SYSTEM ENGINEERING APPROACHES TO ADDRESS CYBERSECURITY CHALLENGES OF THE ELECTRIC GRID

2018 INCOSE San Diego Mini-Conference

December 1, 2018

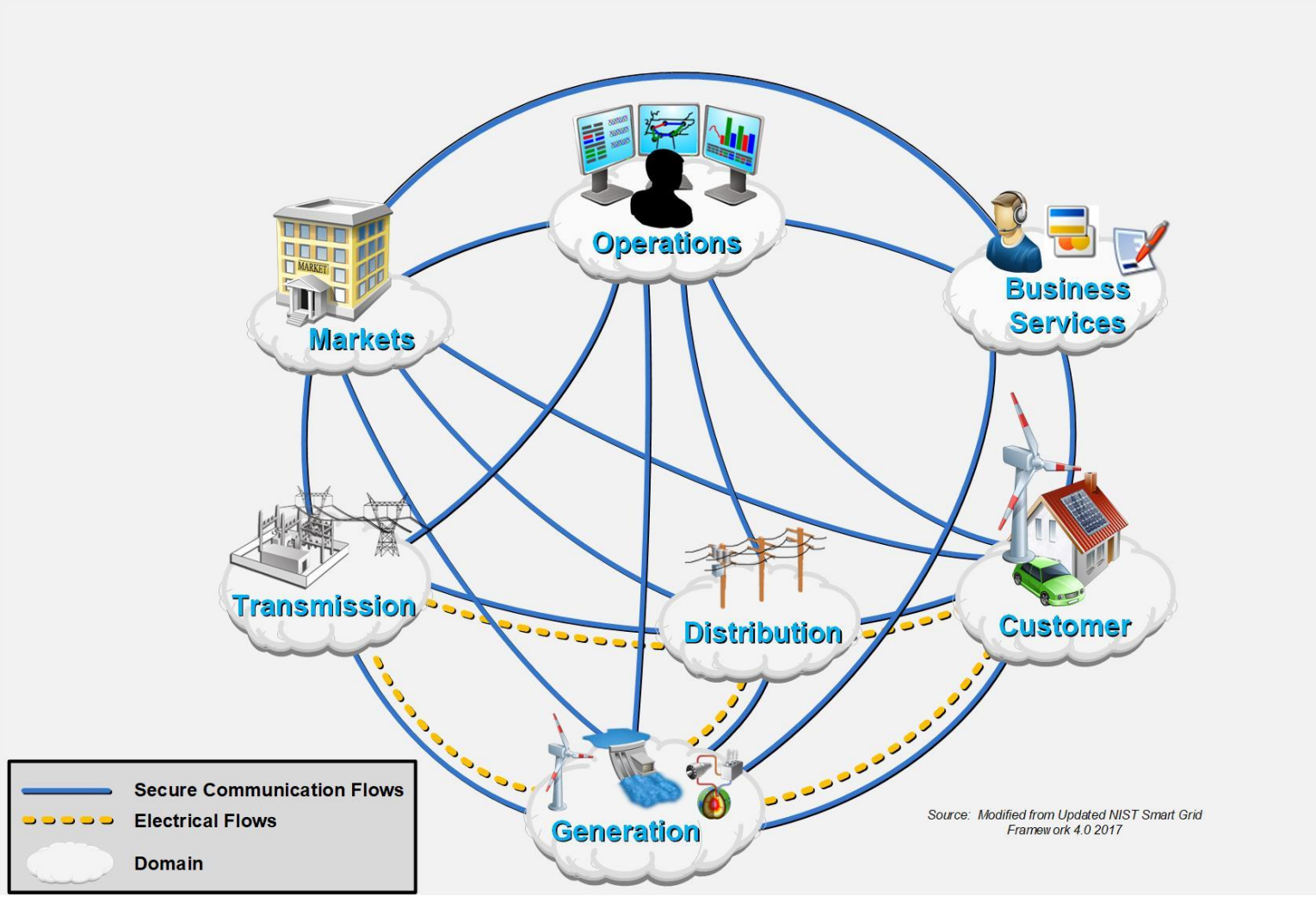
AGENDA

- Topic 1: Introduction to Electric Grid Systems of Systems
- Topic 2: Electric Grid Cyber Security Threats
- Topic 3 Solutions: Cyber Vulnerability Assessment Methodologies
- Topic 4 Solutions: Using Security Assessment & Testing Tools
- Topic 5 Solutions: Examples

Topic I

INTRODUCTION TO ELECTRIC GRID SYSTEM OF SYSTEMS

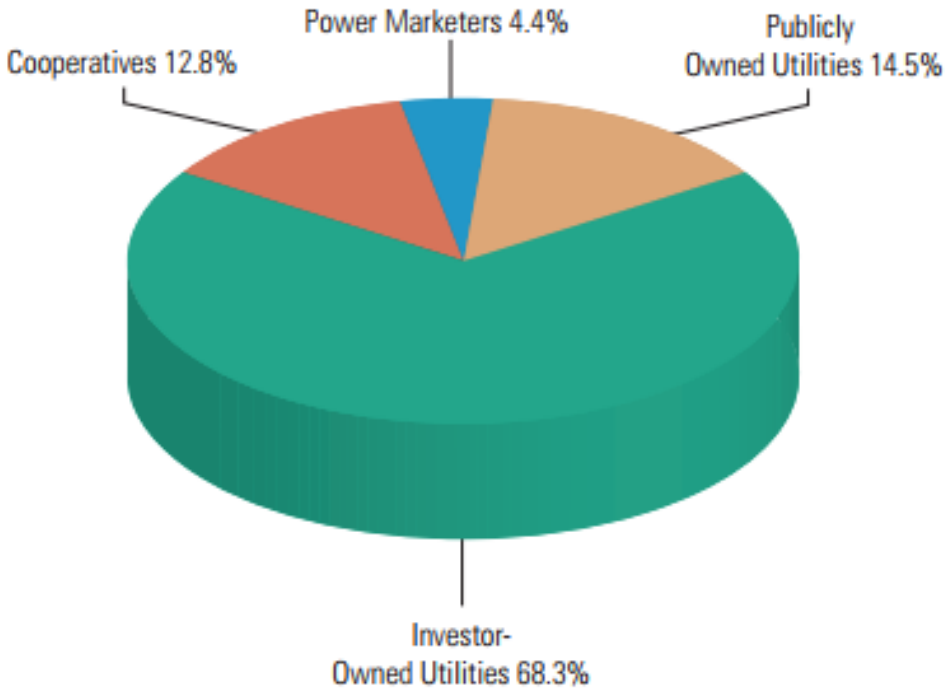
ELECTRIC GRID SYSTEM OF SYSTEMS



EnerNex
A CESI Company

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)



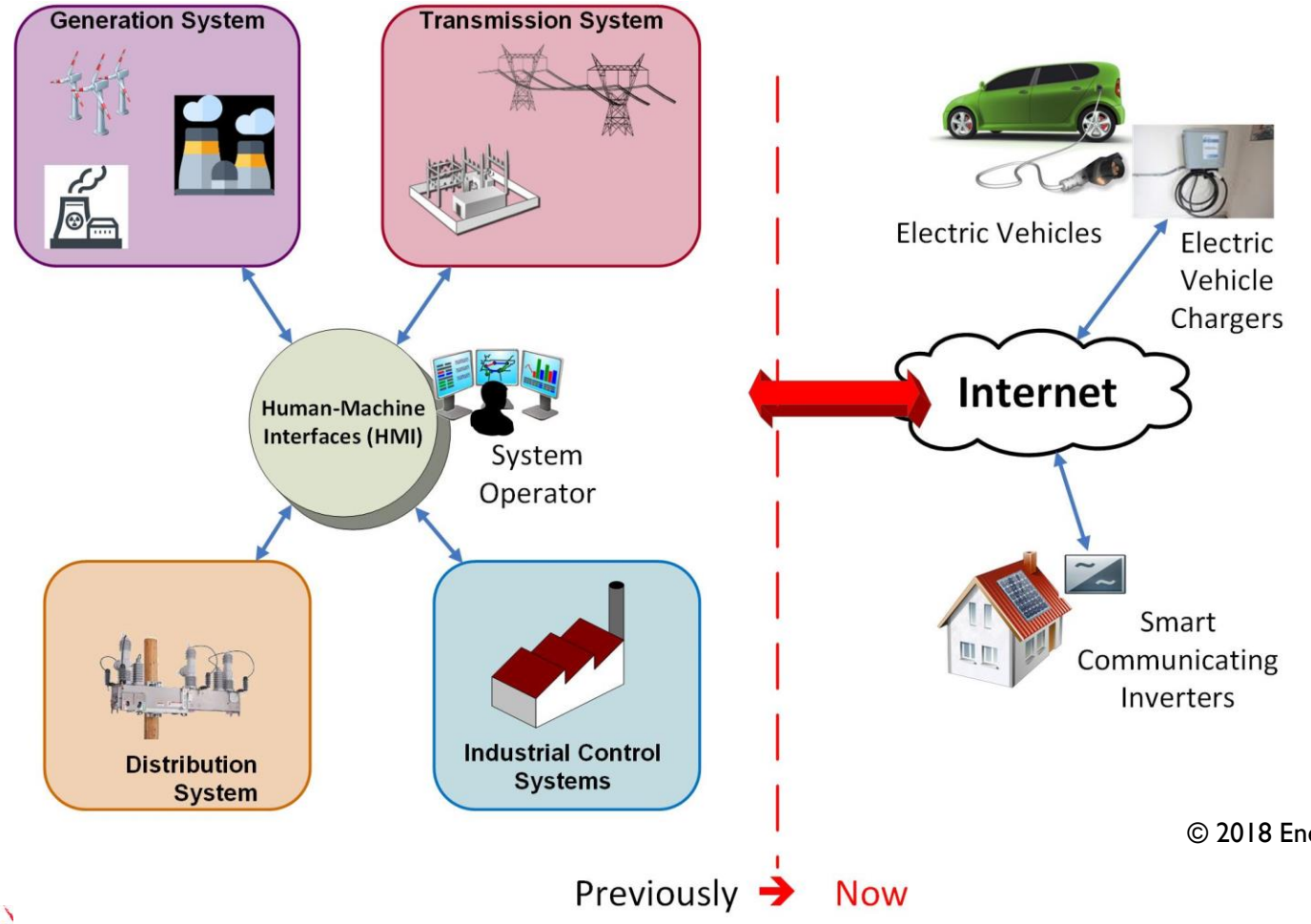
148 million electric customers in the US

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.

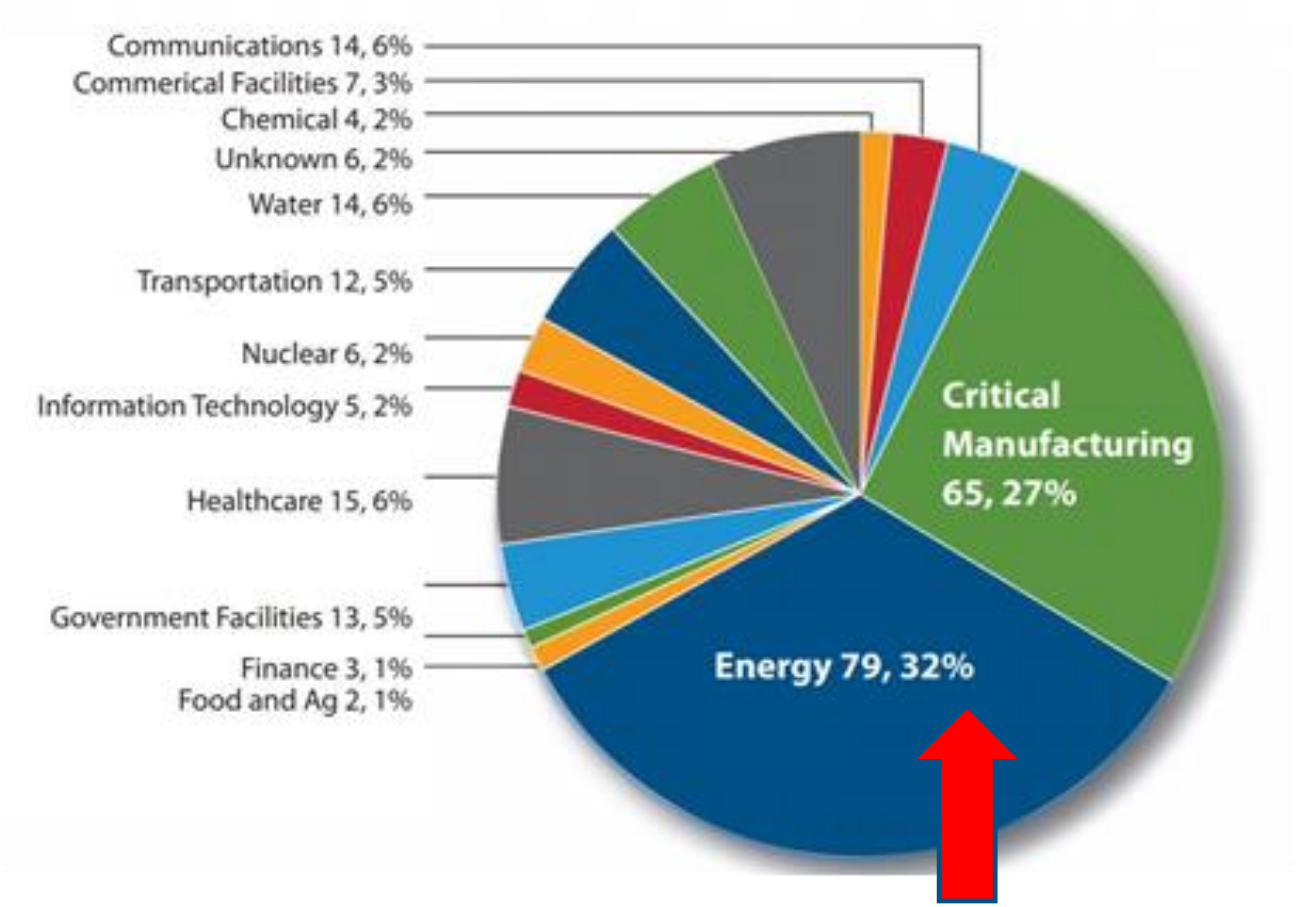
Increasing numbers of customer owned solar Photovoltaic PV, electric vehicles and battery storage systems

Topic 2

ELECTRIC GRID CYBER SECURITY THREATS

CRITICAL INFRASTRUCTURE INCIDENTS PER INDUSTRY

Threats



- In 2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received and responded to 245 incidents reported by asset owners and industry partners.

https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

WHAT WE ARE SEEING - PURPOSE OF ATTACKS

All industries and critical infrastructure assets including electric utilities are under varying levels of attacks.

Many cyber attacks on the electric utilities have an end game:

- Efforts are traditionally intentional, prolonged system probing and data gathering attacks against specific targets with specified intent.
- Advanced Persistent Threats (APT's), usually include unauthorized stealth reconnaissance, data gathering and vulnerability analysis of infrastructure, assets, networks, SCADA systems, data and personal information.
- Intelligence data gathered used to develop more pervasive methods to map out the infrastructure, dig deeper and harvest greater amounts of intelligence.
- At some point, the intelligence is leveraged to better understand how the target operates enabling the initial sponsor to launch clear, specific and focused attacks usually with malicious intent.
- Most attacks are to gain information and data, not to shut down the grid.

High Profile Cyber Attacks

- Stuxnet SCADA Iran nuclear centrifuges
- 2015 Ukraine power grid
- May 2018 US imposed sanctions against Russia for energy, nuclear and critical manufacturing cyber attacks*
- Ransomware, locks all files until cryptocurrency payment made

*Source: https://www.cnn.com/2018/03/15/politics/dhs-fbi-russia-power-grid/index.html

WHAT WE ARE SEEING - MOTIVATION AND JUSTIFICATION

- Many reasons to attack energy resources
  - Control over their own resources and citizens
  - Intellectual property theft, exploitation and disruption
  - High impact events
  - Economic
    - Cheaper to steal than to research or build
    - Profit from selling information
  - Identification of applications, configuration or attack responses
  - Redirects to other nefarious resources for more advanced exploits

- Threat Sources
  - Nation States
  - Intelligence Agencies
  - "Hacktivists"
  - Organized Crime
  - Terrorists
  - Corporate Insiders

WHAT WE ARE SEEING - PROCESS AND METHODS USED

Many ways to attack an electric grid

- Social engineering against soft targets, people and automated processes
- Viruses, malware, trojan horses, worms, key loggers, network sniffers
- Redirects from legitimate websites or unsuspecting personnel
- Calls to helpdesk or key people pretending to be support
- Social media websites
- Targeted email scams
- System compromises
- Compromised OS or platforms
- Fake or hijacked web sites
- Compromised attachments (Word, PDF, spreadsheets)
- Physical methods such as site/personnel observations, cameras and dumpster diving

Some common attack delivery methods include phishing, introducing infected removable media, exploiting human error, introducing malware through network communication paths, and using web-based watering hole attacks.

VULNERABILITIES 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…"

COMMON SECURITY BARRIERS FOR ELECTRIC GRID ORGANIZATIONS

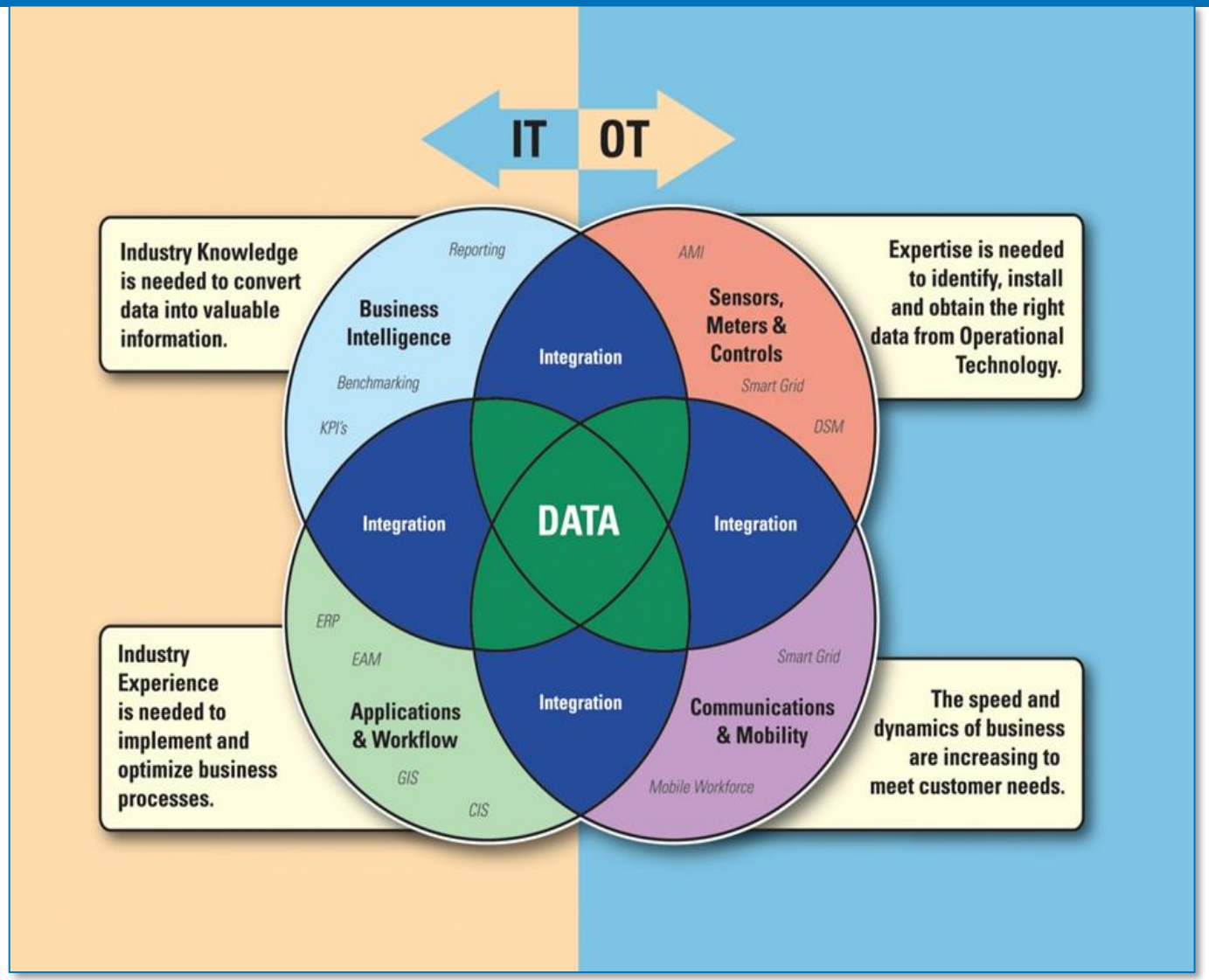
Risks or threats that may impact the implementation of risk management practices:

- Under staffed security and operational departments
- Inadequate policies, procedures and culture governing security
- Inadequately designed systems and networks lack defense-in-depth
- Remote access without appropriate access control
- System administration mechanisms and software not adequately scrutinized, monitored or maintained
- Inadequately secured wireless communications
- Non-dedicated communication channels
- Insufficient use of tools to detect and report suspicious activities
- Unauthorized or inappropriate applications/devices on networks
- Control systems data not authenticated
- Inadequately managed, designed or implemented critical support infrastructure

Section 3

SOLUTIONS: *CYBER VULNERABILITY ASSESSMENT METHODOLOGIES*

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 missions critical system operators are a concern

MAJOR CYBER ASSESSMENT ACTIVITIES

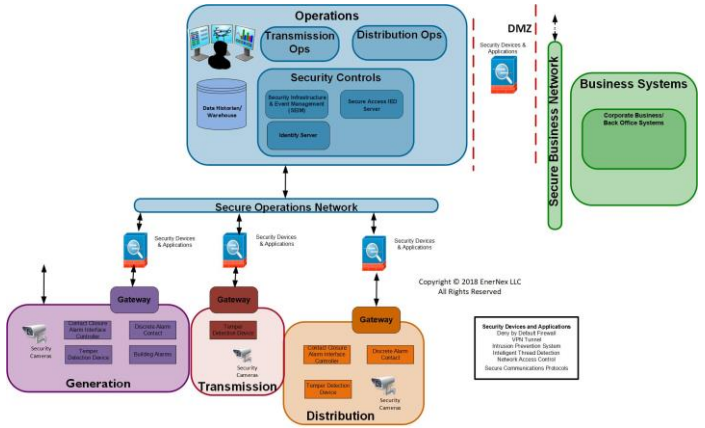
Activity	Device Assessment	System Assessment	
		Top Down	Bottom Up
Scoping/Planning	✓	✓	✓
Requirements Review		✓	
Architecture Review		✓	(optional)
Configuration & Log Review	✓	✓	✓
Physical Review	✓	✓	✓
Policy and Procedure Review		✓	✓
SME Interviews		✓	✓
Vulnerability/Failure Analysis	✓	(optional)	✓
Active Testing	✓	(optional)	✓
Hardware/Software Review	✓		

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 cyber security requirements to systems
- Include cyber security 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

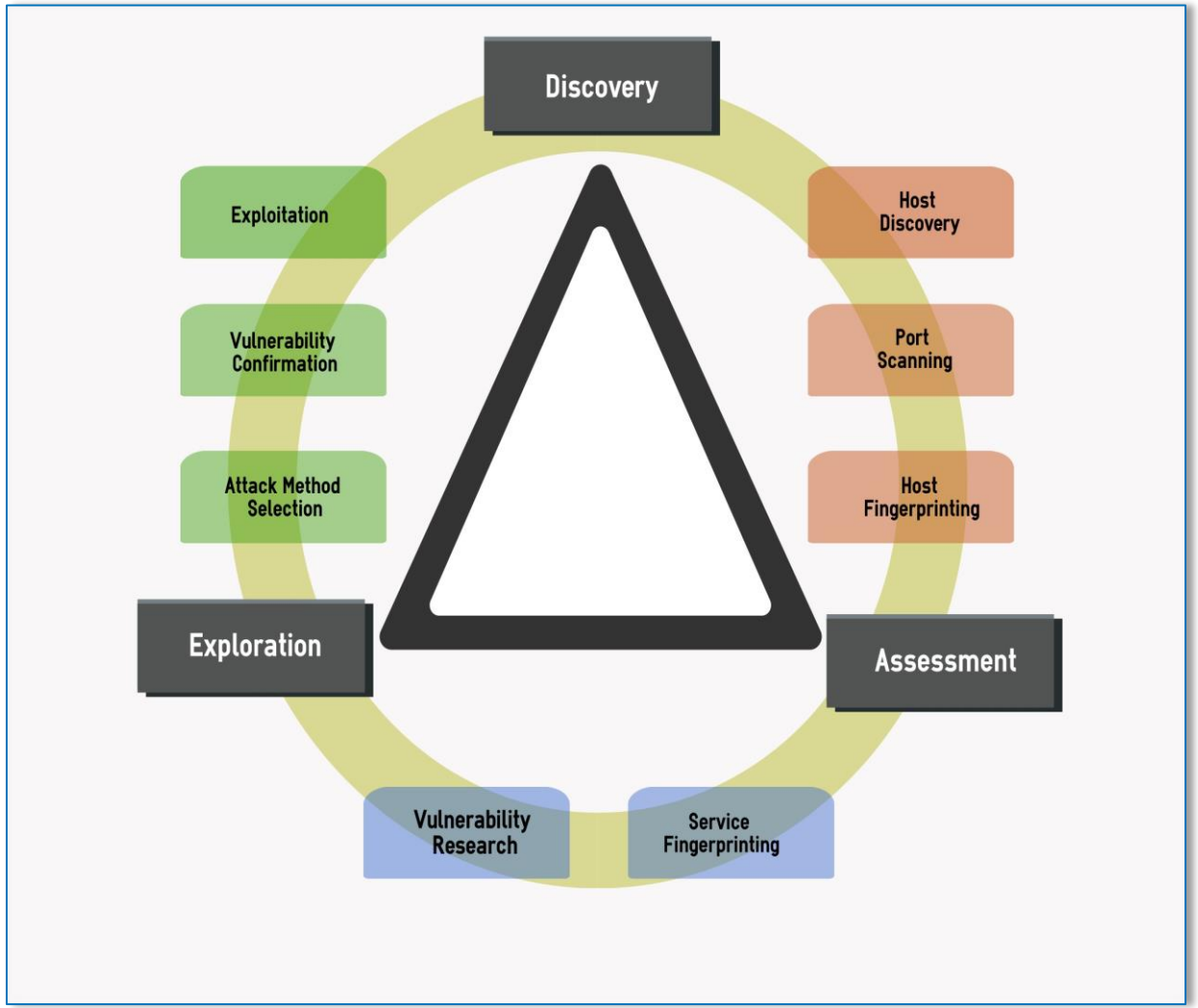


VULNERABILITY/FAILURE ANALYSIS

- Based on:
  - System functionality
  - System architecture
  - Technology utilized
- Identify possible failure modes/scenarios
- Identify possible attack vectors that may lead to identified failure modes
- Identify vulnerabilities that may be exploited to carry out these attacks
- Potentially develop cyber attack use cases

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.

QUALIFYING RISK

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	

Section 4

SOLUTIONS: *USING SECURITY ASSESSMENT & TESTING TOOLS*

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

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION (NERC) CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Solutions

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

DOE ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Solutions

Electricity Subsector Cyber Security Capability Maturity Model (CMM)

RISK Risk Management	ASSET Asset, Change, and Configuration Management	ACCESS Identity and Access Management	THREAT Threat and Vulnerability Management
SITUATION Situational Awareness	SHARING Information Sharing and Communications	RESPONSE Event and Incident Response, Continuity of Operations	DEPENDENCIES Supply Chain and External Dependencies Management
WORKFORCE Workforce Management	CYBER Cybersecurity Program Management	• Domains are logical groupings of cybersecurity practices • Each domain has a short name for easy reference	

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

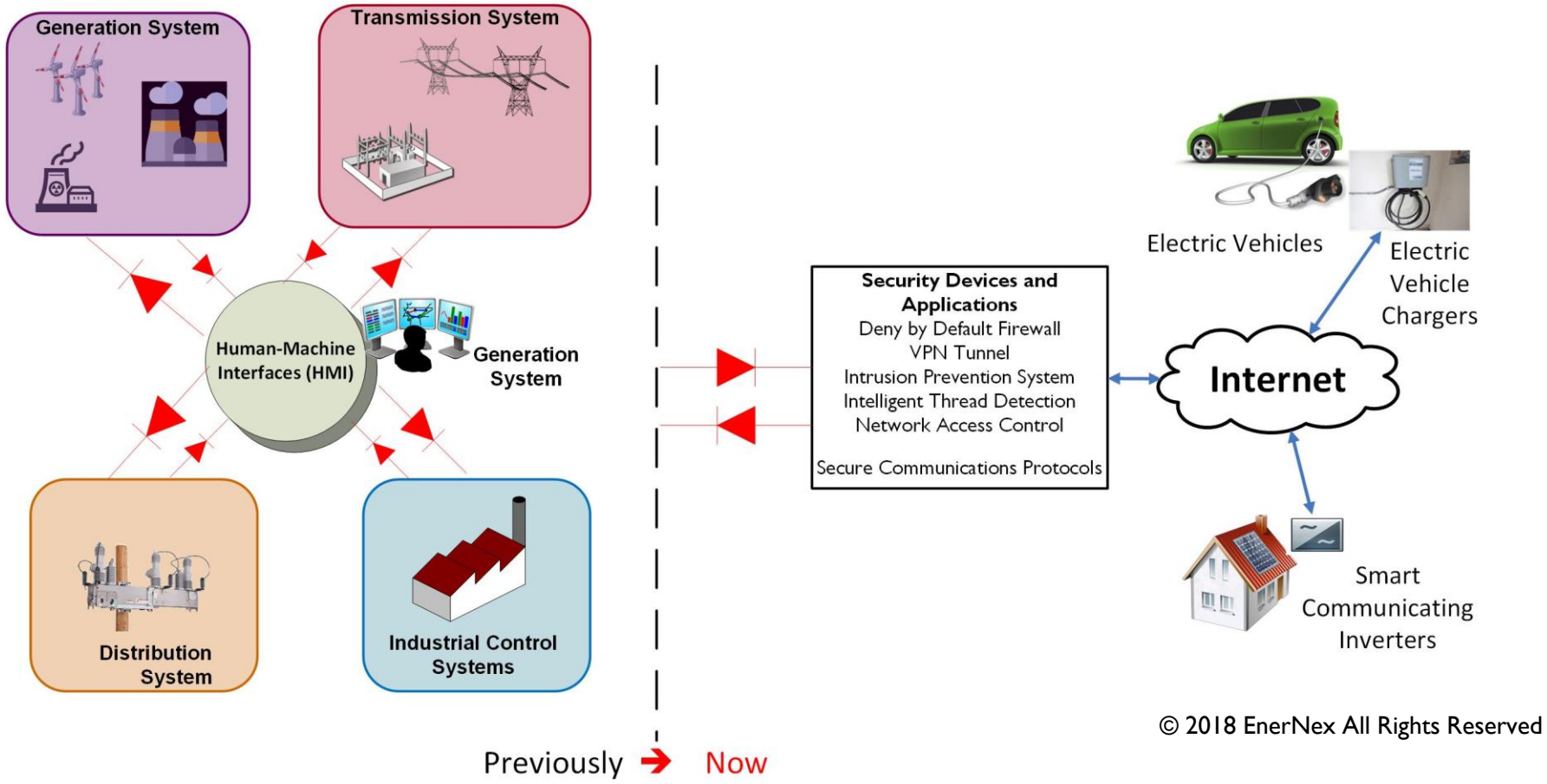
Like other CMMs, workshops and questionnaires are used to score organization's maturity level.

EnerNex
A CESI Company

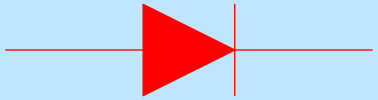
Topic 5

SOLUTIONS: *EXAMPLES*

SCADA CONTROL SYSTEMS CYBER SECURITY ARCHITECTURE



To protect SCADA systems use data diodes.



Data diode hardware physically allows data to travel in only one direction.

Stronger solution than firewalls.

EXAMPLE: SYSTEMS ENGINEERING APPROACH TO SECURITY FROM NATIONAL RENEWABLE ENERGY RESOURCES LAB (NREL)

Solutions

NREL System Engineering Cyber Security Activities

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

NREL 10 Step System Engineering Cyber Security Approach

1. Assess cyber-governance (security controls in place, prioritized action items for gaps in security controls) **(identify and protect)**
2. Implement technical plan to address gaps from cyber-governance assessment **(protect)**
3. Perform due diligence on cutting-edge cybersecurity technologies for energy systems, including functional and integration testing **(identify and protect)**
4. Develop procurement language for secure, reliable, and resilient SCADA systems **(protect)**
5. Review SCADA cybersecurity architecture and benchmark against NREL's nine-layer cybersecurity model, including vulnerability assessment and risk mitigation (identify, protect, monitor, and respond)
6. Scan software code and binary executables to identify malware and cyber risks as well as techniques for mitigation **(identify and protect)**
7. Test data fuzz of SCADA systems with risk mitigations **(identify and protect)**
8. Pen-test SCADA systems to identify residual cyber risks and provide mitigations **(monitor, respond, and recover)**
9. Develop and analyze failure scenarios with mitigations **(recover)**
10. 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

EXAMPLE: SECURITY PENETRATION TEST PREPARATION

- In the IT/OT networks
  - Harden the network first
  - Perform patching, hardening and critical tasks before pen test to avoid taking down the system(s).
  - Vulnerability assessment is a full evaluation of the current system state typically performed using commercial software that scans the system for both internal and external security issues.
  - Implement remediation findings from the vulnerability assessment.
  - Prepare for penetration testing by reviewing remediation work performed
  - Perform penetration testing using whatever types of tools, attacks or breach techniques that are needed to defeat the now upgraded security.

SMART METER DATA FLOW FOR PENETRATION TESTING

Solutions

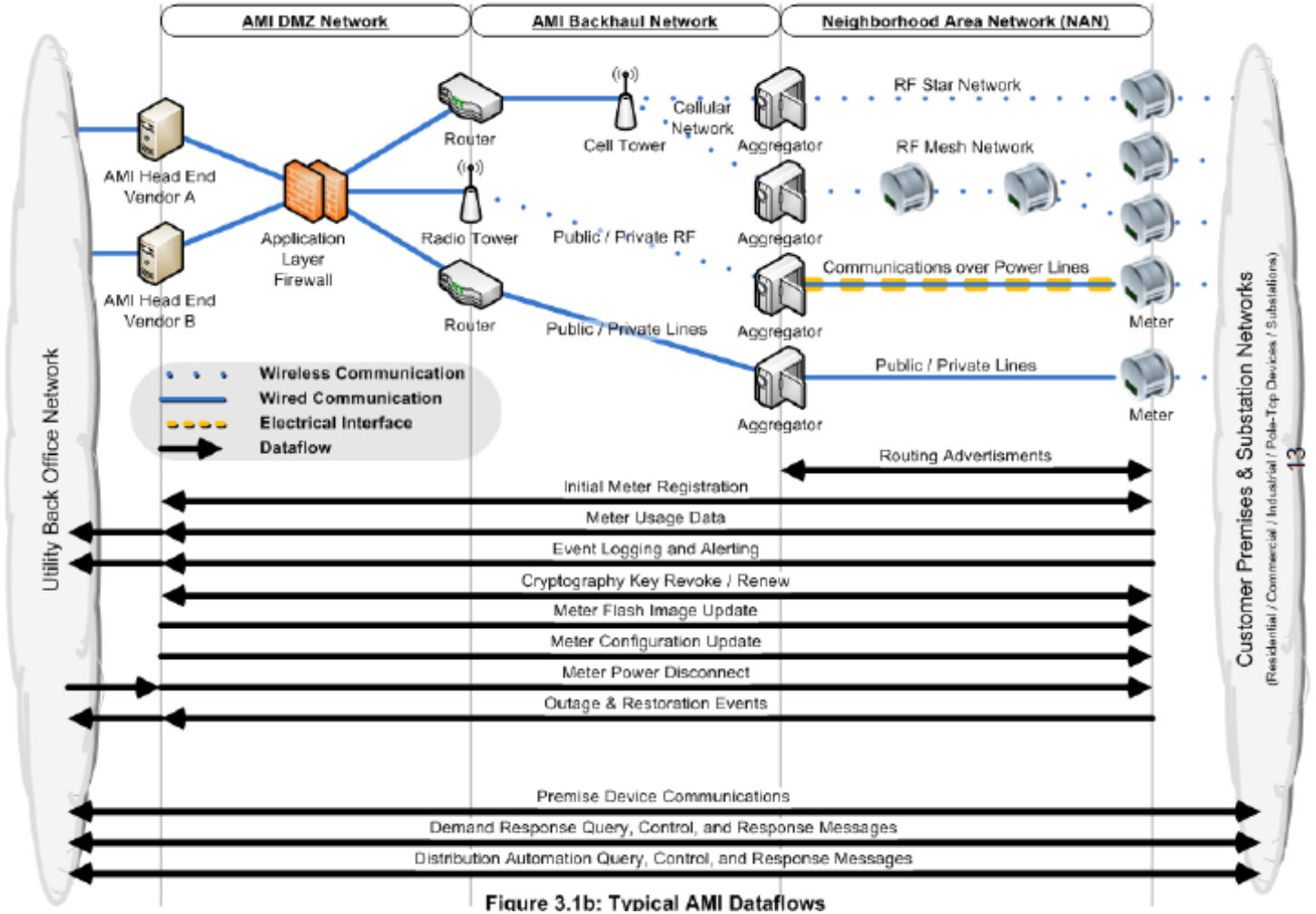
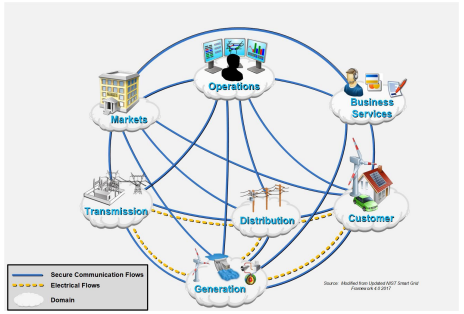


Figure 3.1b: Typical AMI Dataflows

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

SUMMARY

- Improve cyber security using system engineering techniques
  - Requirements
    - Ensure cyber security requirements e.g. NERC CIP are documented
    - Include consistent cyber security requirements in all RFPs
    - Develop cyber security 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 cyber security solutions
  - Actively test cyber security requirements
  - Vulnerability/threat/failure analyses
    - Leverage requirements, enterprise architecture and testing artifacts

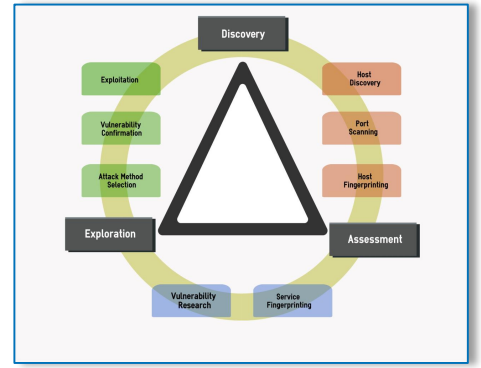


IMPACT LEVELS

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



EnerNex
A CESI Company

CONTACT INFORMATION

Kay Stefferud

Director of Implementation Projects

EnerNex, a CESI Company

http://www.enernex.com/

kay@enernex.com