SYSTEM ENGINEERING APPROACHES TO ELECTRIC GRID CYBERSECURITY CHALLENGES

Webinar Presenters

Kay Stefferud

Director of Implementation Services

kay@enernex.com

Brian Smith

Principal Consultant

bsmith@enernex.com

Agenda

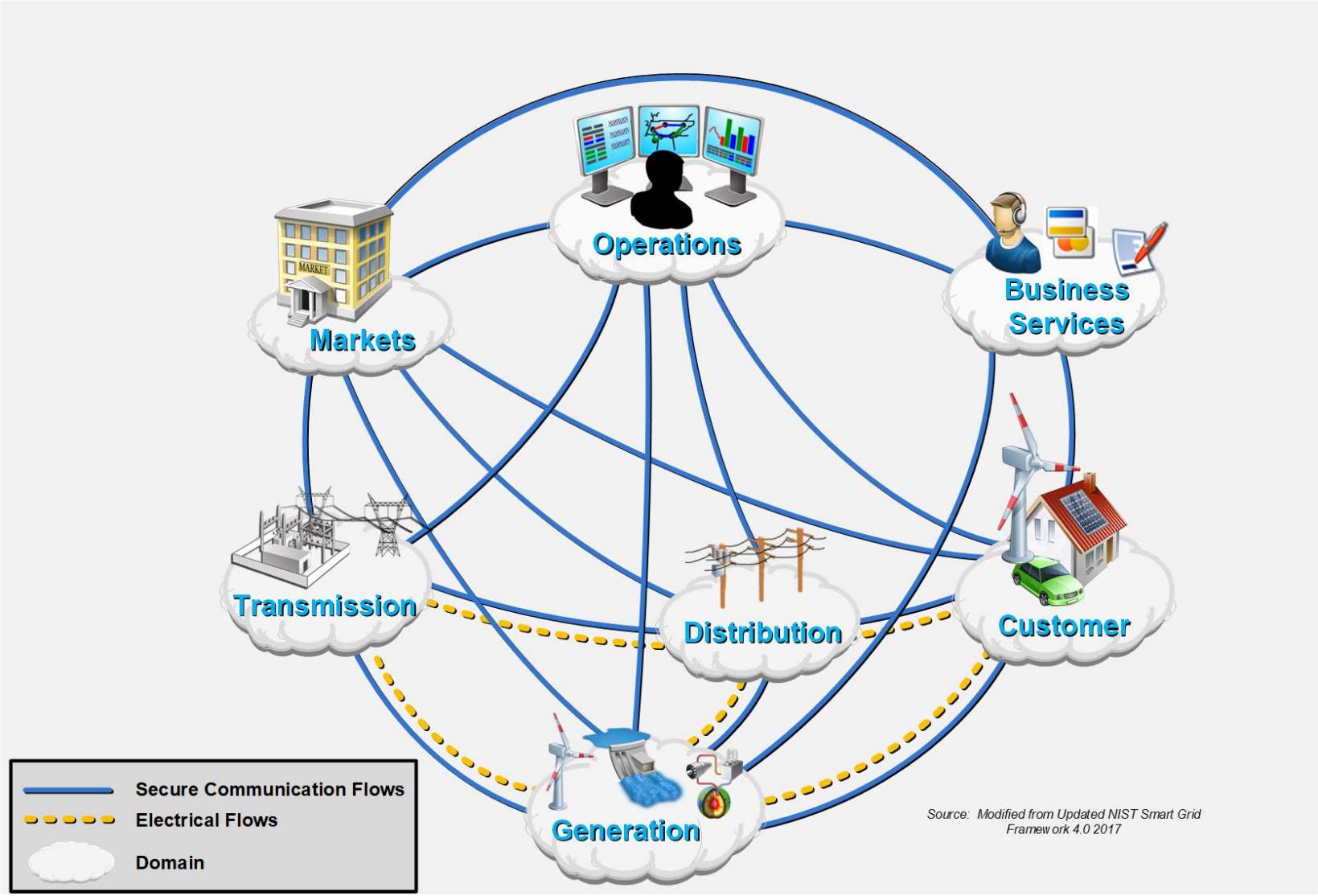
- *Topic 1: The Electric Grid - A Systems of Systems*
- *Topic 2: Cybersecurity Frameworks & Assessing and Qualifying Risk in OT Environments*
- *Topic 3: Developing OT Cybersecurity Architecture and Requirements*
- *Topic 4: Vulnerability Assessment and Testing*
- *Topic 5: Example*
- *Q&A*

EnerNex
A CESI Company

TOPIC 1

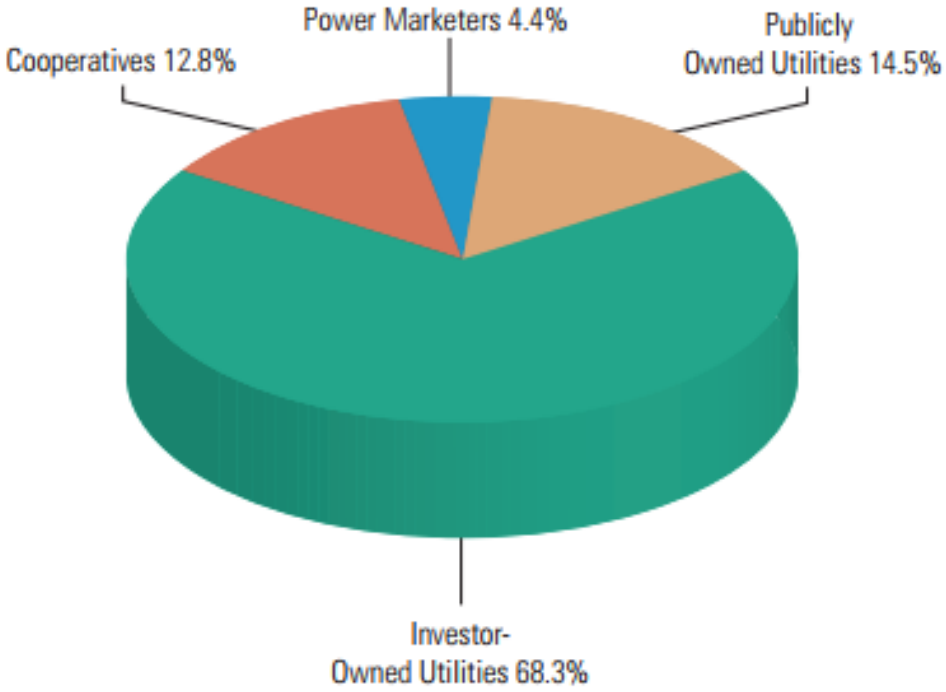
THE ELECTRIC GRID: A SYSTEM OF SYSTEMS

Electric Grid System of Systems



Electric Utilities General Overview

- *Approximately 3100 electric utilities in the US*
- *Three Major Categories:*
  - Investor Owned Utility -IOU (approx. 200)
  - Public Utilities Municipal - government or city-owned (approx. 2000)
  - Rural or Co-operative (aka Co-ops) member-owned (approx. 900)



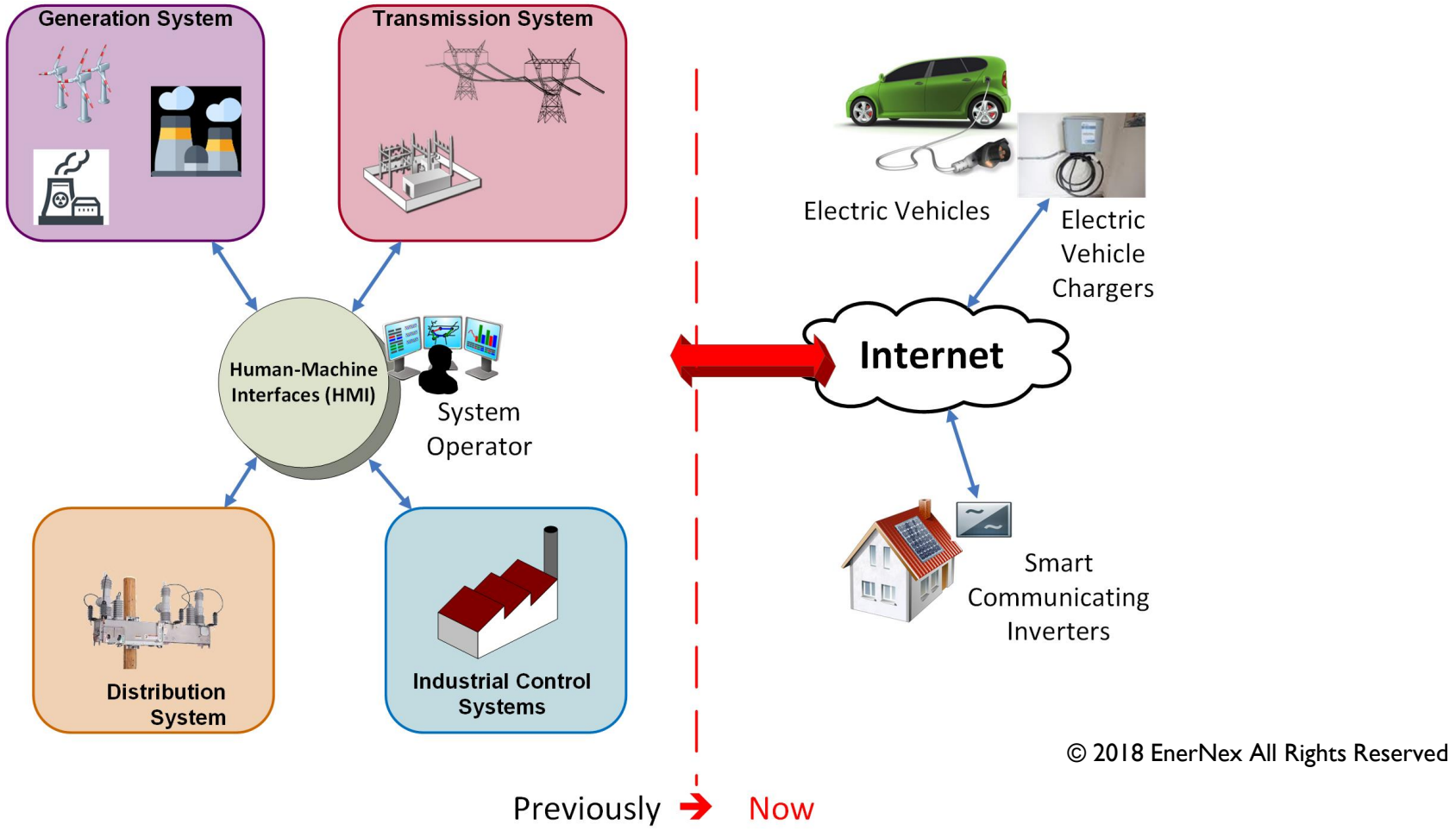
148 million electric customers in the US

200 Investor Owned Utilities (IOUs) such as SDG&E, serve most customers

Cyber attacks can target over 3100 separate electric utilities

SCADA Control Systems

- *Supervisory Control And Data Acquisition (SCADA) Control Many Grid Devices*

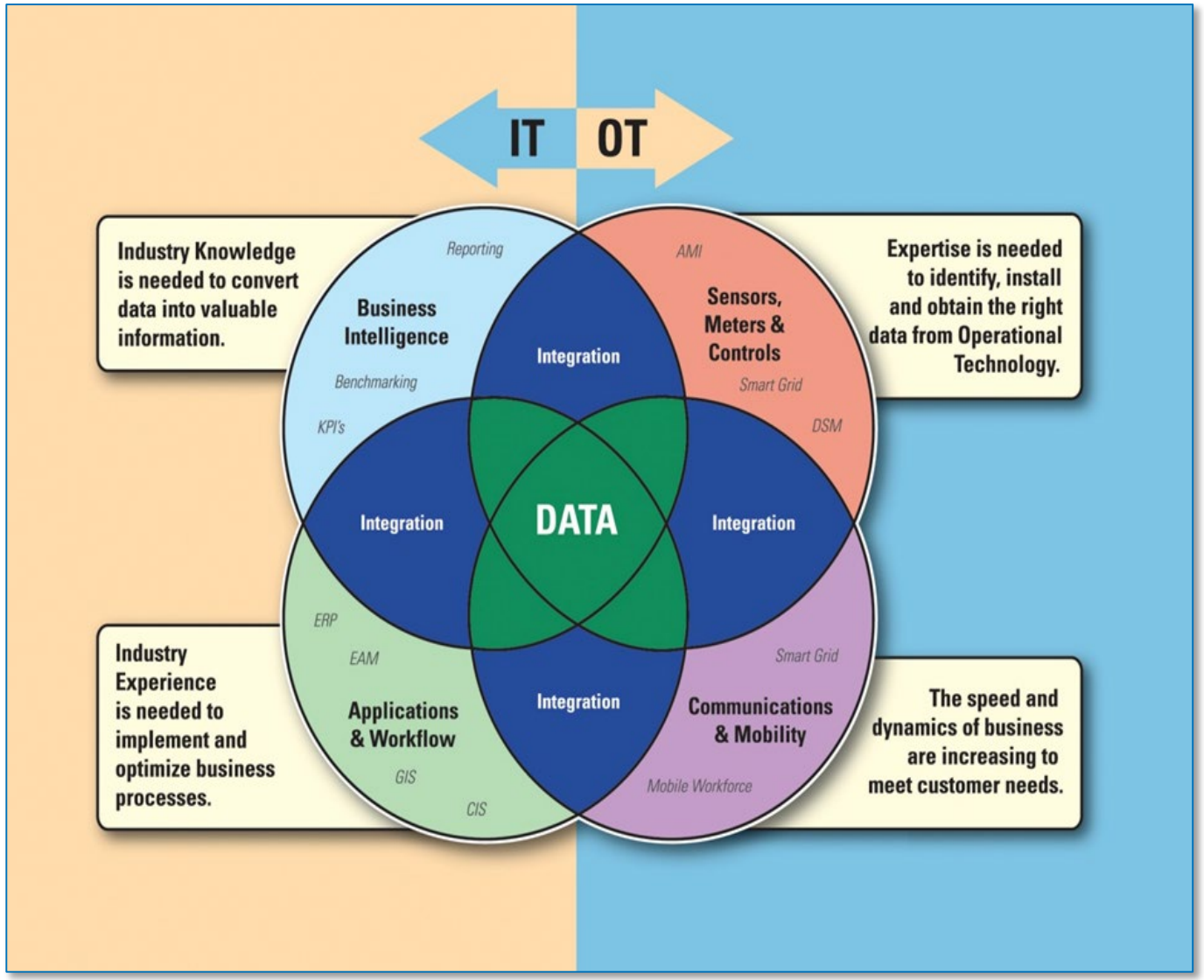


Until recently SCADA systems were isolated.

Newer control systems are exposing SCADA systems to the Internet.

Increasing numbers of customer owned solar Photovoltaic PV, electric vehicles and battery storage systems.

Information Technology (IT) vs. Operational Technology (OT)



- *Information Technology (IT) and Operational Technology (OT) systems face different threats*
- *Tools appropriate to use in IT environment may shut down or compromise OT assets*
- *Restoring compromised systems from backups poor fit for SCADA systems as SCADA controlled hardware cannot simply be restored*
- *Long complex passwords for mission critical system operators are a concern*

EnerNex
A CESI Company

Challenges for Electric Utilities

Excerpts from "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector," prepared by Idaho National Laboratory for the Office of Energy Policy and Systems Analysis (EPSA) in the U.S. Department of Energy

- Growth of networks and communication protocols used throughout control networks pose vulnerabilities that will continue to provide attack vectors that threat actors will seek to exploit for the foreseeable future. The interoperable technologies created for a shift toward a smart grid will continue to expand the cyber attack landscape.
- Threat actors on multiple fronts continue to seek to exploit cyber vulnerabilities in the U.S. electrical grid. Nation-states like Russia, China, and Iran and non-state actors, including foreign terrorist and hacktivist groups, pose varying threats to the power grid. A determined, well-funded, capable threat actor with the appropriate attack vector can succeed to varying levels depending on what defenses are in place.
- Utilities often lack full scope perspective of their cyber security posture. Total awareness of all vulnerabilities and threats at all times is improbable, but without enough cyber security staff and/or resources utilities often lack the capabilities to identify cyber assets and fully comprehend system and network architectures necessary for conducting cyber security assessments, monitoring, and upgrades…"

EnerNex

A CESI Company

TOPIC 2

CYBERSECURITY FRAMEWORKS

ASSESSING AND QUALIFYING RISK IN OPERATIONAL TECHNOLOGY ENVIRONMENTS

Cybersecurity Frameworks Examples

- *Many cybersecurity frameworks available and often confusing where to start*
  - Risk Frameworks
    - Identify, measure, and quantify risk
    - Example: *NIST SP800-30, SP800-37, SP800-39*
  - Cybersecurity Program Frameworks
    - Building a cybersecurity program
    - Measuring maturity of a cybersecurity program
    - Example: *NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF)*
    - Example: *DOE Electric Sector Cybersecurity Capabilities Maturity Model (ES-C2M2)*
  - Cybersecurity Control & Requirements Frameworks
    - Developing cybersecurity controls/requirements
    - Examples: *IEC-62443, NERC CIP, NISTIR 7628, NIST SP800-53, etc.*

Assessing Risk – Challenges in OT Environments

- *The classic IT view of risk is not a good fit for the OT environment*
- *Utilizing a methodology derived largely from IT practice can be expensive, invasive, and not necessarily cost-effective*
- *Most IT centric assessment methodologies tend to focus on identifying vulnerabilities and attack vectors*
- *Assessment methodologies in OT environments need to identify the operational, safety, and compliance impacts*
  - Helps to prioritize expenditures

Qualifying Risk - Example

Primary objective of a cyber assessment is to provide information necessary to manage identified risks.

Recommended approach is to base risk on:

- Safety Impacts
- Operational Impacts
- Compliance Impacts e.g.VSL (Violation Severity Level)

IMPACT LEVELS	SAFETY	OPERATIONS	COMPLIANCE
CRITICAL	Potential for Loss of Life or Injury	Destabilizing Event	NERC CIP Severe VSL
HIGH	Not defined	Loss of Load or Generation > 100MW	NERC CIP High VSL
MEDIUM	Not defined	Loss of Load or Generation < 100MW	NERC CIP Moderate VSL
LOW	Not defined	Loss of Load < 1MW	NERC CIP Lower VSL
		CATEGORIES	

EnerNex

A CESI Company

TOPIC 3

DEVELOPING OT CYBERSECURITY ARCHITECTURE AND REQUIREMENTS

Methodology – a Combination of Framework and Approach

- *Two Key Elements of a Good Systems Engineering Methodology*
  - Framework – High level architecture guidance and/or catalog of cybersecurity controls
  - Approach – How to apply the framework to your specific OT environment
- *Needs are similar whether addressing the cybersecurity posture of exiting deployed systems or developing architecture and requirements for new systems*

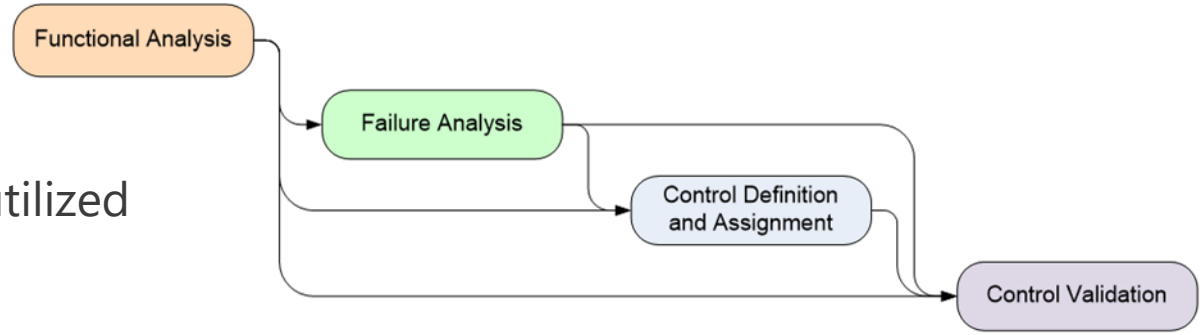
Utilize a Framework

- *Best to utilize a structured framework when defining cybersecurity controls/requirements for OT systems*
- *Lack of a structured methodology often results in gaps*
  - Many times cybersecurity controls/requirements defined ad hoc or brainstormed
    - Highly dependent on the available resources and experience
    - Not repeatable
  - Need to address a wide variety of cybersecurity topics
    - Example: NIST SP800-53 has 18 control families
  - Need to have a balance of preventative, detective, corrective cybersecurity controls/requirements

Select an Approach

- *Now that you have selected a framework, you need an approach to utilize it*
- *Focus is on selecting or developing cybersecurity controls/requirements*
- *One option is to utilize a particular framework's native approach*
- *Other methods can also be utilized based on available time and resources*
  - Top Down Approach
  - Bottom Up/Basic Approach

Top Down Approach



- *Based on:*
  - System functionality, architecture, technology utilized
- *May be resource intensive*
- *Mostly utilized when deploying new systems*
- *Vulnerability/Failure Analysis based on system functionality*
  - Possible attack vectors that may lead to identified failure modes
  - Vulnerabilities that may be exploited to carry out these attacks
- *Primary cybersecurity controls identified to address identified failure modes*
- *Example:* ***ASAP-SG Security Profiles***

Example: Smart Meter Data Flows

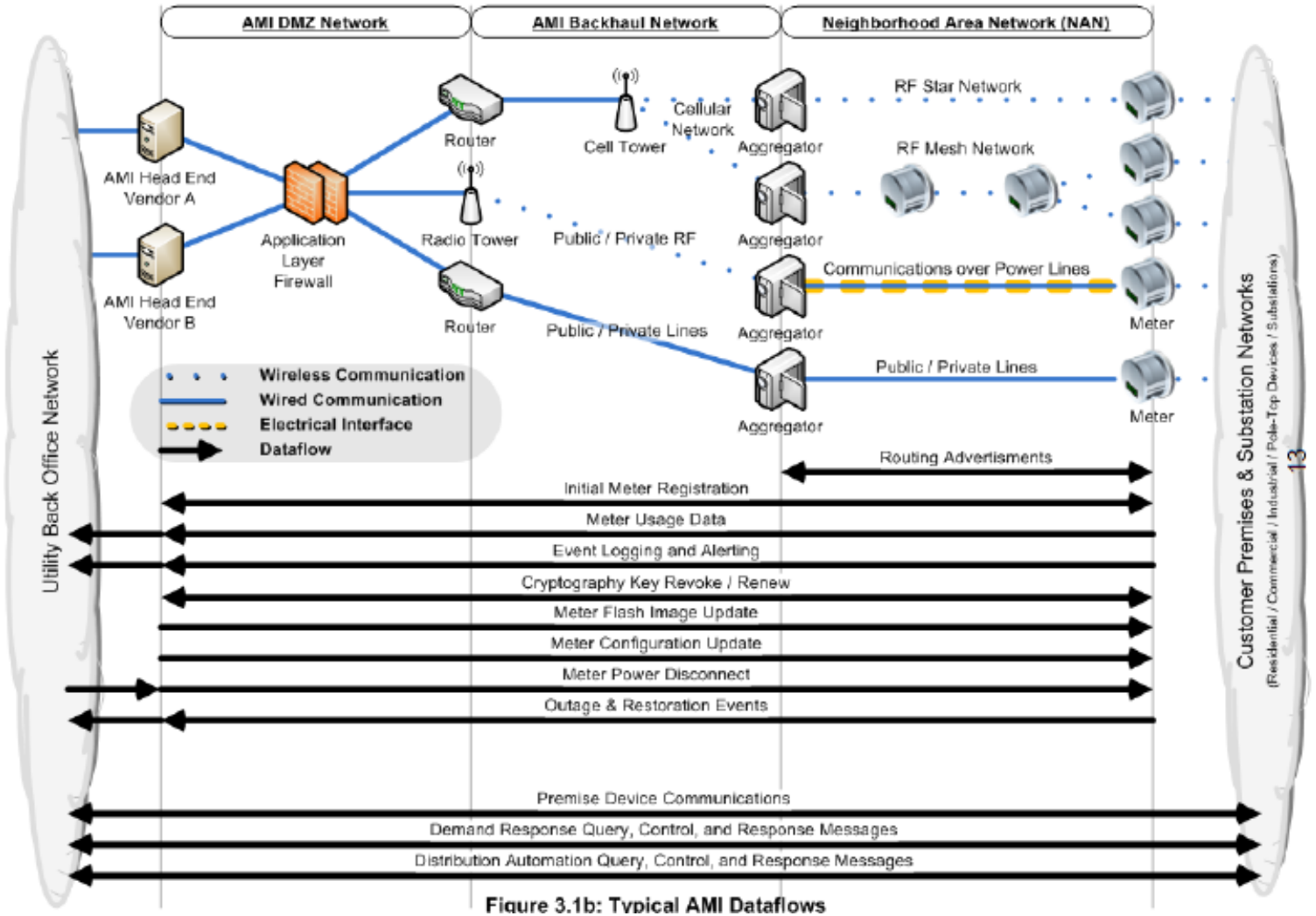


Figure 3.1b: Typical AMI Dataflows

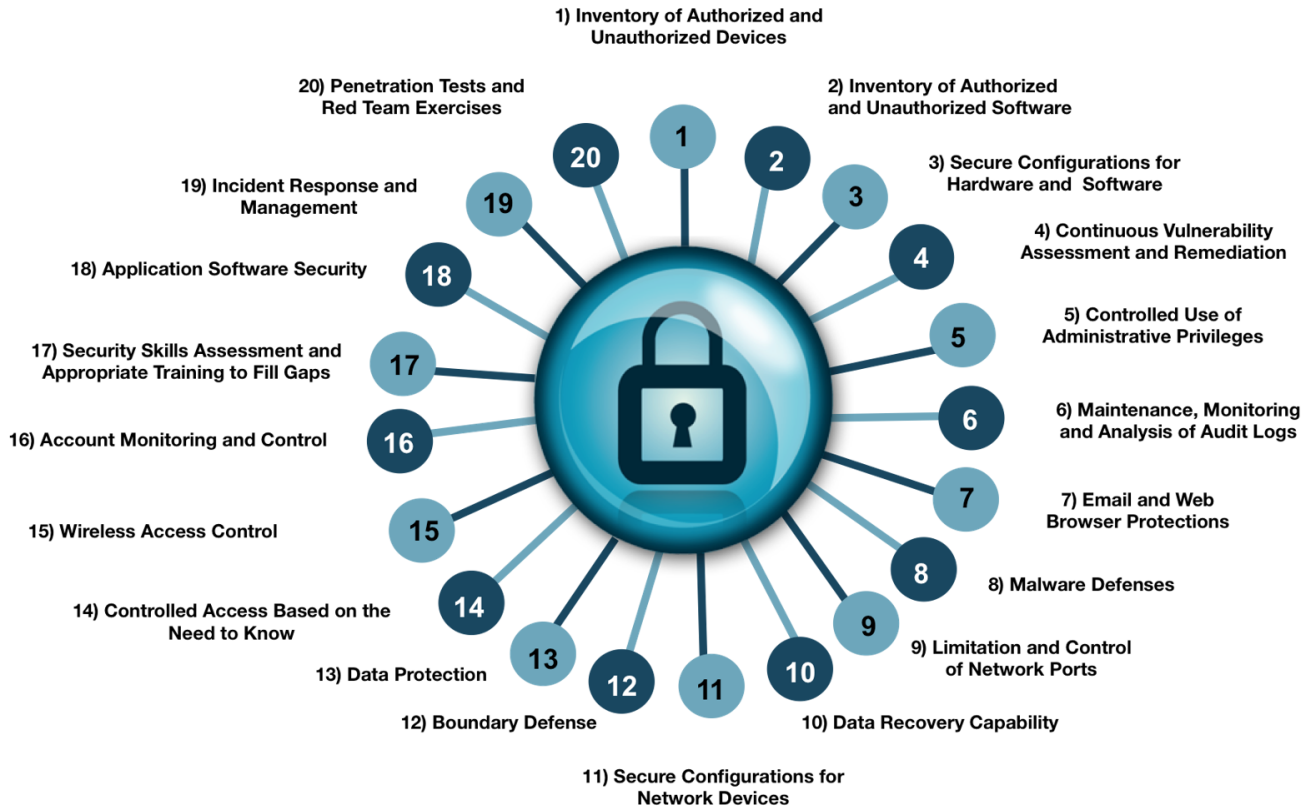
Source: NESCOR Guide to Penetration Testing for Electric Utilities, Version 3

Native Framework Approach

- *Some frameworks provide a native approach for selecting cybersecurity controls*
- *Easier on resources*
- *A superset of industry experience and expertise*
- *Typically will not map one-to-one to any particular system*
  - Some elements do not apply to your specific system
- *Cybersecurity controls/requirements determined by basic criteria/categorization*
- *Example:* ***NISTIR 7628 - Guidelines for Smart Grid Cyber Security***

Bottom Up Approach

- *Applies a standard set of cybersecurity controls/requirements to all systems*
- *Based on a set of known attack vectors*
- *Very little analysis of the underlying system*
- *Good starting point*
- *Easiest on resources*
- *Example:* ***The CIS Top 20 Critical Security Controls***



Cybersecurity Control/Requirement Tailoring

- *Regardless of framework and approach, some tailoring of the cybersecurity controls/requirements is often needed*
  - Most frameworks and catalogs of security controls are generic IT language
    - Need to customize to be specific to the OT environment (Underlying technology, functions, processes, etc.)
  - Most frameworks and catalogs of security controls are relative to the "system"
    - Need to be able to break things down to identify which components of the system that the security control/requirement applies
    - Especially important if the effort is supporting procurement
      - "System must be compliant to NERC CIP" is not a good requirement for a procurement specification

EnerNex
A CESI Company

TOPIC 4

VULNERABILITY ASSESSMENTS AND TESTING

Which Assessment Should You Use and When?

Type of Assessment	IT	OT/SCADA	Recommendations
Vulnerability Assessment	✓	✓	▪ Quarterly ▪ Must be cautious in Control/SCADA environment
Penetration Test	✓	✓	▪ Quarterly ▪ May interrupt Control/SCADA environment
Audit	✓	✓	▪ Annually
Risk Assessment	✓	✓	▪ Major environment changes
Threat Assessment	✓	✓	▪ Major environment changes
Red Team Assessment	✓	✓	▪ Annually ▪ May interrupt Control/SCADA environment
White/Grey/Black-box Assessment	✓	✓	▪ Annually ▪ May interrupt Control/SCADA environment
Application Security Assessment	✓	✓	▪ Major environment changes
PCI Assessment	✓		▪ Annually ▪ Limited to credit/debit card processing systems
HIPAA Assessment	✓		▪ Annually ▪ Limited to healthcare/HR processing systems
SoX Assessment	✓		▪ Annually ▪ Limited to financial data processing systems
NERC CIP		✓	▪ As required ▪ Limited to Control/SCADA environment

Level of Risk of Potential Impact to Environment

✓ Low

✓ Medium

✓ High

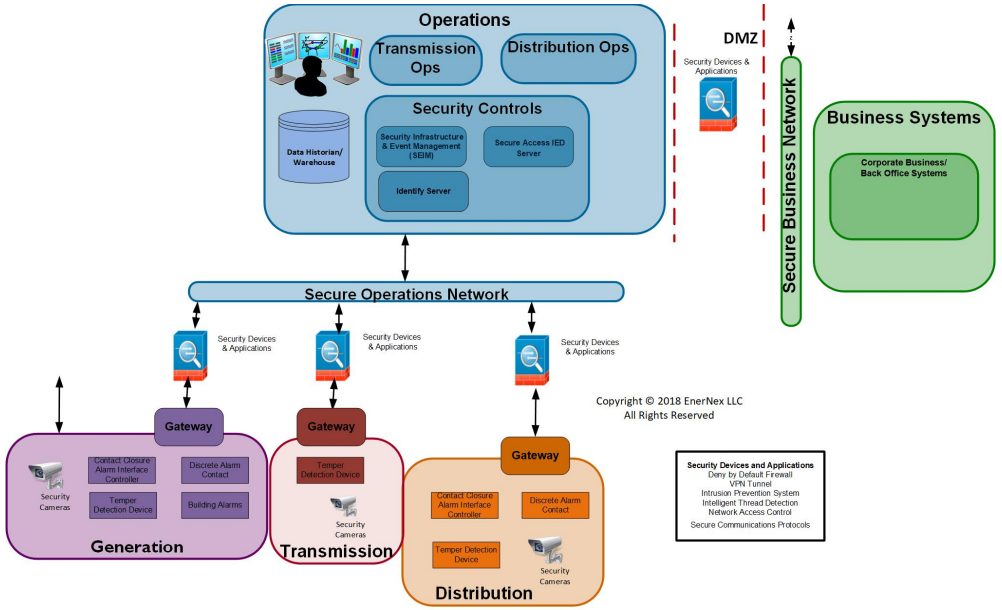
EnerNex
A CESI Company

Requirements Review

- *Document North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements*
- *Determine if requirements are defined relative to system functionality and aligned with the organization's security goals and objectives*
- *Determine if requirements are mapped to specific solutions deployed to meet requirements*
- *Map cybersecurity requirements to systems*
- *Include cybersecurity requirements in all procurement specifications and RFPs*
- *Identify potential gaps*
  - Incomplete or missing requirements
  - Controls (verification methods) not present, weak, untestable, etc.

Architecture Review

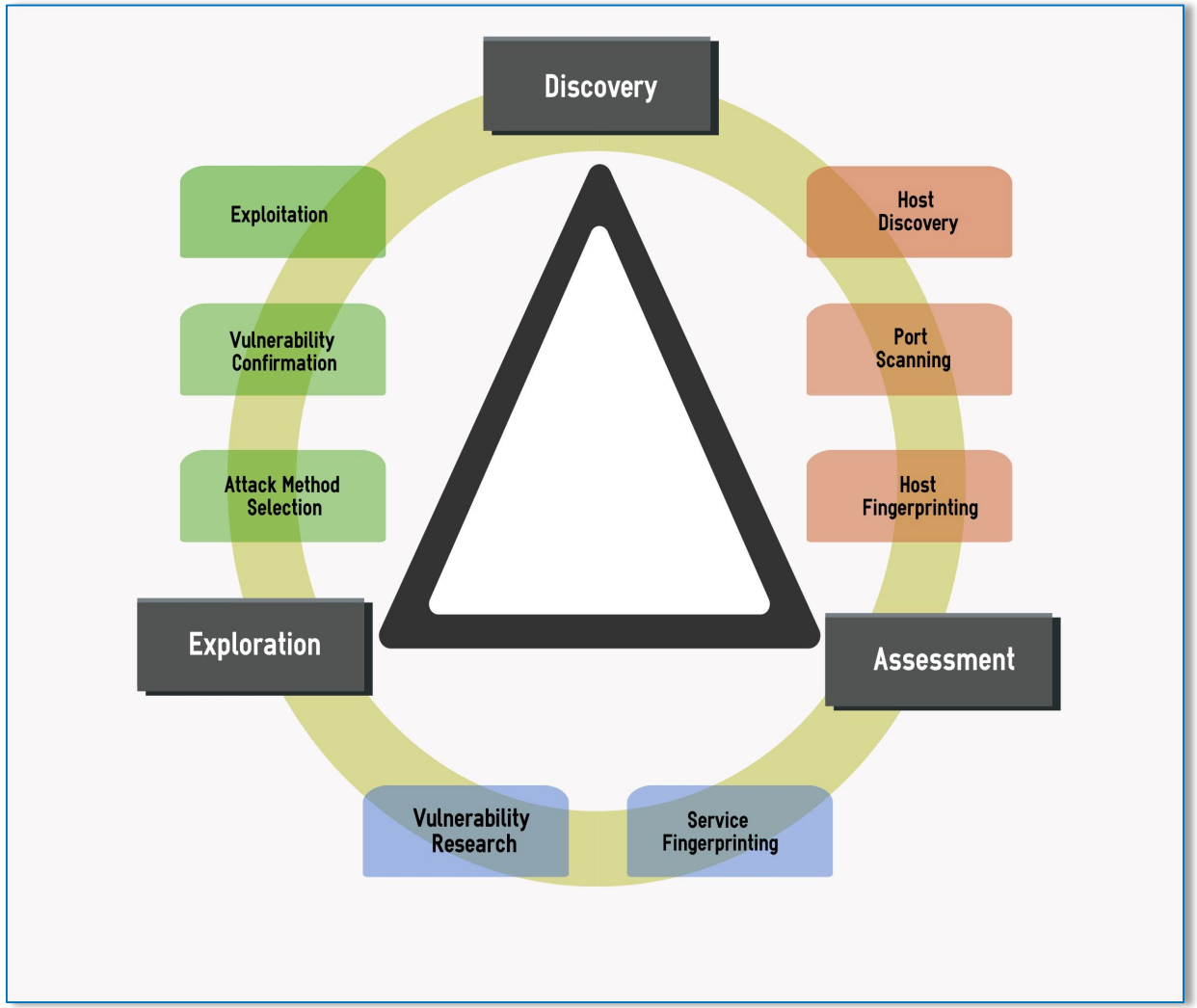
- *Network architecture review evaluates the function and placement of network components*
  - Security perimeters, segregation, and separation
  - Access points
  - Information flows
  - Dependencies
  - Resiliency



- *Can be used to help drive common cyber enterprise architecture*
  - Ideally assists with acquiring stakeholder support across IT and operational groups

Overview of Security Penetration Test

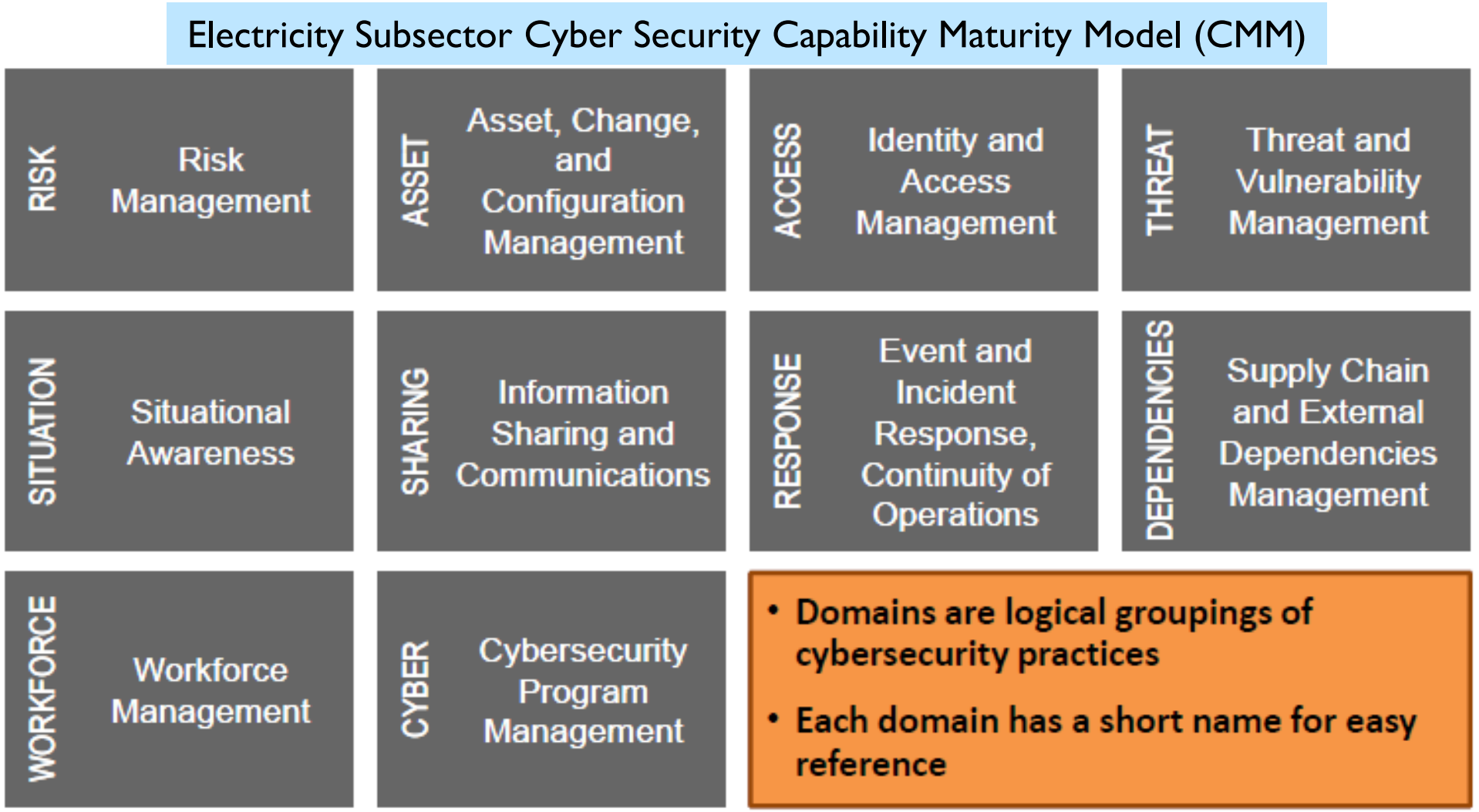
- *Many ways to perform a pen test depending on scope and environment*



Cyber testing focuses on system and component communications interfaces.

In addition to penetration testing, testing is typically performed to assess insider threats including users with elevated access levels.

DOE Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)



Goal of an assessment is to assess an organization's security posture and preparedness to deal with cyber attacks and breaches.

Like other CMMs, workshops and questionnaires are used to score organization's maturity level.

EnerNex
A CESI Company

North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)

NERC CIP requirements designed to secure North America's bulk electric system (BES)

CIP-002-5.1a	Cyber Security - BES Cyber System Categorization
CIP-003-6	Cyber Security - Security Management Controls
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security - Information Protection
CIP-013-1	Cyber Security - Supply Chain Risk Management
CIP-014-2	Physical Security

Recommended System Engineering Approach

Document & map each NERC CIP requirement to:

- Applicable systems
- Acceptable evidence types (measures)
- Responsible organizations
- Responsible persons with contact information
- Title of evidence
- Location of evidence
- Link to evidence

EnerNex

A CESI Company

TOPIC 5

EXAMPLE

Example: Systems Engineering Approach to Security from National Renewable Energy Resources Lab (NREL)

NREL System Engineering Cyber Security Activities

1. Identify
2. Protect
3. Monitor
4. Respond
5. Recover

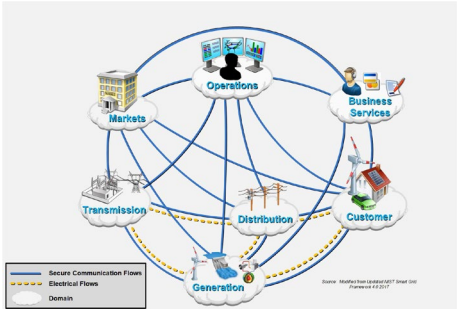
NREL 10 Step System Engineering Cyber Security Approach

- Assess cyber-governance (security controls in place, prioritized action items for gaps in security controls) (identify and protect)
- Implement technical plan to address gaps from cyber-governance assessment (protect)
- Perform due diligence on cutting-edge cybersecurity technologies for energy systems, including functional and integration testing (identify and protect)
- Develop procurement language for secure, reliable, and resilient SCADA systems (protect)
- Review SCADA cybersecurity architecture and benchmark against NREL's nine-layer cybersecurity model, including vulnerability assessment and risk mitigation (identify, protect, monitor, and respond)
- Scan software code and binary executables to identify malware and cyber risks as well as techniques for mitigation (identify and protect)
- Test data fuzz of SCADA systems with risk mitigations (identify and protect)
- Pen-test SCADA systems to identify residual cyber risks and provide mitigations (monitor, respond, and recover)
- Develop and analyze failure scenarios with mitigations (recover)
- Provide training on cybersecurity awareness for corporate staff and information technology/operation technology audiences to reduce cyber risks from social engineering and phishing schemes from advanced persistent threats (all)

Source: https://www.nrel.gov/esif/cybersecurity-resilience-10-step.html

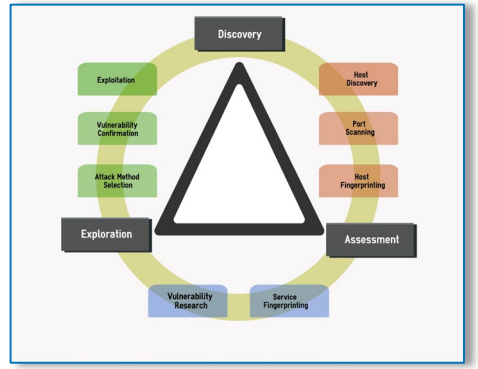
Summary

- *Improve cybersecurity using system engineering techniques*
  - Requirements
    - Ensure cybersecurity requirements e.g. NERC CIP are documented
    - Include consistent cybersecurity requirements in all RFPs
    - Develop cybersecurity use cases
  - Enterprise Architecture
    - Use standard electric grid industry reference architectures e.g. NIST
    - Coordinate IT and OT architectures into integrated enterprise architecture
    - Recognize IT and OT cyber systems face differ threats and need different cybersecurity solutions
  - Actively test cybersecurity requirements
  - Vulnerability/threat/failure analyses
    - Leverage requirements, enterprise architecture and testing artifacts



IMPACT LEVELS				
CRITICAL	Potential for Loss of Life or Injury	Destabilizing Event	NERC CIP Severe VSL
HIGH	Not defined	Loss of Load or Generation > 100MW	NERC CIP High VSL
MEDIUM	Not defined	Loss of Load or Generation < 100MW	NERC CIP Moderate VSL
LOW	Not defined	Loss of Load < 1MW	NERC CIP Lower VSL
	SAFETY	OPERATIONS	COMPLIANCE
		CATEGORIES	

EXAMPLE



Q&A

At this time, please submit your questions for the presenters in the chat box.

The slides from today, along with on-demand access to this presentation, will be emailed within 24 hours of the close of this webinar.

Contact Information

Kay Stefferud

Director of Implementation Services

kay@enernex.com

Brian Smith

Principal Consultant

bsmith@enernex.com

THANK YOU!

Connect with Us

enernex.com

cesi.it

EnerNex
A CESI Company