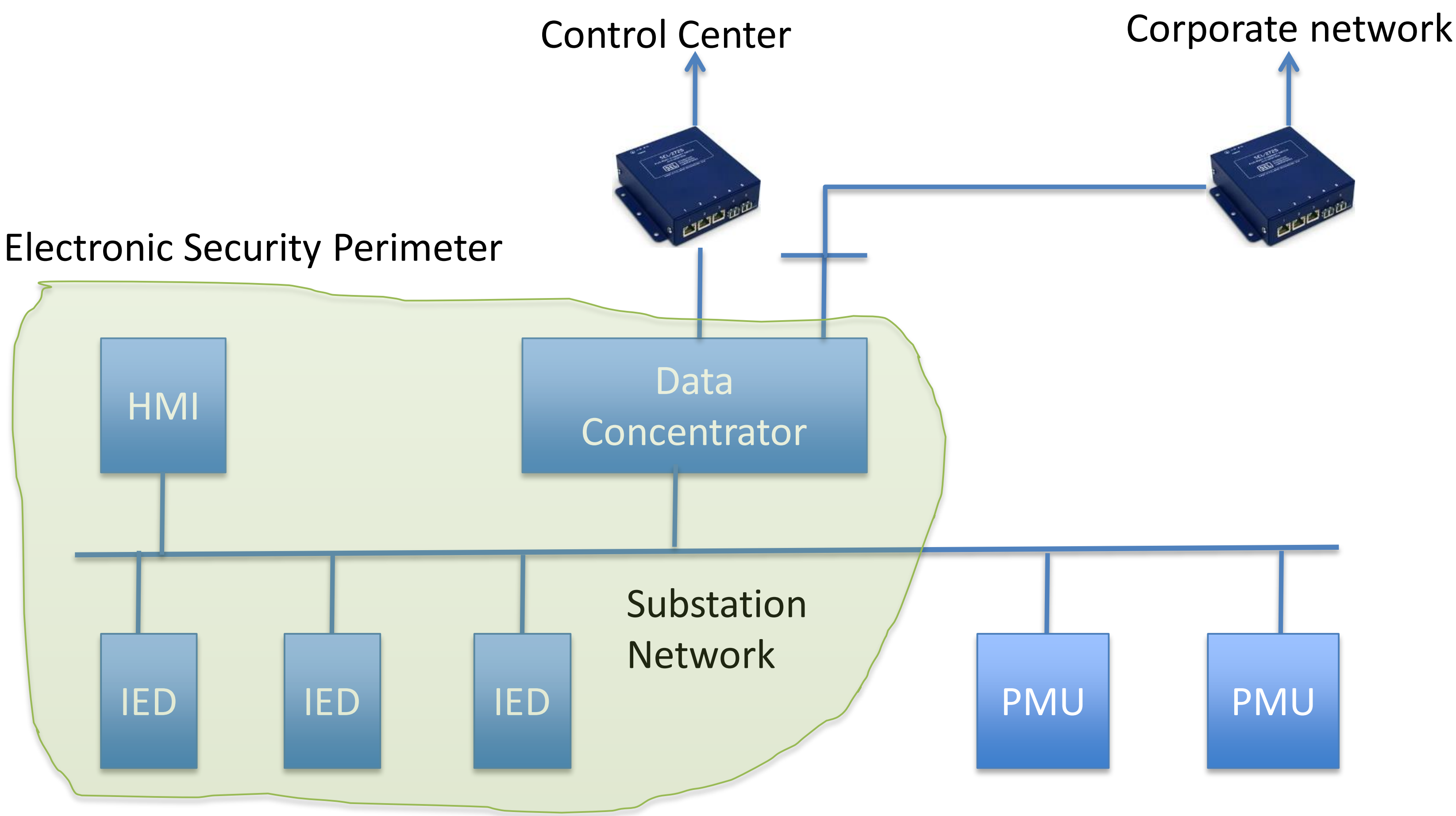
Source: North American Electric Reliability Council (NERC) Critical Infrastructure Protection Standards CIP 001-009 (www.nerc.com)

NERC CIP and Synchrophasors

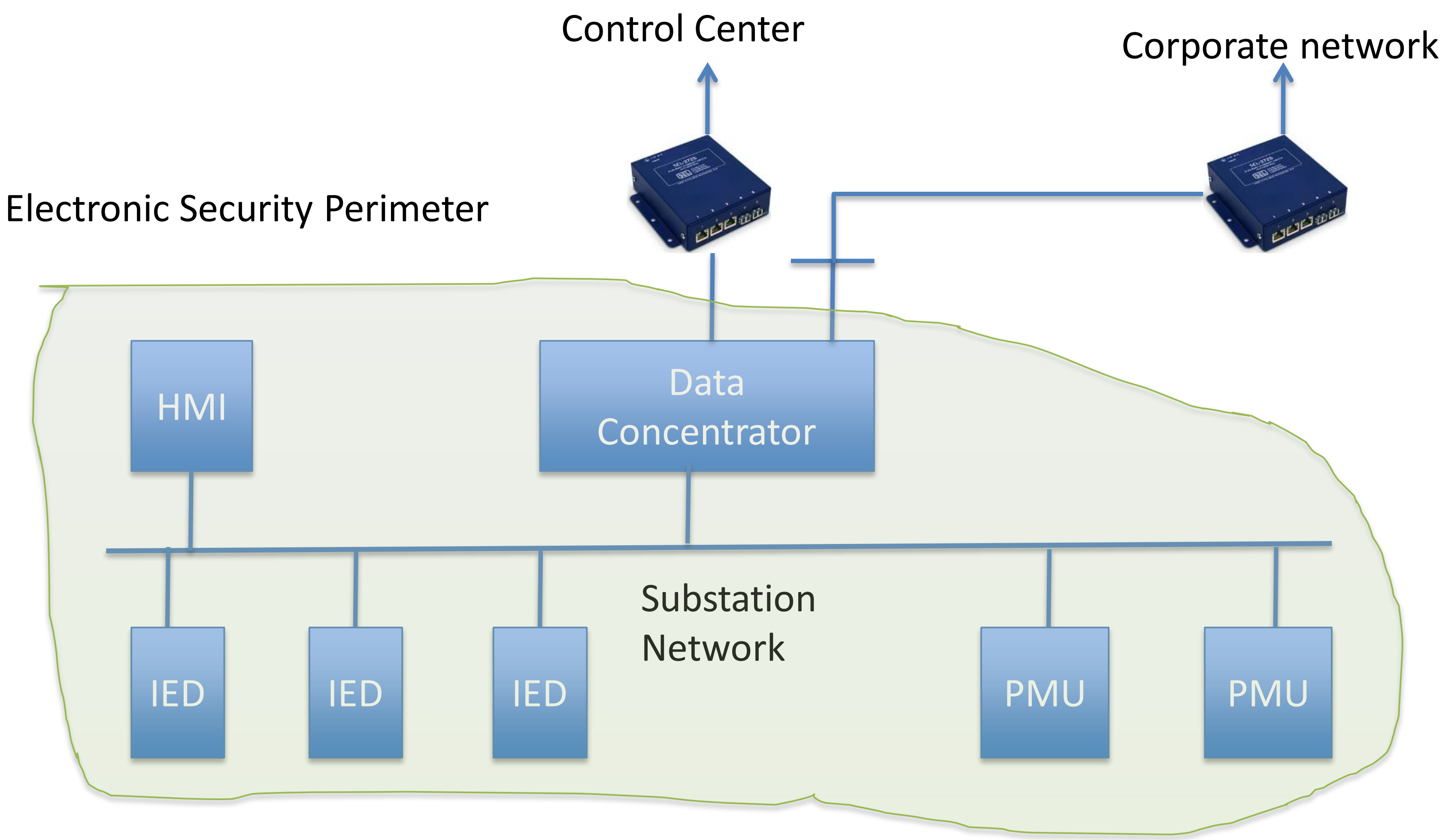
- Currently, Synchrophasor data is not used for mission-critical applications
- Synchrophasors under 'BES Cyber Assets'
  - If Synchrophasor data is used for real-time control applications?
  - Then, NERC CIP compliance applies to synchrophasor data and infrastructure.
- Also, NERC CIP 005-5 requires the identification of an "**Electronic Security Perimeter**" to manage electronic access to the BES cyber system elements in support of protecting them against malicious cyber events.

Source: North American Electric Reliability Council (NERC) Critical Infrastructure Protection Standards CIP 001-011 (www.nerc.com)

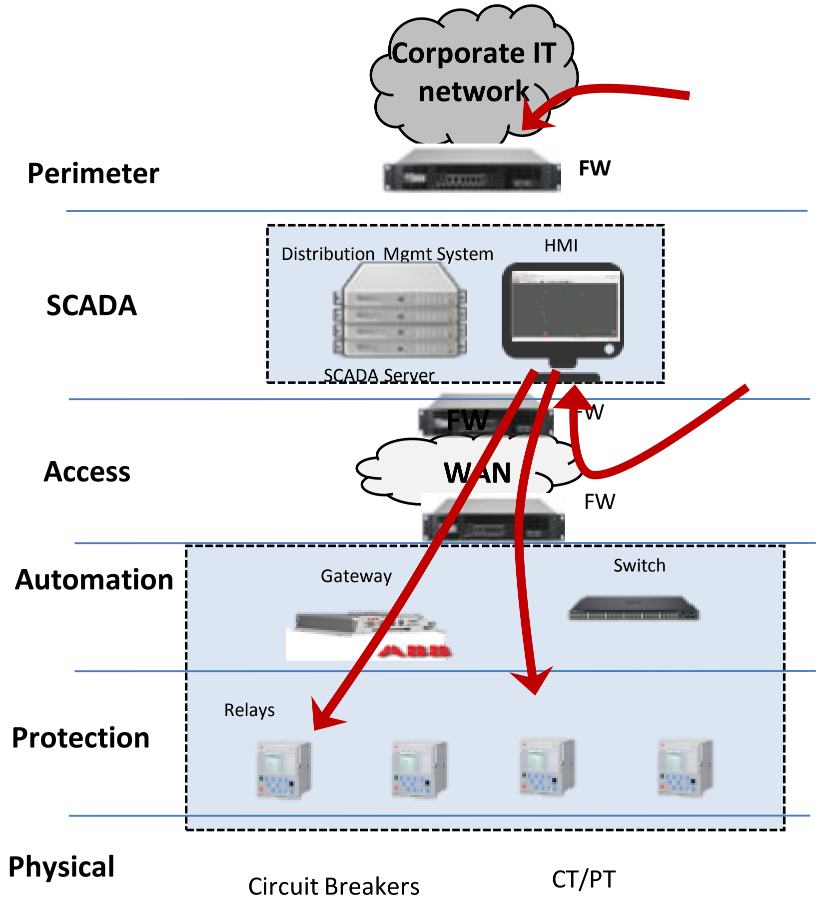
NERC CIP and Synchrophasors: Current State ?



NERC CIP and Synchrophasors: Future State



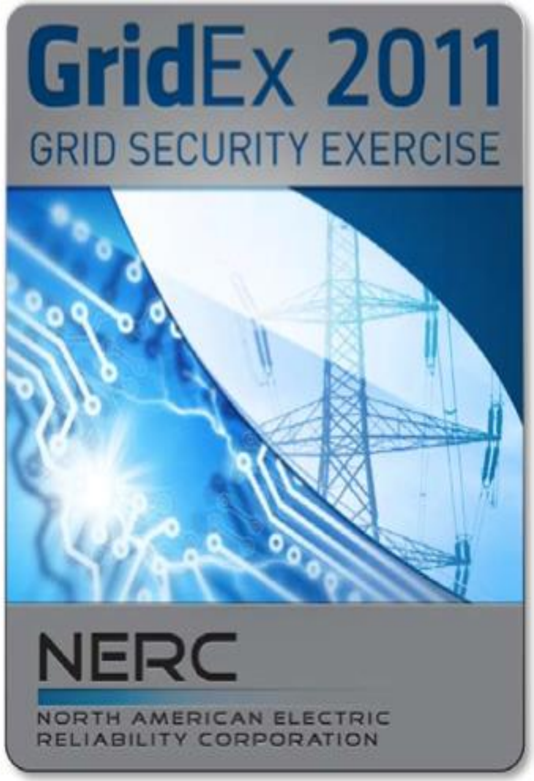
Prevention & Detection (NERC CIP)

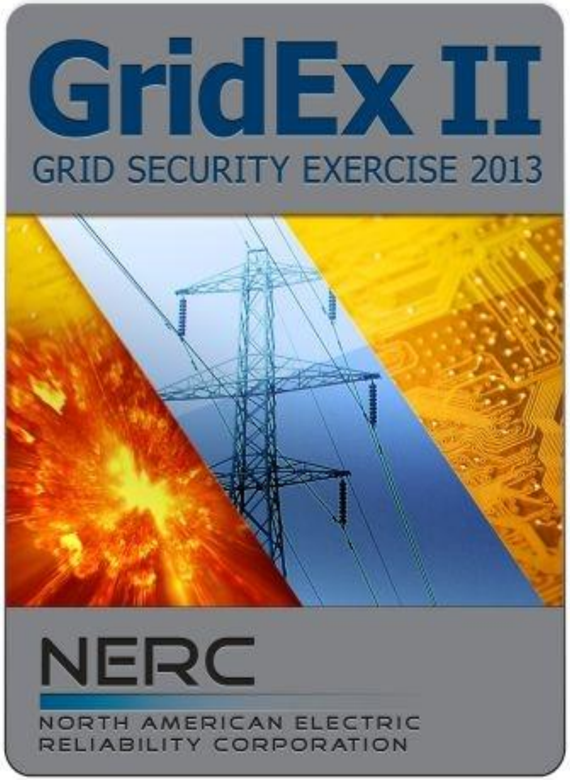


NERC CIP Controls	OT Pre-Impact
CIP-005-5 R1.3 Multi-factor authentication for interactive sessions	3.ot vpn login Stolen credential from DC used to remotely login to vpn
CIP-007-5 R3.1 Deploy methods to deter, detect, and prevent malicious code	4.install malware BlackEnergy malware installed on control systems
	5.remote hmi session Created remote operators session to SCADA server
CIP-005-5 R1.3 Mechanisms to detect malicious communications	6.trip breakers Operate key circuit breakers, 225,000 customers offline

Ack: Adam Hahn, Washington State University

NERC CIP Outreach





NERC CIP Outreach

- **Critical Infrastructure Department (CID)** coordinates NERC's efforts to share CIP information.
  - Standards development, risk assessment and preparedness, industry alerts, webinars and conferences

Some examples of CID's outreach activities are:

- **Grid Security Exercise (GridEx) series**
- **Grid Security Conference (GridSecCon) series**
- **Sufficiency Review Program (SRP)**
- **Critical Infrastructure Protection Compliance program**

GridEx series

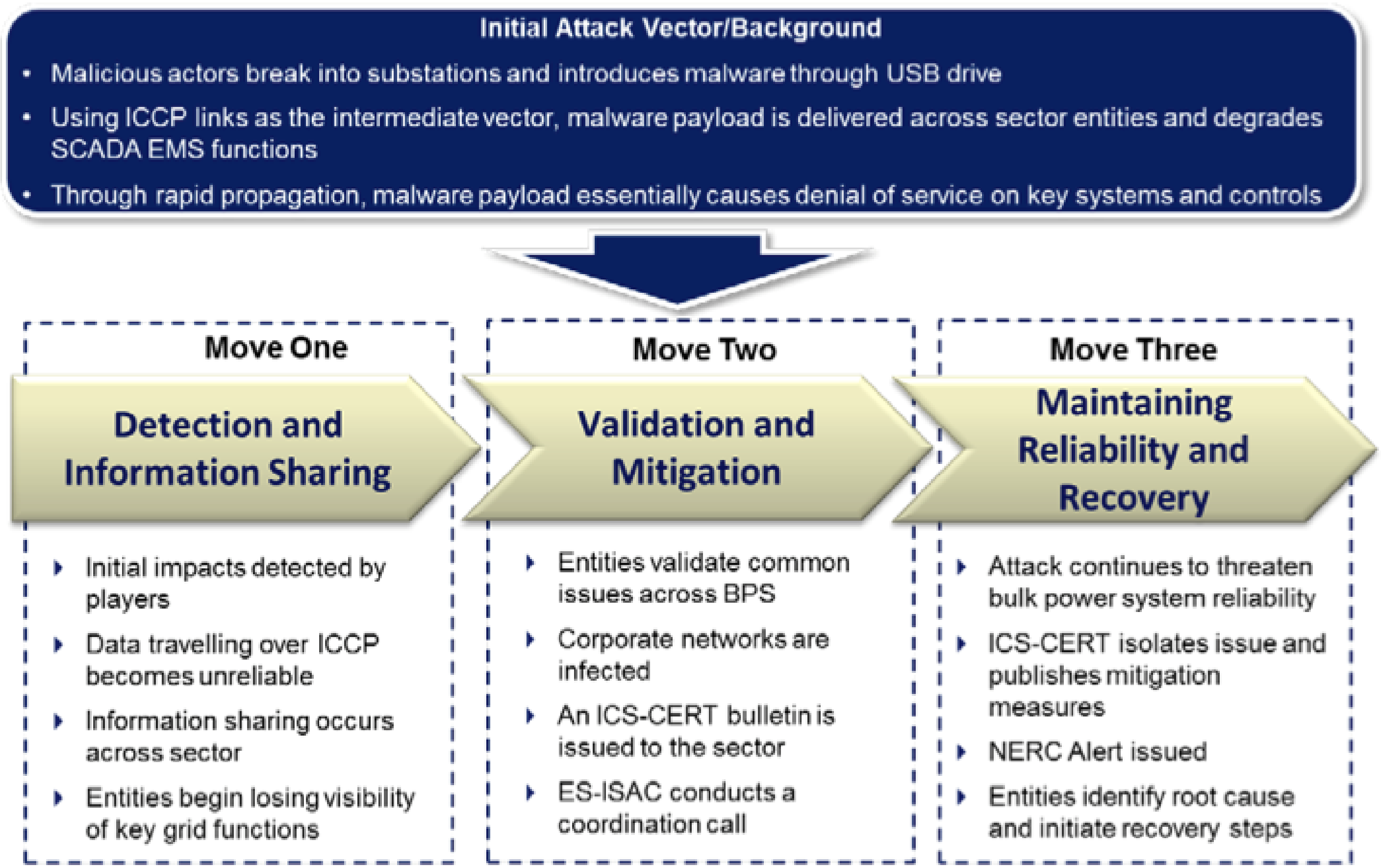
Grid Security Exercise (GridEx) series, a North American-wide biennial physical security and cybersecurity exercise

Objectives:

- Validate the current readiness of the electricity industry to respond to a cyber incident and provide input for security program improvements
- Exercise NERC and industry crisis response plans and identify gaps in plans, security programs, and skills
- Assess, test, validate existing command, control, and communication plans for key NERC stakeholders
- Identify potential improvements in physical and cybersecurity plans, programs and responder skills (GridEx II)

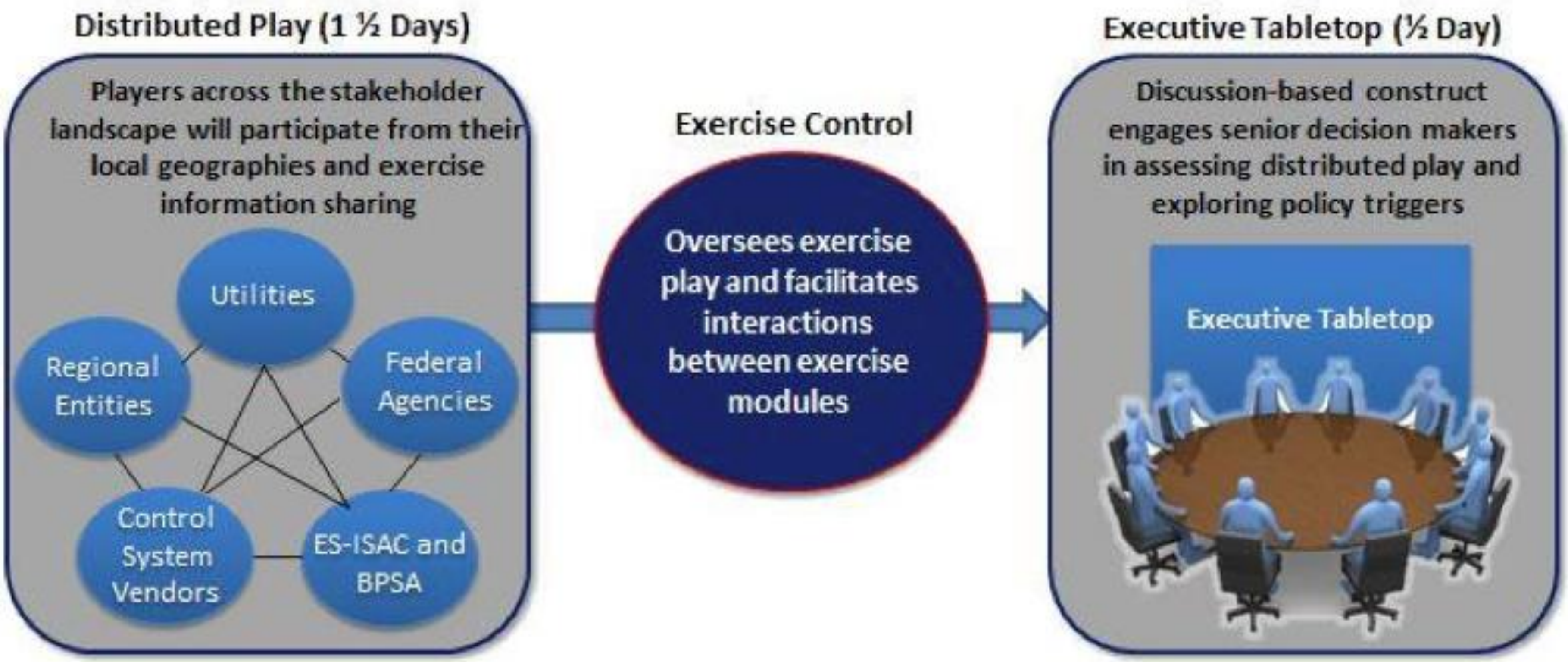
GridEx I: Scenario narrative

- Malware consistent with APT introduced



Source: NERC GridEx After-Action Report

GridEx II: Scenario Construct



Source: NERC GridEx II, After-Action Report

GridEx II: Lessons learned

- Continue to Enhance Information Sharing
- Continue to Enhance NERC Coordination
- Challenge of Simultaneous Attack
- Continue Improvement of Incident Response
- Continue Improvement of Situational Awareness Content
- Continue to Improve the Grid Exercise Program

GridEx II: Lessons learned

- Tabletop Exercise
  - Situation Assessment Scalability
  - Public Communications
  - Unity of Effort
  - Cyber Attacks Create Unique Restoration Challenges
  - Physical Attacks Create Unique Restoration Challenges
  - Mutual Aid and Critical Spares

GridSecCon

Grid Security Conference (GridSecCon) series, an annual forum for policy and information sharing on CIP and other security issues and is organized every year by NERC.

Objectives:

- Promoting reliability of the bulk power system (BPS) through training and industry education.
- Delivering cutting-edge discussions on Critical Infrastructure Protection (CIP) security threats, vulnerabilities, and lessons-learned from senior industry and government leaders.
- Informing industry with security best-practice discussions on reliability concerns, risk mitigation, and physical and cybersecurity threat awareness.

Outline of **Module 7**

- US NERC CIP Compliance & NERC GridEx
- **US NISTIR 7628**
- US DHS ICS Best Practices
- US DOE C2M2 model & DOE CEDS Roadmap

NIST – Smart Grid Interoperability Panel

NIST – Smart Grid Scope

- **Research**
  - Energy management and Metering
  - Smart-grid Architecture and Operations
  - Wide-Area Monitoring and control
  - Communication protocols and cybersecurity
  - Electric vehicles and storage
- **Standards Development**
  - Interoperability standards
  - Cybersecurity standards [**NISTIR 7628** – Guidelines for Smart Grid Cyber Security]

NISTIR 7628 – Guidelines for Smart Grid Cybersecurity

Vol. 1 **Security Strategy, Architecture and High-Level Requirements**

- Applicability of CIA in the smart grid environment
- Access control, Cryptography and key management
- Risk management and assessment

Vol. 2 **Privacy and the Smart Grid**

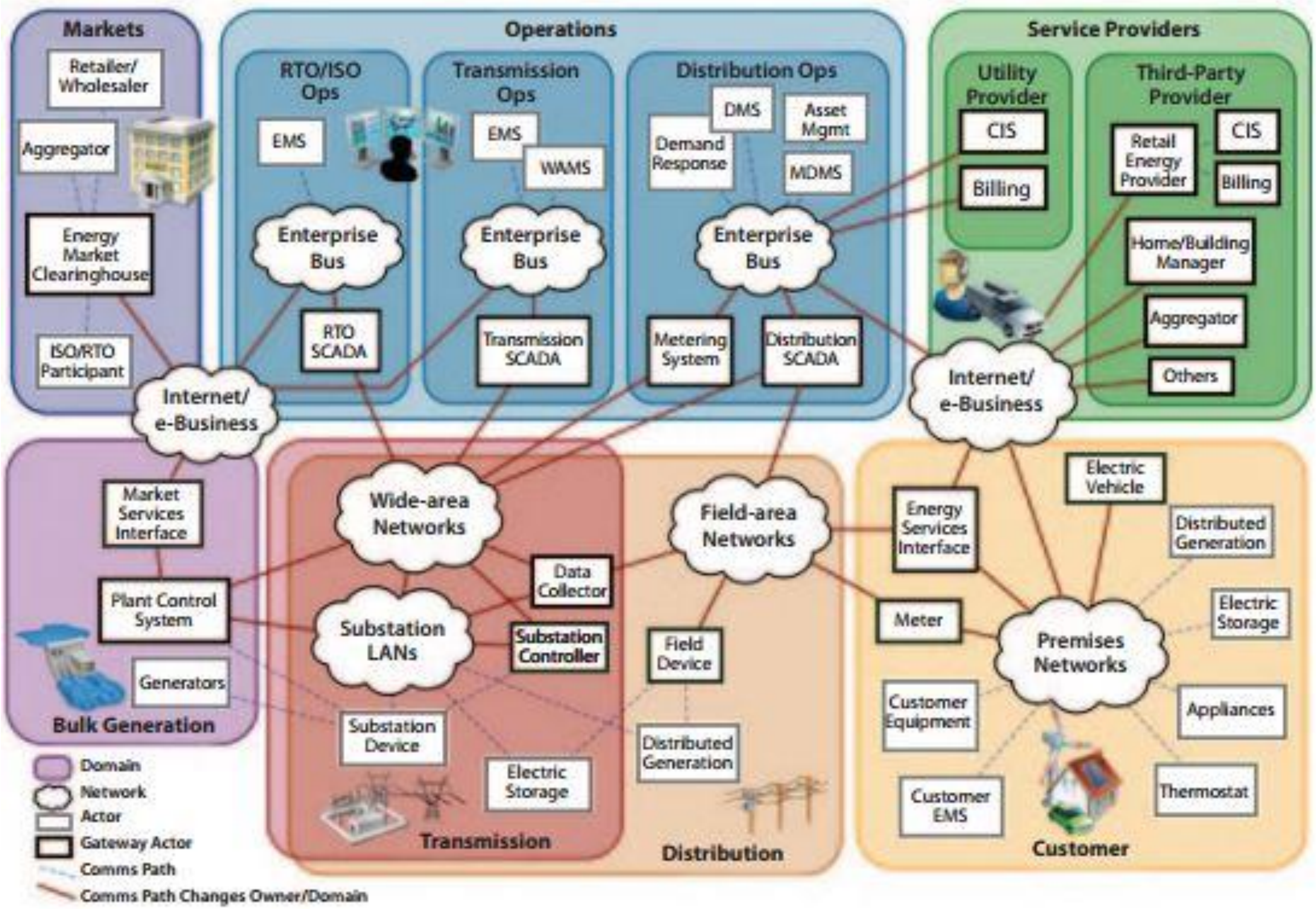
- New privacy concerns and classification of privacy
- Laws and regulations with respect to privacy

Vol. 3 **Supportive Analysis and References**

- Vulnerability definition and classification
- Bottom-up Security Analysis
- Security requirements –
    - Device security
    - Cryptography and key management
    - Network security
    - System security architectures

NIST SGIP Smart Grid schematic

"The Future of the Electric Grid" MIT Report



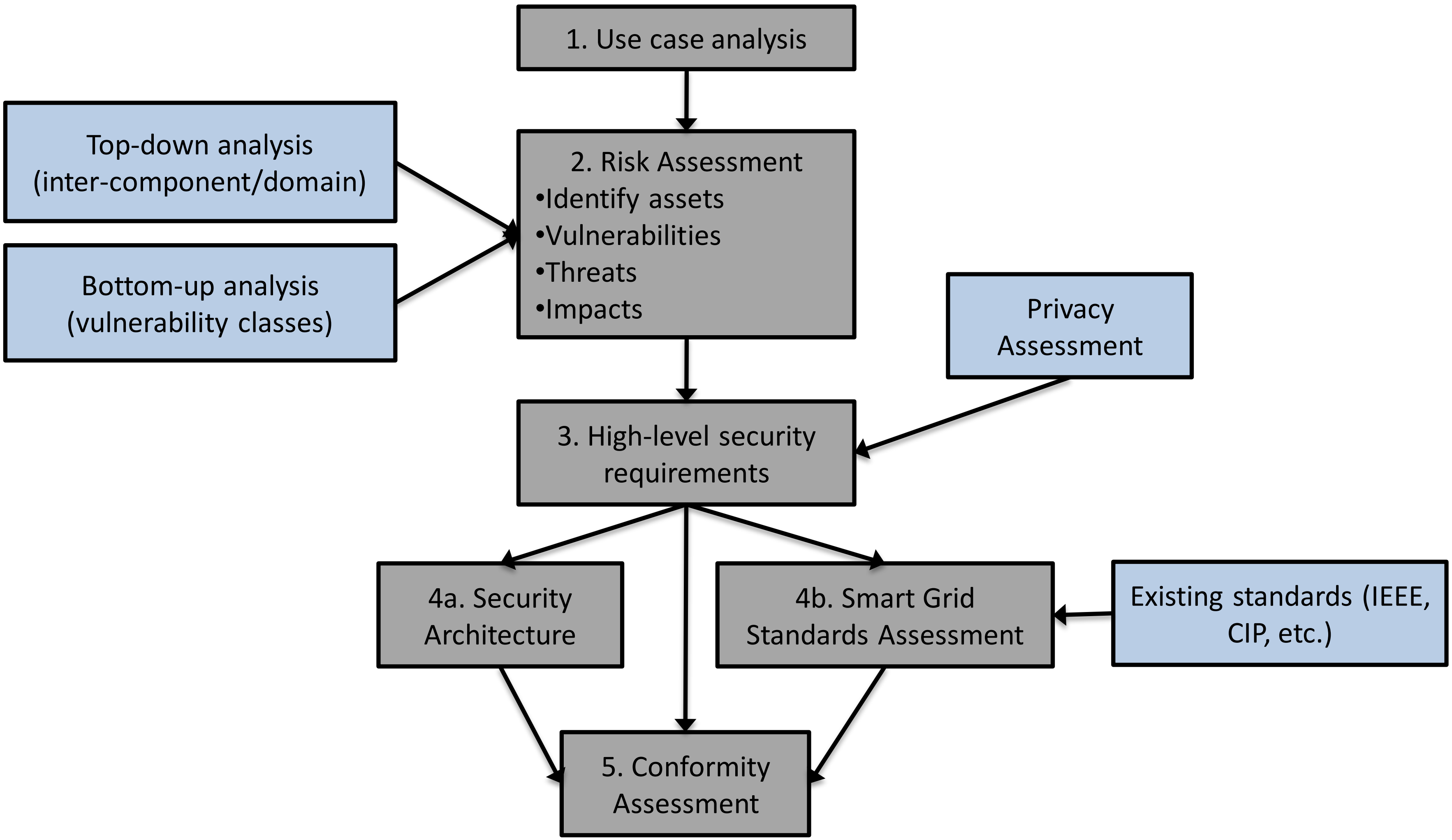
NISTIR 7628 Framework

- NISTIR 4628 identifies 8 priorities: demand response and consumer energy efficiency, wide-area situational awareness, energy storage, electric transportation, advanced metering infrastructure, distribution grid management, cybersecurity, and network communications.

- It presents an analytical framework organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart-grid-related characteristics, risks, and vulnerabilities.

- Two approached are used for risk assessment – top down approach and bottom up approach.

NISTIR 7628 – Smart Grid Cyber Security Strategy



Sample analysis of NISTIR 7628 - for EV charging

- Example: Security vulnerabilities of NISTIR 7628 for EV ecosystem.

- Device Authentication:

The authentication/identification of EV devices for charging

- The consumer privacy against utility-operator

Device Identification/Authentication

- Substitution attacks can happen
  - Stolen vehicles charging …
- Potential solutions
  - Using physical processes, events, or characteristics that appear on the charging cable and are measurable by both the EV and the charging station, but are difficult for the attacker to measure or clone.
  - Applying a distance bounding protocol wherein the charging station sends a challenge to the IED, which responds according to the challenge, and the delay of receiving a response since a challenge has been sent and is used as a test for physical proximity

EV Location Privacy

- The major problem of NISTIR 7628 is that it regards the utility operator always as a trusted entity.

- It is important to raise awareness that the attacker might breach the privacy of EV owners.

- The privacy of EV owners could possibly be protected through the use of a cryptographic protocol combined with the EV playing the man in the middle to relay all messages between the servers and charging station.

Standard needs to evolve …

- Cybersecurity has been identified as an area falling short of the expectation of the envisioned smart grid, its standardization has relatively slow progress compared to other areas of smart grid research.

- The NISTIR 7628 framework might not be able to capture all the essential security criteria by demonstrating two types of vulnerabilities: a substitution attack on EV device authentication and the user location privacy problem.

- NISTIR 7628 only considers cybersecurity alone, which may not be adequate.

- There is need for cyber-physical security that is essential since the physical aspect cannot be ignored in systems such as the smart grid.

Cyber security Best Practices

***Defense in Depth** approach*

Protect network boundaries

Protect computing environment

Firewalls

- Limit inbound and outbound connections
- Authorize appropriate outbound connections
- Filter malicious traffic

Intrusion Detection/Prevention Systems

- Analyze network traffic in near real-time
- Based on signatures, anomaly based

- Regular OS patching and updating
- OS Hardening
- Periodic Anti-virus updates
- Use of Host based Firewalls
- Routine Vulnerability Scanning
- Use of Proxy servers and Web content filters
- Email attachment filtering
- Monitoring logs
- Authorize devices on LAN

Source: Malware Threats and Mitigation Strategies, US-CERT Informational Whitepaper, May 2005

ICS-CERT best practices…..

- Implement account lockout policies to reduce the risk from brute forcing attempts.

- Implement policies requiring the use of strong passwords

- Monitor the creation of administrator level accounts by third-party vendors.

- Adopt a regular patch life cycle to ensure that the most recent security updates are installed.

Source: http://www.ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

US ICS-CERT best practices

- Minimize network exposure for all control system devices.
- Firewall and isolate control network
- Secure remote access using VPN's
- Account lockout policies
- Password management policies
- Access control management policies
- Patch management policies

Source: http://www.ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

ICS-CERT best practices

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Remove, disable, or rename any default system accounts wherever possible.

Source: http://www.ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

ICS CERT Best Practices for Malware in ICS

- Identify effective and safe cleaning procedures that could be used to remove the malicious software

- Identify best practices to prevent and detect future malware infections in every organization's control environment

Malware Mitigation Strategies

- Multiple layers of defenses – ***Defense in Depth*** *approach*
- Tradeoff between protection, capability, cost, performance and operational considerations
- Defense in depth layers:
  - *Protect network boundaries*
  - *Protect computing environment*

Source: Malware Threats and Mitigation Strategies, US-CERT Informational Whitepaper, May 2005

Outline of **Module 7**

- US NERC CIP Compliance & NERC GridEx
- US NISTIR 7628
- US DHS ICS Best Practices
- US DOE C2M2 model & DOE CEDS Roadmap

DOE Cybersecurity Capability Maturity Model (C2M2)

Source: US Department of Energy, NERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE, 2015

- “This Framework Implementation Guidance designed to assist organization to
- Characterize their current and target cybersecurity posture
- Identify gaps in their existing cybersecurity risk management programs using the Framework as a guide
- identify areas where current practices may exceed the Framework.
- Recognize that existing sector tools, standards, and guidelines may support Framework implementation
- Effectively demonstrate and communicate their risk management approach and use of the Framework to both internal and external stakeholders.”

Energy Sector C2M2 (ES-C2M2)

C2M2 Framework has three steps:

- Domains – domains covered
- Scaling -- Maturity Indicator Level (MIL)
- Diagnostic Methodology (Assessement)

Source:

https://resources.sei.cmu.edu/asset_files/Webinar/2014_018_101_294052.pdf

Roadmap to Achieve Energy Delivery Systems Cybersecurity, US DOE, 2011

Vision: Secure and resilient energy delivery system withstanding cyber attacks

Barriers: Legacy infrastructure, dynamic threat landscape, increasing attack surface ….

Five-step **Strategy:**

- Build a Culture of Security
- Assess and Monitor Risk
- Develop and Implement New Protective Measures to Reduce Risk
- Manage Incidents
- Sustain Security Improvements

Emerging latency requirements for Energy Delivery Systems (Source: DOE CEDS Roadmap)

- <= 4 msecs for protective relaying
- Sub-seconds for transmission wide-area situational awareness monitoring
- Seconds for substation and feeder supervisory control and data acquisition (SCADA) data

- Minutes for monitoring noncritical equipment and some market pricing information
- Hours for meter reading and longer term market pricing information
- Days/weeks/months for collecting long-term data, such as power quality information

Roadmap structure

- Near-term milestones (0-3 Years)
- Medium-term milestones (4-7 Years)
- Long-term issues (8-10 Years)

For each Strategy (1-5)

- Milestones
- Barriers
- Priorities

Source: US DOE CEDS Roadmap, 2011

https://www.energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf

Summary

- Cyber Security standards overview
- NERC CIP – Standards, Compliance Process
- NERC GridEx – Scenarios, Findings, Recommendations
- NISTIR 7628 Guidelines
- DHS Cyber Security best practices
- DOE C2M2 model & DOE CEDS Roadmap