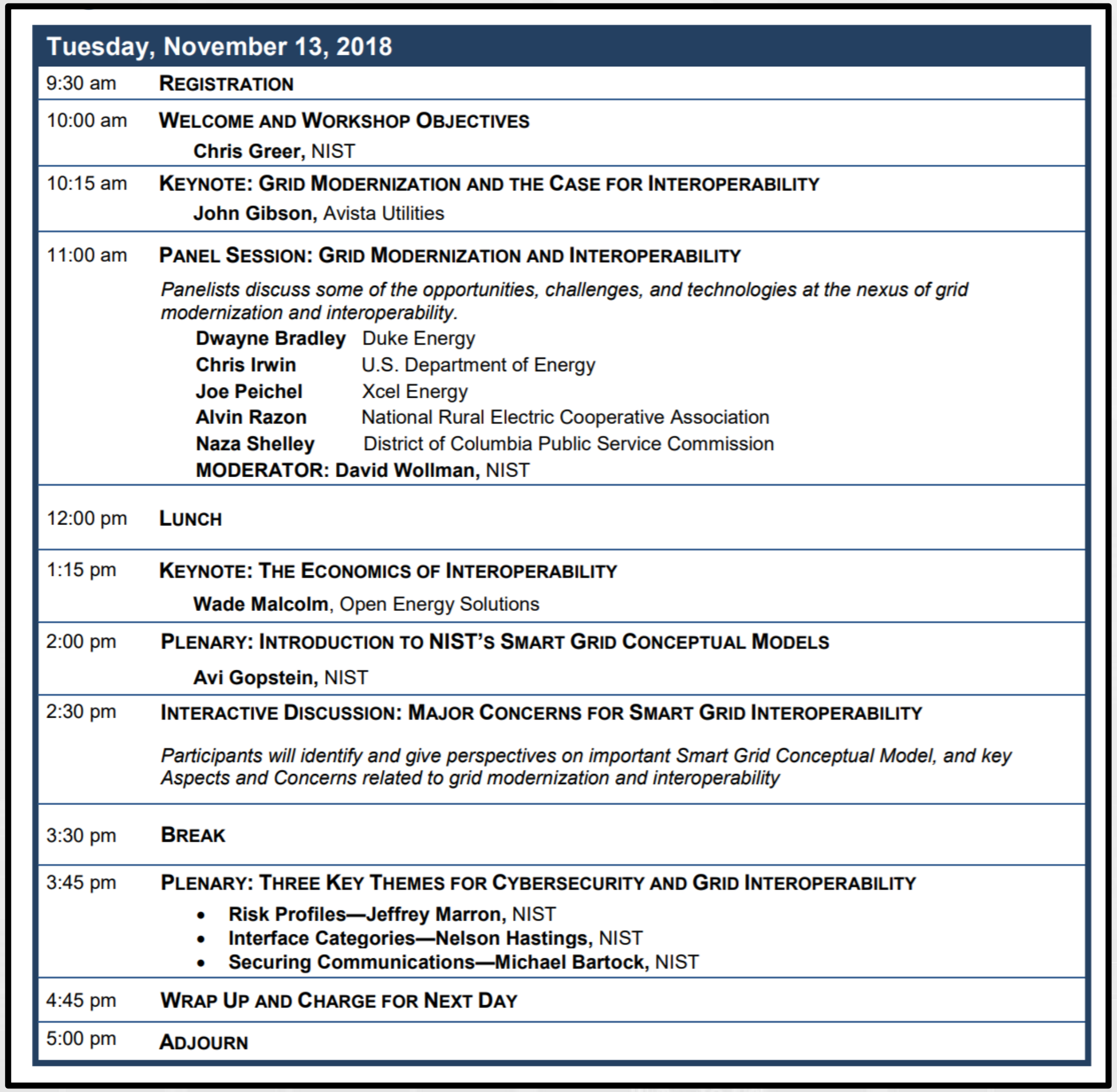
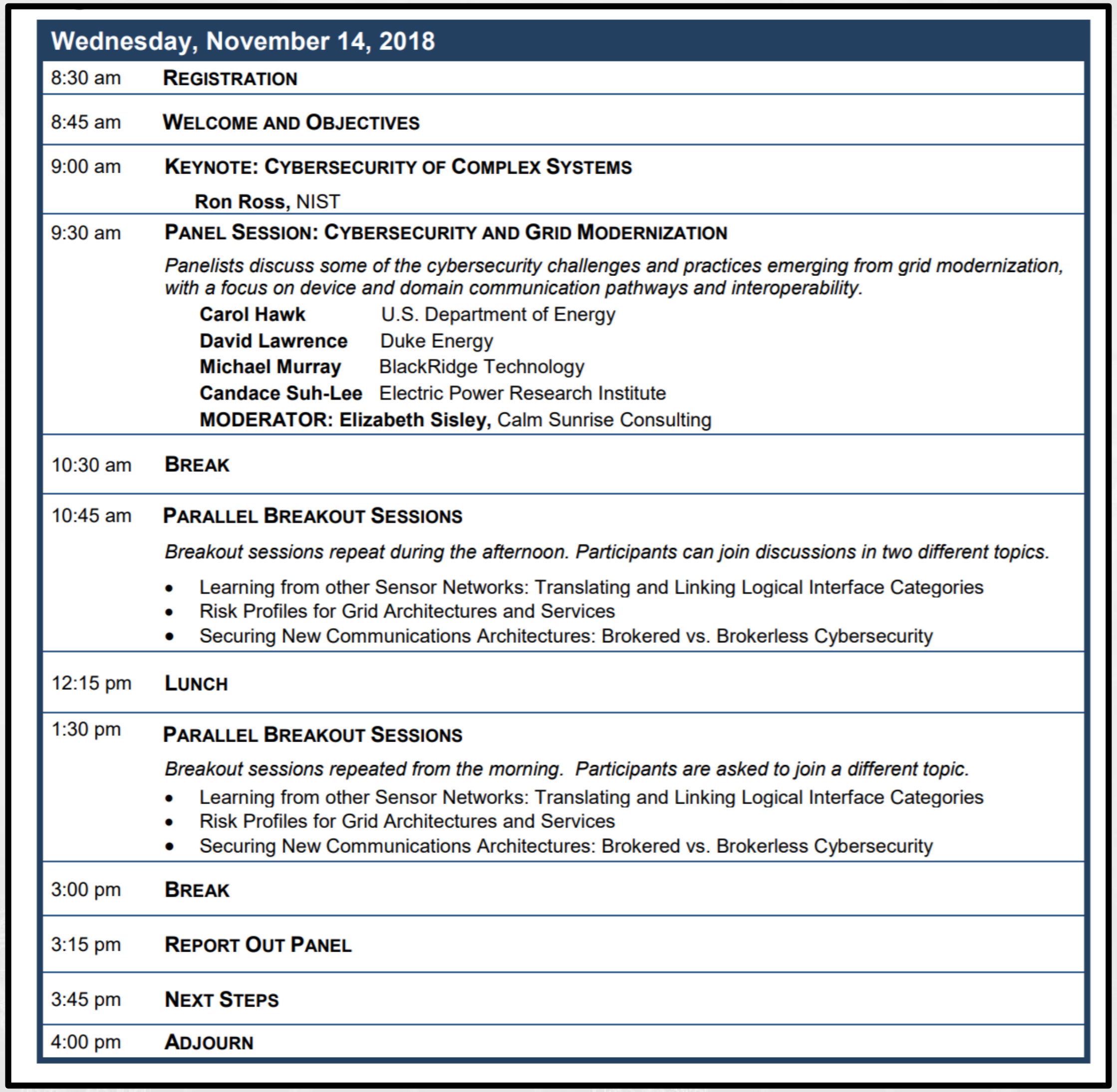
Welcome and Objectives

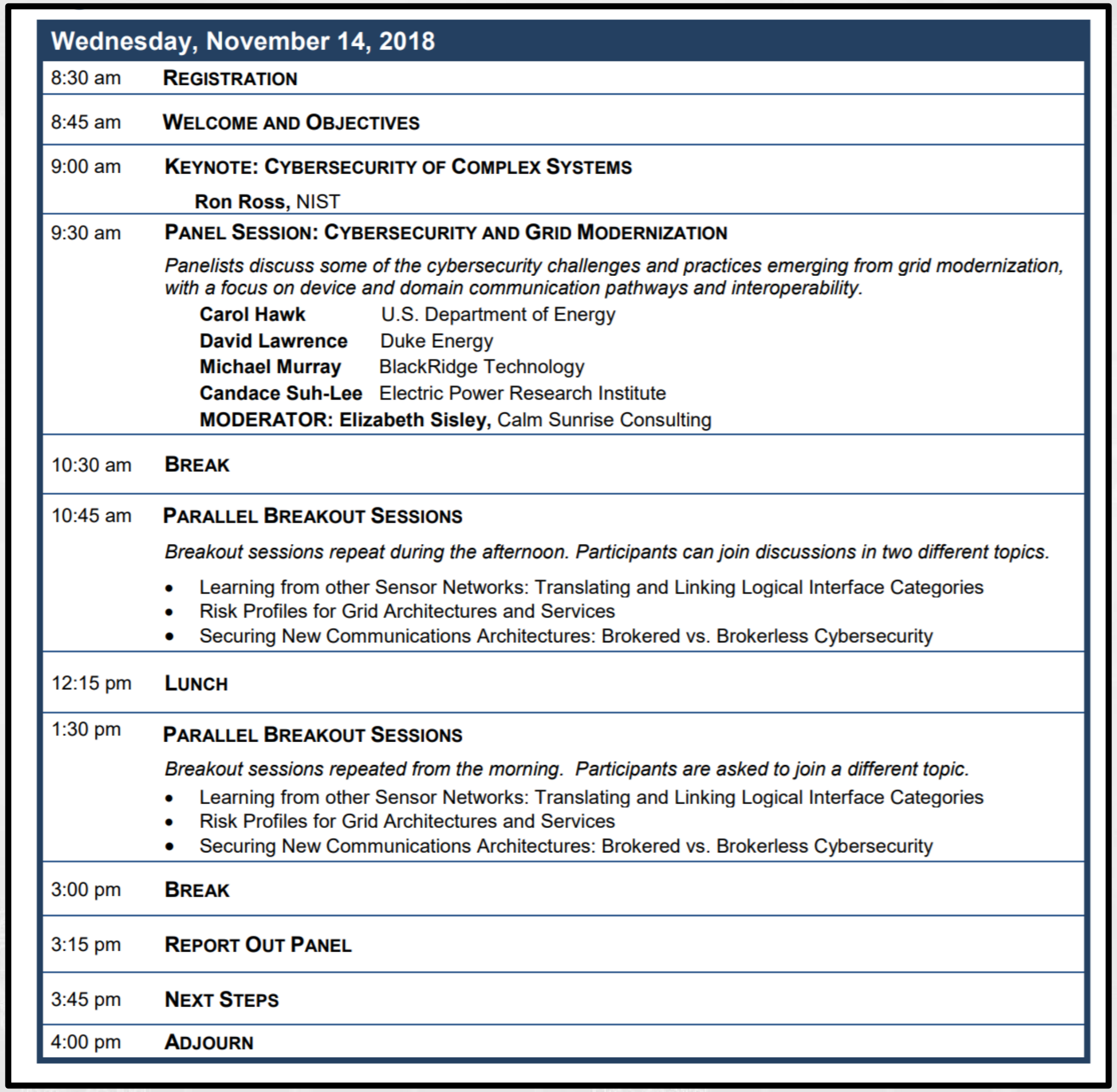


Tuesday, November 13, 2018	
9:30 am	**Registration**
10:00 am	**Welcome and Workshop Objectives** **Chris Greer**, NIST
10:15 am	**Keynote: Grid Modernization and the Case for Interoperability** **John Gibson**, Avista Utilities
11:00 am	**Panel Session: Grid Modernization and Interoperability** *Panelists discuss some of the opportunities, challenges, and technologies at the nexus of grid modernization and interoperability.* **Dwayne Bradley** Duke Energy **Chris Irwin** U.S. Department of Energy **Joe Peichel** Xcel Energy **Alvin Razon** National Rural Electric Cooperative Association **Naza Shelley** District of Columbia Public Service Commission **MODERATOR: David Wollman,** NIST
12:00 pm	**Lunch**
1:15 pm	**Keynote: The Economics of Interoperability** **Wade Malcolm**, Open Energy Solutions
2:00 pm	**Plenary: Introduction to NIST's Smart Grid Conceptual Models** **Avi Gopstein,** NIST
2:30 pm	**Interactive Discussion: Major Concerns for Smart Grid Interoperability** *Participants will identify and give perspectives on important Smart Grid Conceptual Model, and key Aspects and Concerns related to grid modernization and interoperability*
3:30 pm	**Break**
3:45 pm	**Plenary: Three Key Themes for Cybersecurity and Grid Interoperability** • **Risk Profiles—Jeffrey Marron,** NIST • **Interface Categories—Nelson Hastings,** NIST • **Securing Communications—Michael Bartock,** NIST
4:45 pm	**Wrap Up and Charge for Next Day**
5:00 pm	**Adjourn**



Wednesday, November 14, 2018	
8:30 am	**Registration**
8:45 am	**Welcome and Objectives**
9:00 am	**Keynote: Cybersecurity of Complex Systems** **Ron Ross,** NIST
9:30 am	**Panel Session: Cybersecurity and Grid Modernization** *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	**Break**
10:45 am	**Parallel Breakout Sessions** *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	**Lunch**
1:30 pm	**Parallel Breakout Sessions** *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	**Break**
3:15 pm	**Report Out Panel**
3:45 pm	**Next Steps**
4:00 pm	**Adjourn**

Cybersecurity of Complex Systems – Ron Ross



Wednesday, November 14, 2018

8:30 am	**Registration**
8:45 am	**Welcome and Objectives**
9:00 am	**Keynote: Cybersecurity of Complex Systems** **Ron Ross**, NIST
9:30 am	**Panel Session: Cybersecurity and Grid Modernization** *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	**Break**
10:45 am	**Parallel Breakout Sessions** *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	**Lunch**
1:30 pm	**Parallel Breakout Sessions** *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	**Break**
3:15 pm	**Report Out Panel**
3:45 pm	**Next Steps**
4:00 pm	**Adjourn**

Cybersecurity of Complex Systems

An Urgent International Imperative

The Current Landscape.

It’s a dangerous world in cyberspace…

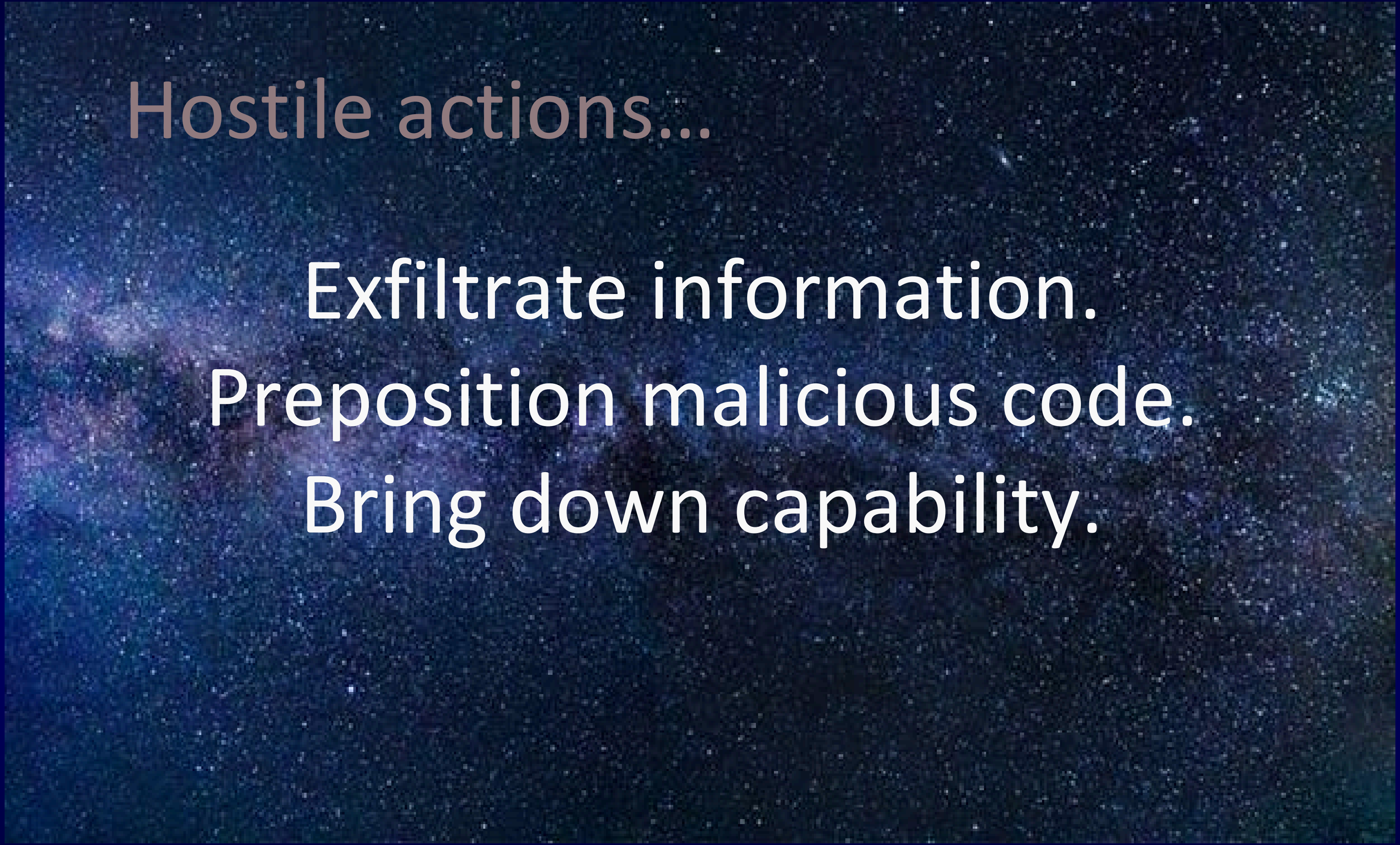
Cyber adversaries…

Nation states.

Terrorist groups.

Criminal enterprises.

Disgruntled individuals.



Hostile actions…

Exfiltrate information.

Preposition malicious code.

Bring down capability.

Complexity.

Attack surface.

Our appetite for *advanced technology* is rapidly exceeding our ability to protect it.

Data. Data. Everywhere.

Cyber Risk.

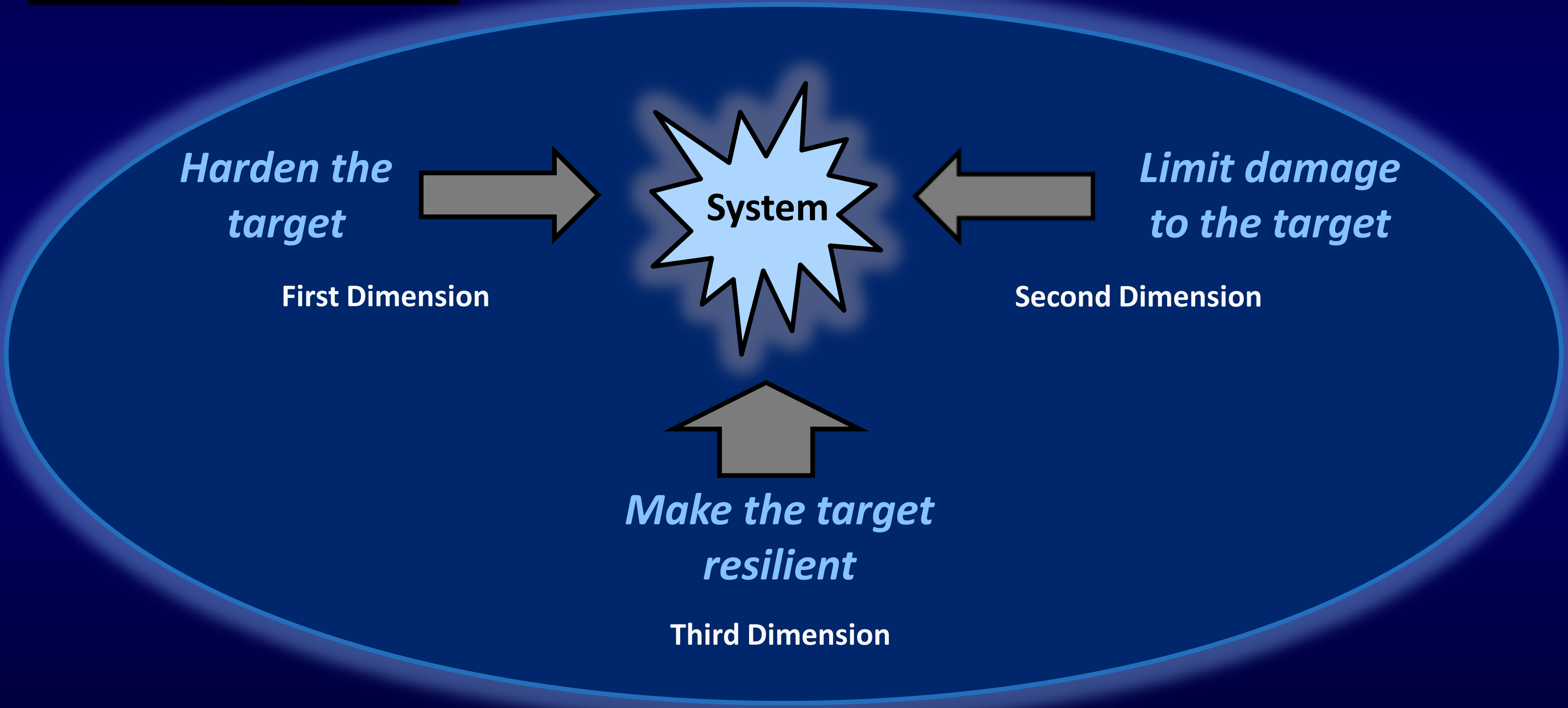
Function (threat, vulnerability, impact, likelihood)

Protecting critical systems and assets—

The highest priority for the national and economic security interests of the United States and our Allies.

Defending cyberspace
in 2018 and beyond.

Reducing susceptibility to *cyber threats* requires a multidimensional strategy.



Cyber Resiliency.

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

Cyber resiliency relationships with other specialty engineering disciplines.

Cyber Resiliency Constructs in System Life Cycle.

ISO/IEC/IEEE 15288:2015

Systems and software engineering — System life cycle processes

ISO IEEE IEC

- Business or mission analysis
  - Stakeholder needs and requirements definition
    - System requirements definition
      - Architecture definition
        - Design definition
          - System analysis
            - Implementation
            - Integration
          - Verification
        - Transition
      - Validation
    - Operation
  - Maintenance
- Disposal

NIST SP 800-160

CREF

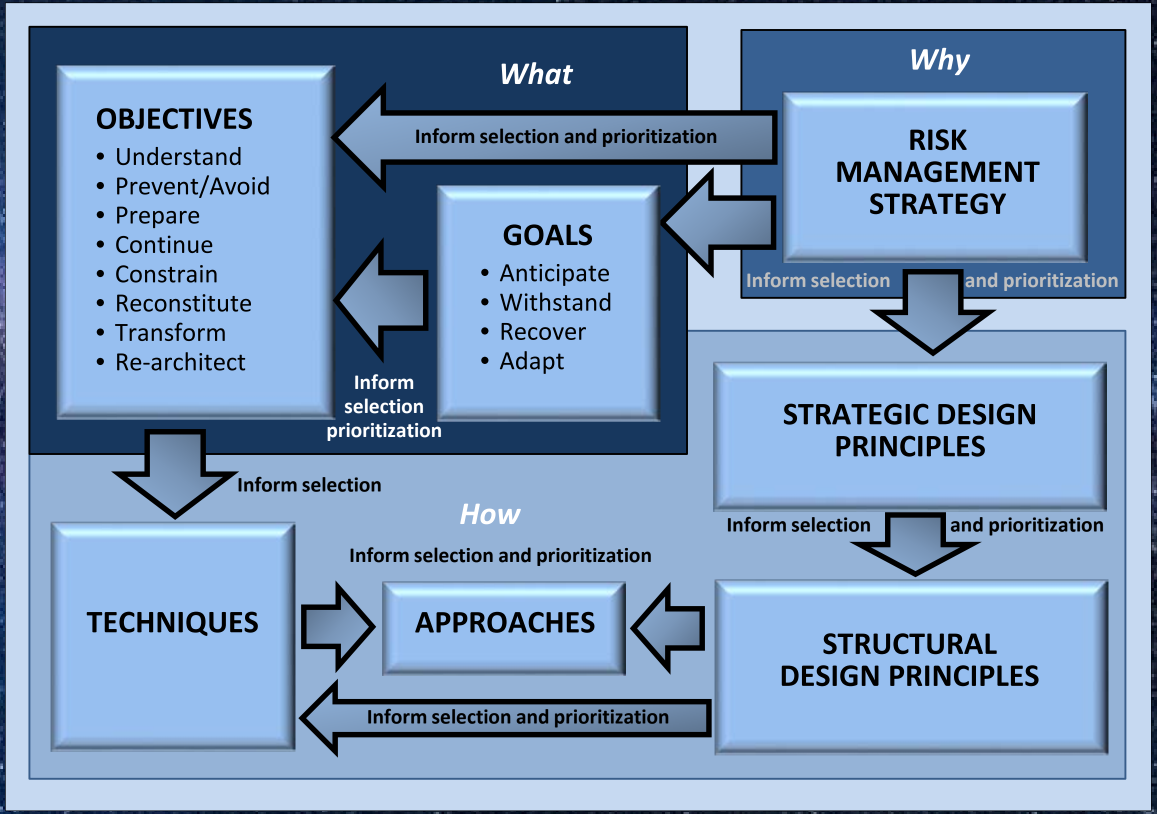
CYBER RESILIENCY ENGINEERING FRAMEWORK

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

Constructs

- Goals
  - Objectives
    - Techniques
      - Approaches
        - Strategic Design Principles
          - Structural Design Principles
            - Risk Management Strategy

Relationship among cyber resiliency constructs.



CREF

CYBER RESILIENCY ENGINEERING FRAMEWORK

PROTECTION. DAMAGE LIMITATION. RESILIENCY.

Techniques

- Adaptive Response
- Analytic Monitoring
- Coordinated Protection
- Substantiated Integrity
- Privilege Restriction
- Dynamic Positioning
- Dynamic Representation

- Non-Persistence
- Diversity
- Realignment
- Redundancy
- Segmentation
- Deception
- Unpredictability

Transparency.

Traceability.

Trust.

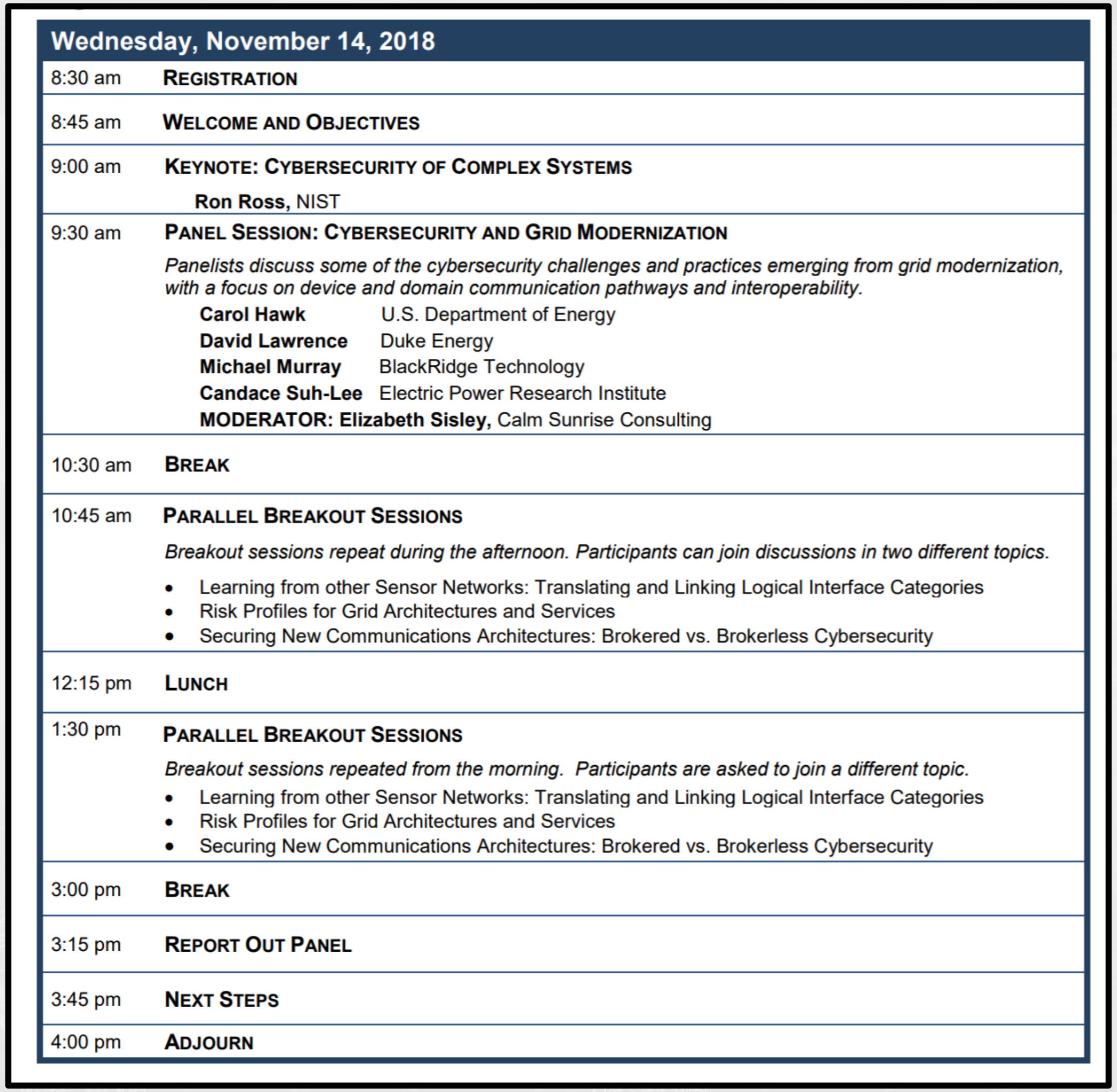
Government

Academia

The essential partnership.

Industry

Cybersecurity & Grid Modernization – Panel

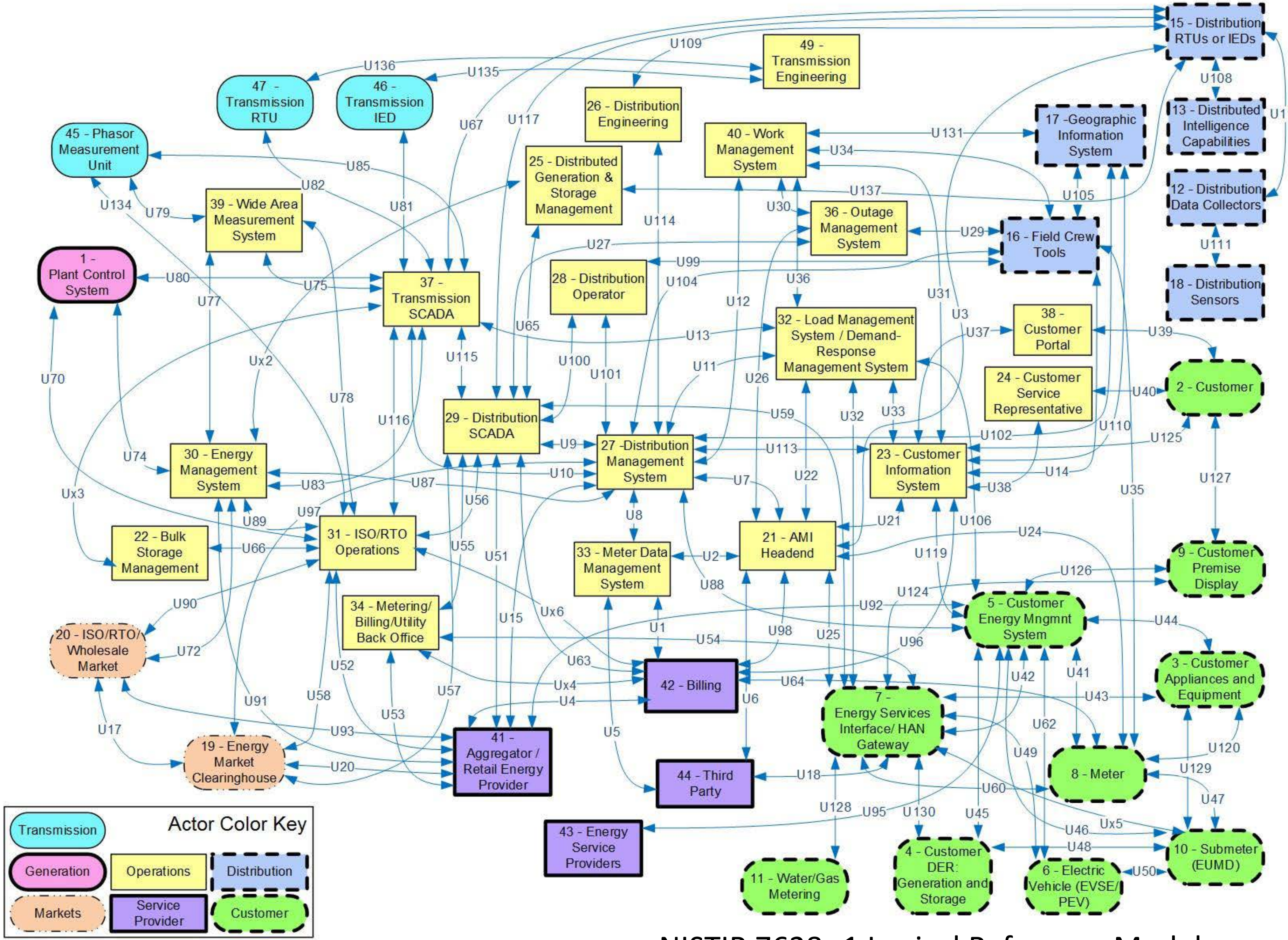


Wednesday, November 14, 2018	
8:30 am	**Registration**
8:45 am	**Welcome and Objectives**
9:00 am	**Keynote: Cybersecurity of Complex Systems** **Ron Ross,** NIST
9:30 am	**Panel Session: Cybersecurity and Grid Modernization** *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	**Break**
10:45 am	**Parallel Breakout Sessions** *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	**Lunch**
1:30 pm	**Parallel Breakout Sessions** *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	**Break**
3:15 pm	**Report Out Panel**
3:45 pm	**Next Steps**
4:00 pm	**Adjourn**

PANEL SESSION: CYBERSECURITY AND GRID MODERNIZATION

- *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.*
  - **Carol Hawk** U.S. Department of Energy
  - **David Lawrence** Duke Energy
  - **Michael Murray** BlackRidge Technology
  - **Candace Suh-Lee** Electric Power Research Institute
  - **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting

- SEPA (originally SGIP):
  - Active member of both Architecture and Cybersecurity Committees since 2009, primary architect for the NISTIR 7628's Logical Reference Architecture
  - Chair of Grid Architecture Ontology Task Force
    - With the initial work complete, the next step is to understand how the ontology results and methods can be applied in the DOE GMLC Grid Architecture work. A micro grid example is planned.
  - Chair of Cyber-Physical Resiliency Task Force
    - Catalog of CPR Best Practices
      - https://sepapower.org/knowledge/catalog-of-cyber-physical-resiliency-best-practices/
    - Started a Crosswalk between 7628r1 cybersecurity controls and CPR Best Practices to create a supplemental SEPA document of Resiliency Controls



1 - Plant Control System

2 - Customer

3 - Customer Appliances and Equipment

4 - Customer DER: Generation and Storage

5 - Customer Energy Mngmnt System

6 - Electric Vehicle (EVSE/ PEV)

7 - Energy Services Interface/ HAN Gateway

8 - Meter

9 - Customer Premise Display

10 - Submeter (EUMD)

11 - Water/Gas Metering

12 - Distribution Data Collectors

13 - Distributed Intelligence Capabilities

15 - Distribution RTUs or IEDs

16 - Field Crew Tools

17 -Geographic Information System

18 - Distribution Sensors

19 - Energy Market Clearinghouse

20 - ISO/RTO/ Wholesale Market

21 - AMI Headend

22 - Bulk Storage Management

23 - Customer Information System

24 - Customer Service Representative

25 - Distributed Generation & Storage Management

26 - Distribution Engineering

27 -Distribution Management System

28 - Distribution Operator

29 - Distribution SCADA

30 - Energy Management System

31 - ISO/RTO Operations

32 - Load Management System / Demand-Response Management System

33 - Meter Data Management System

34 - Metering/ Billing/Utility Back Office

36 - Outage Management System

37 - Transmission SCADA

38 - Customer Portal

39 - Wide Area Measurement System

40 - Work Management System

41 - Aggregator / Retail Energy Provider

42 - Billing

43 - Energy Service Providers

44 - Third Party

45 - Phasor Measurement Unit

46 - Transmission IED

47 - Transmission RTU

49 - Transmission Engineering

Actor Color Key

Actor Color Key
Transmission
Generation
Operations
Distribution
Markets
Service Provider
Customer

NISTIR 7628 r1 Logical Reference Model

Carol Hawk – U.S. Department of Energy

U.S. DEPARTMENT OF
ENERGY

OFFICE OF
CYBERSECURITY, ENERGY SECURITY,
AND EMERGENCY RESPONSE

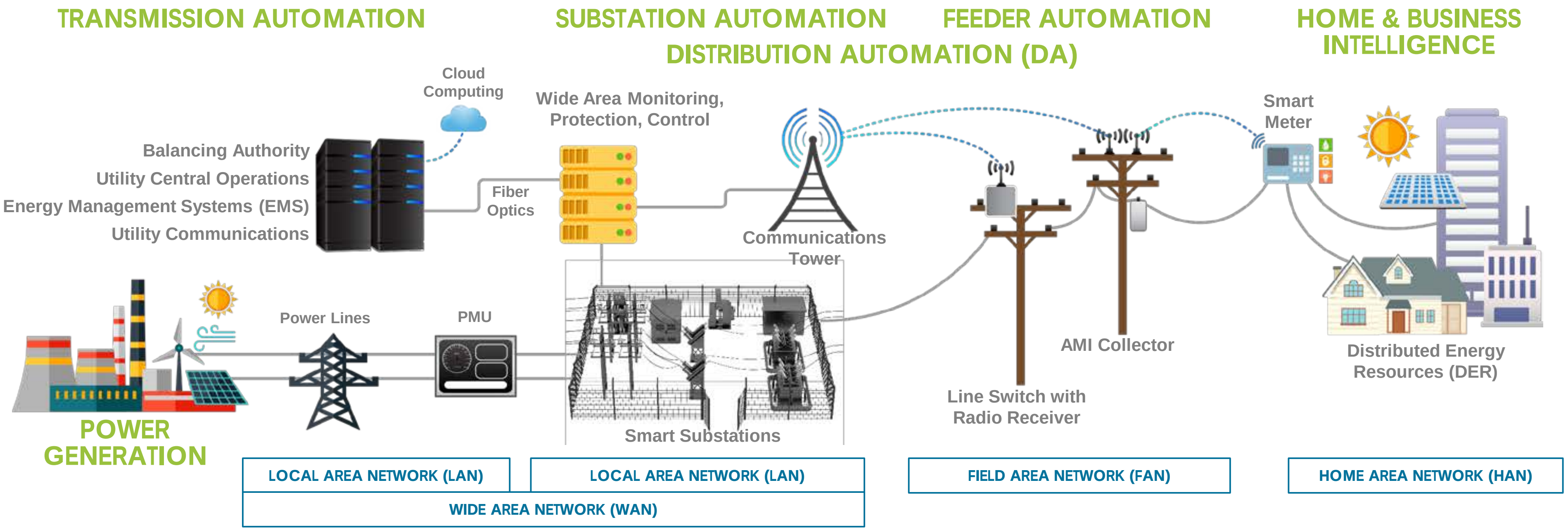
Cybersecurity for Energy Delivery Systems (CEDS) Division Overview

Carol Hawk

Acting Deputy Assistant Secretary

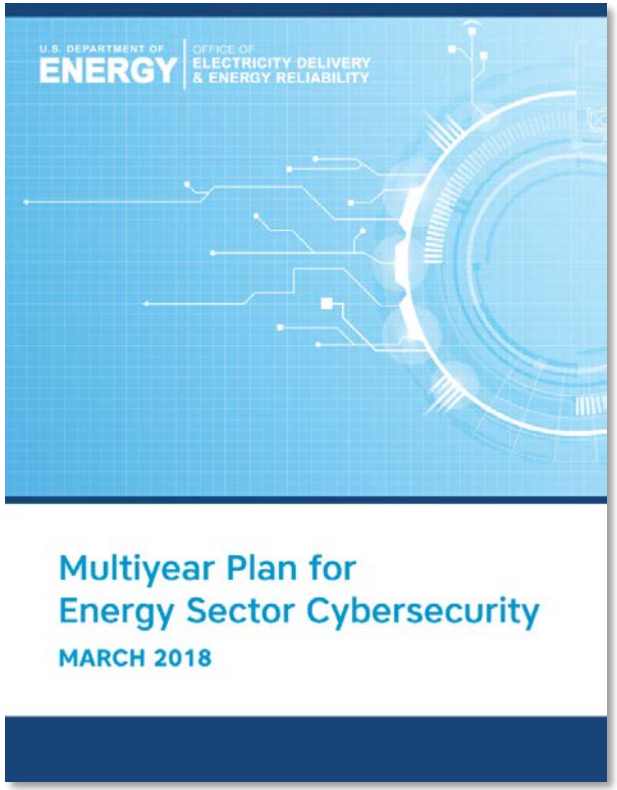
November 14, 2018

Electricity Delivery Infrastructure



U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

DOE CESER Multiyear Plan for Energy Sector Cybersecurity



U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

Multiyear Plan for Energy Sector Cybersecurity

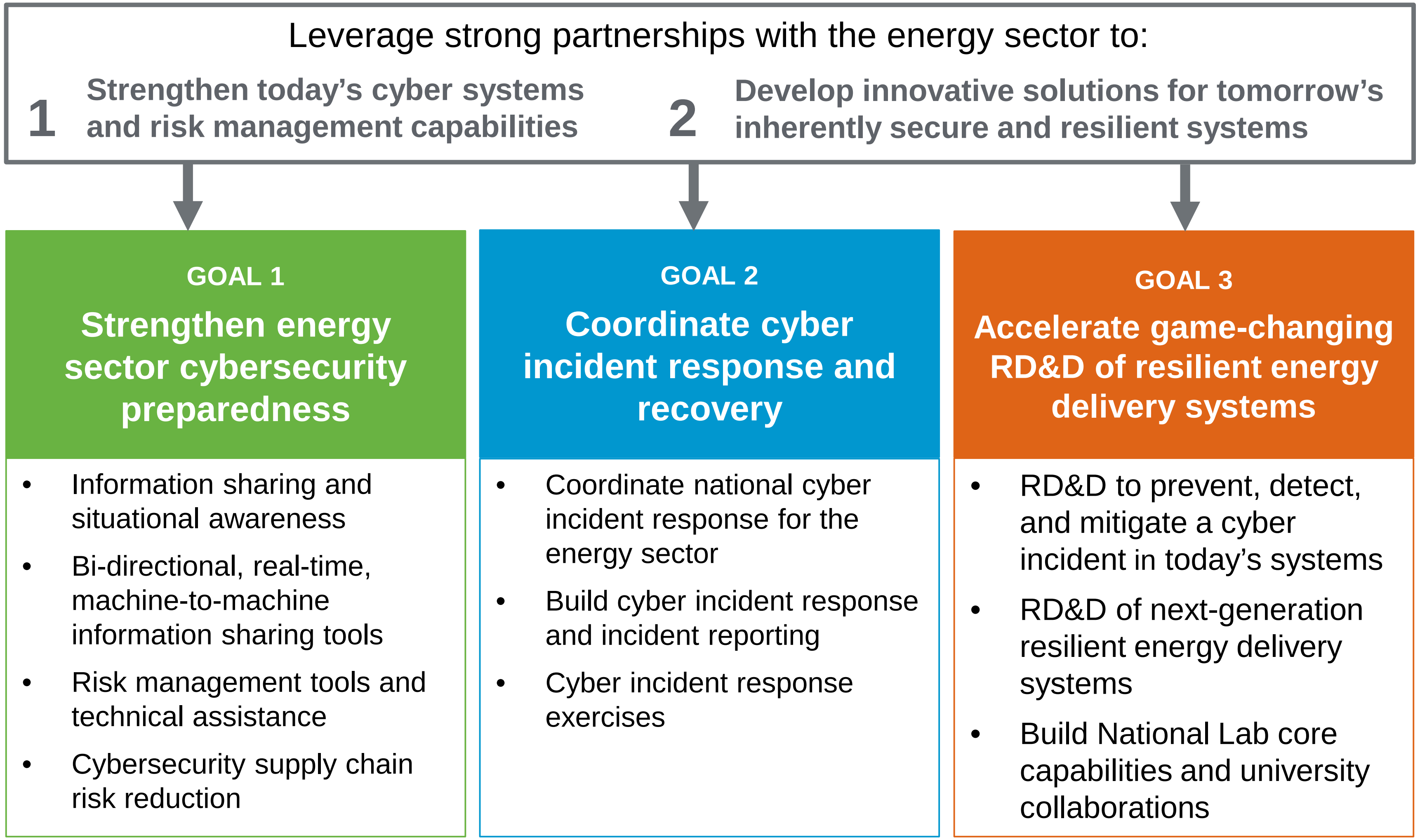
MARCH 2018

- **DOE’s strategy** for partnering with industry to protect U.S. energy system from cyber risks
- **Guided by direct industry input** on cybersecurity needs and priorities – complements the Energy Sector Roadmap
- **Market-based approach** encourages investment and cost-sharing of promising technologies and practices
- **Establishes goals, objectives, and activities** to improve both near- and long-term energy cybersecurity

DOE Vision

Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions

DOE’s Strategy for Energy Sector Cybersecurity



Leverage strong partnerships with the energy sector to:

1 Strengthen today’s cyber systems and risk management capabilities

2 Develop innovative solutions for tomorrow’s inherently secure and resilient systems

GOAL 1
Strengthen energy sector cybersecurity preparedness

- Information sharing and situational awareness
- Bi-directional, real-time, machine-to-machine information sharing tools
- Risk management tools and technical assistance
- Cybersecurity supply chain risk reduction

GOAL 2
Coordinate cyber incident response and recovery

- Coordinate national cyber incident response for the energy sector
- Build cyber incident response and incident reporting
- Cyber incident response exercises

GOAL 3
Accelerate game-changing RD&D of resilient energy delivery systems

- RD&D to prevent, detect, and mitigate a cyber incident in today’s systems
- RD&D of next-generation resilient energy delivery systems
- Build National Lab core capabilities and university collaborations

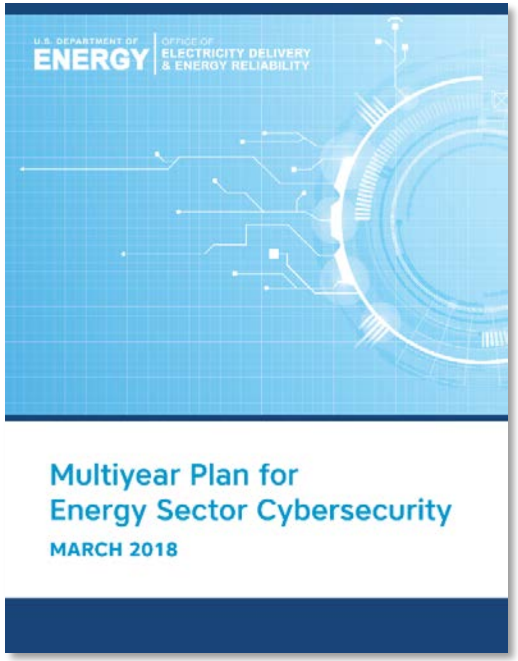
Coordination with Other Federal Cybersecurity R&D Programs

NITRD

- Primary mechanism for U.S. Government, unclassified Networking and IT R&D (NITRD) coordination
- Supports Networking and Information Technology policy making in the White House Office of Science and Technology Policy (OSTP)

DARPA
U.S. Department of Homeland Security
Department of Energy United States of America
NNSA National Nuclear Security Administration
United States Environmental Protection Agency
National Institutes of Health
NASA
NIST
The Office of the National Coordinator for Health Information Technology
NOAA National Oceanic and Atmospheric Administration U.S. Department of Commerce
AHRQ
NSF
National Archives
National Security Agency United States of America
National Reconnaissance Office United States of America
Department of Defense United States of America

For More Information, Please Contact:



U.S. DEPARTMENT OF ENERGY | OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY

Multiyear Plan for Energy Sector Cybersecurity

MARCH 2018

Dr. Carol Hawk
Acting Deputy Assistant Secretary
Cybersecurity for Energy Delivery Systems (CEDS) Division
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)

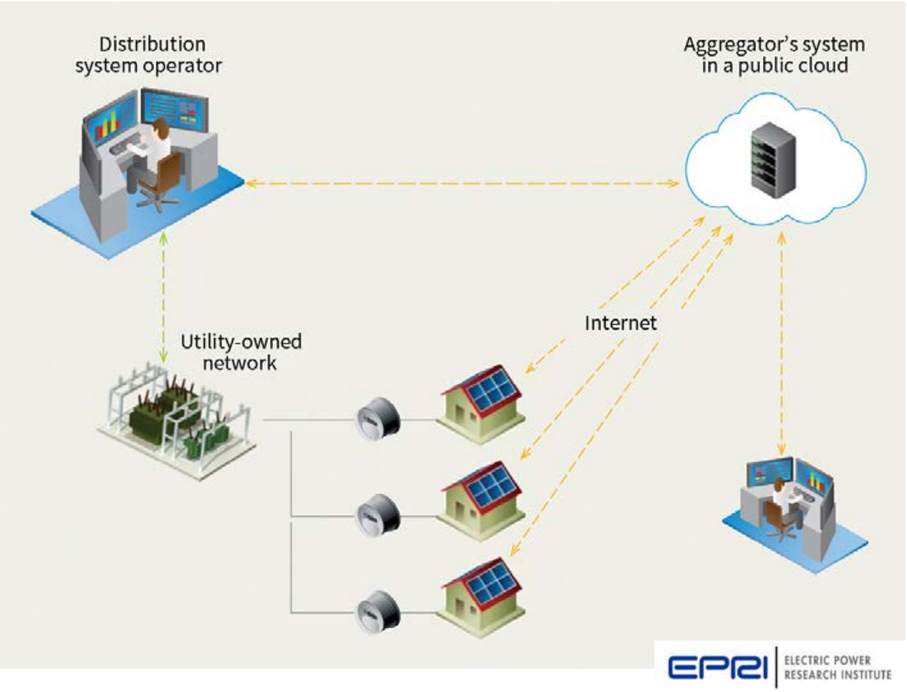
Carol.Hawk@hq.doe.gov
202-586-3247

Visit: https://www.energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response

David Lawrence – Duke Energy

Regulatory Gaps in Cybersecurity

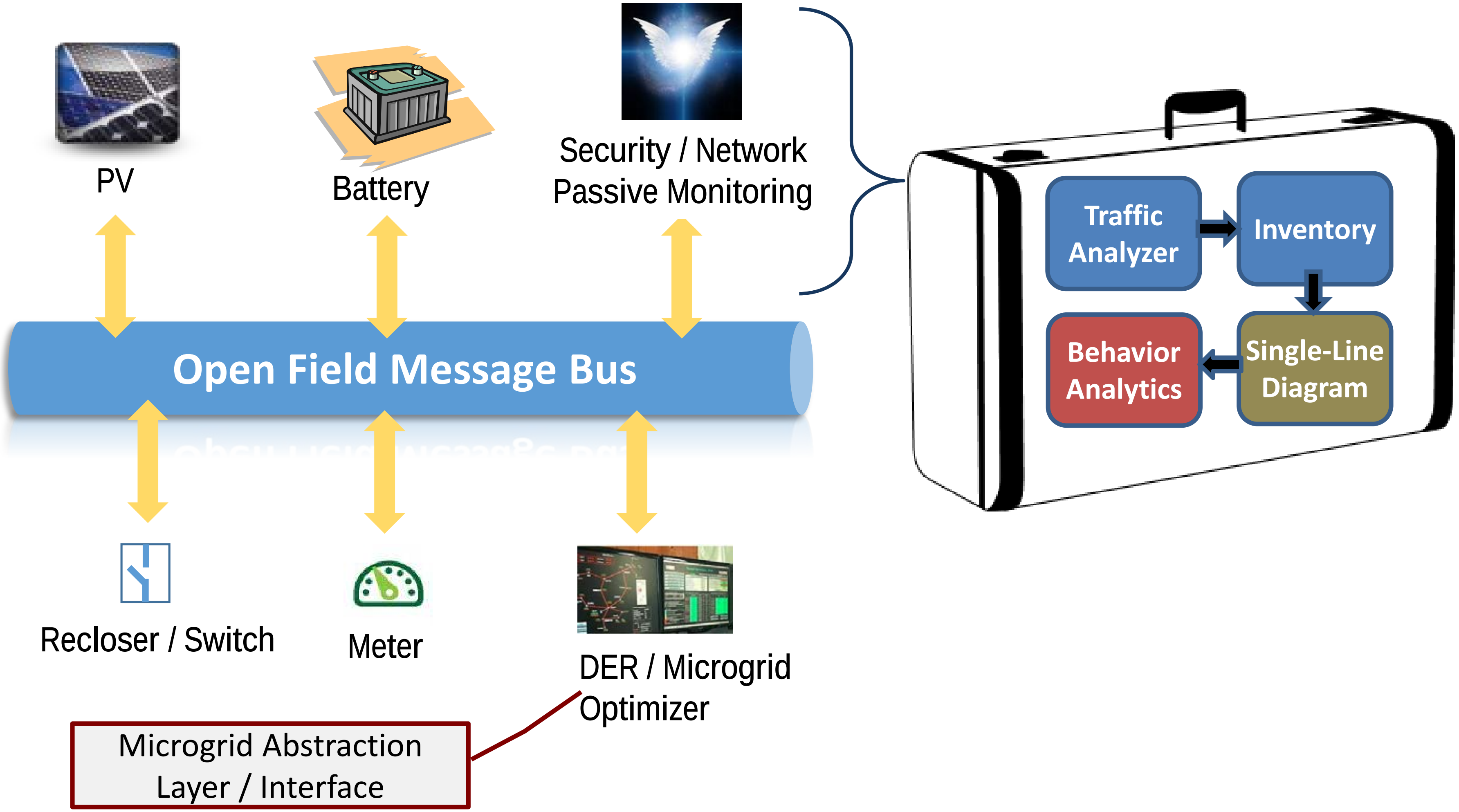
- **IEEE 1547 – 2018 DER Interconnection Standard**
  - Addresses interoperability by specifying mandatory protocols for smart inverter’s communications interfaces
    - IEEE P2030.5, DNP3, or SunSpec Modbus
    - Only P2030.5 suggests TLS 1.2 over HTTPS for 3rd party BTM aggregators.


Distribution system operator
Aggregator’s system in a public cloud
Internet
Utility-owned network
EPRI ELECTRIC POWER RESEARCH INSTITUTE

  - **Does not address Cybersecurity** needs, concerns, or requirements for the communication protocols, devices, or interfaces

- **Situational awareness continues to be a major gap for OT!**

ICS Passive Monitoring - POC



PV

Battery

Security / Network Passive Monitoring

Open Field Message Bus

Recloser / Switch

Meter

DER / Microgrid Optimizer

Microgrid Abstraction Layer / Interface

Traffic Analyzer

Inventory

Single-Line Diagram

Behavior Analytics

OpenFMB Cybersecurity 2019 Initiatives

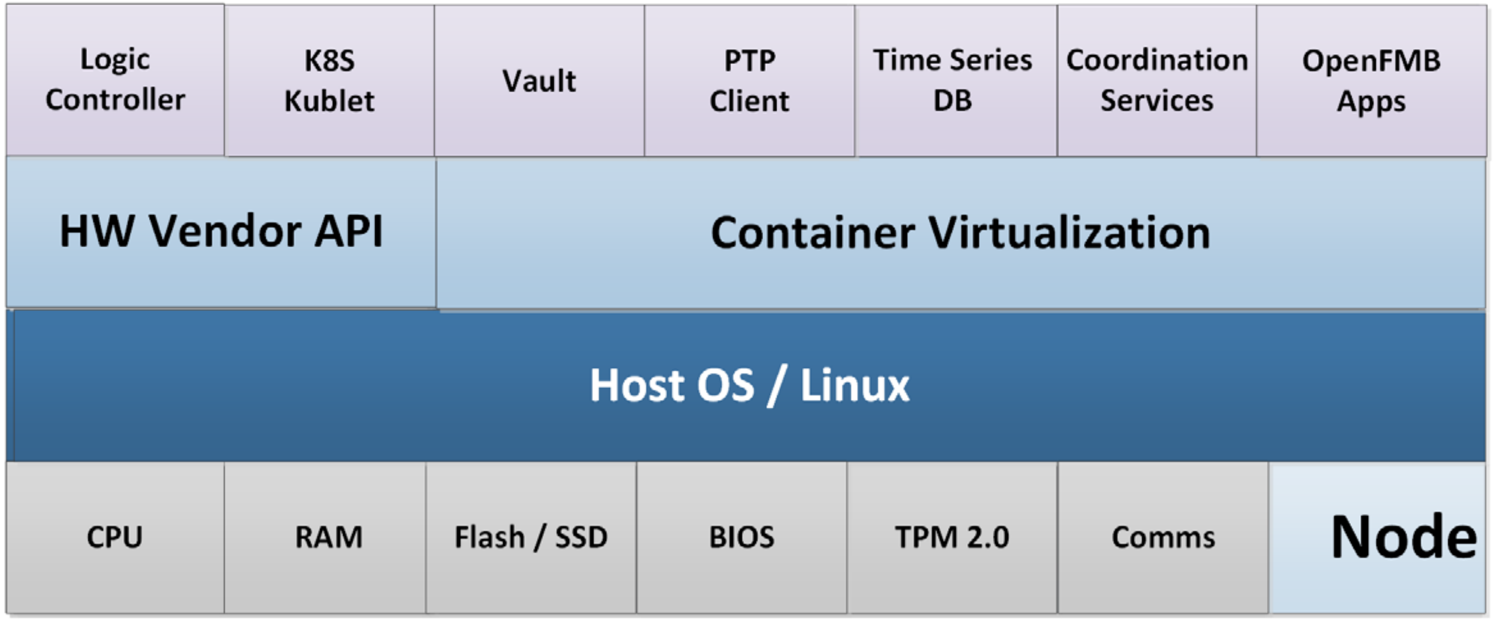
- Identity Management
  - Grid Device Provisioning – Use Case Modeling
  - TPM 2.0 for Hardened Identity
  - Secure Boot, OS, Containers
  - Pub / Sub Protocol Integration with TPM 2.0

- Key Management, DPKI
  - Refer to IEC 62351-9 and SSP21; Use Case Modeling

- Network and System Management (NSM) IEC 62351–7
  - Coordinate with past EPRI MIB definition work
  - Situational Awareness: ICS Network Monitoring and Microgrid Analytics

- Dynamic Grid – Pub / Sub Architecture Strawman
  - Microgrid, FLISR, Circuit-segment orchestration
  - Software Defined Networking (SDN)
  - Scope of Certificates with FLISR

Node Architecture



Logic Controller | K8S Kublet | Vault | PTP Client | Time Series DB | Coordination Services | OpenFMB Apps

HW Vendor API | Container Virtualization

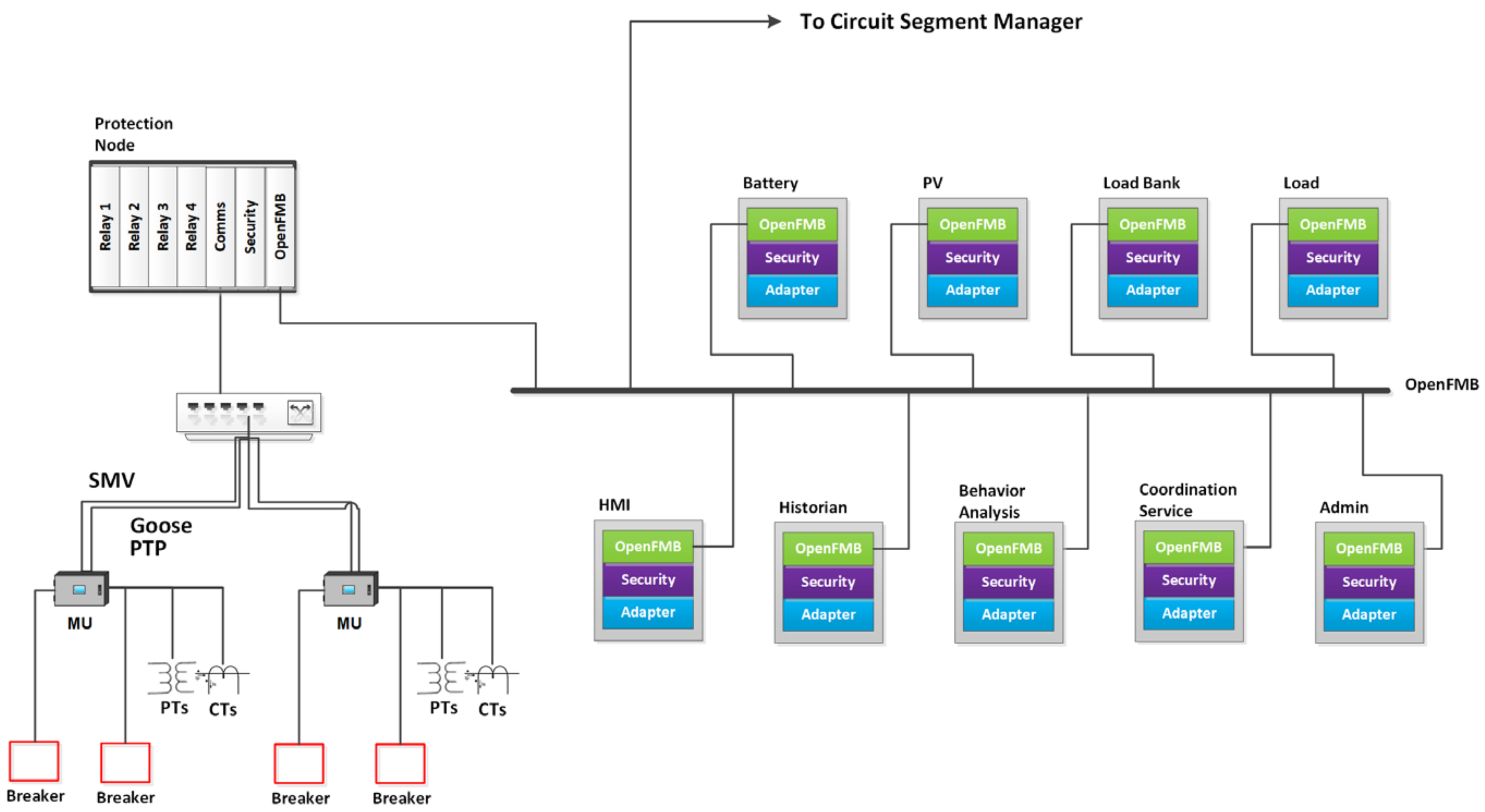
Host OS / Linux

CPU | RAM | Flash / SSD | BIOS | TPM 2.0 | Comms | Node

- Pods are the atomic unit for Kubernetes management
- 1 Pod can be equal to 1 Container or multiple Containers
- Containers are on an internal 10.x.x.x network for cross Container communications

- Discuss / define the Boot sequence
- TPM 2.0 interface / drivers / library
- Coordination between Containers, and Containers and TPM

IEC 61850 Digital Microgrid & OpenFMB

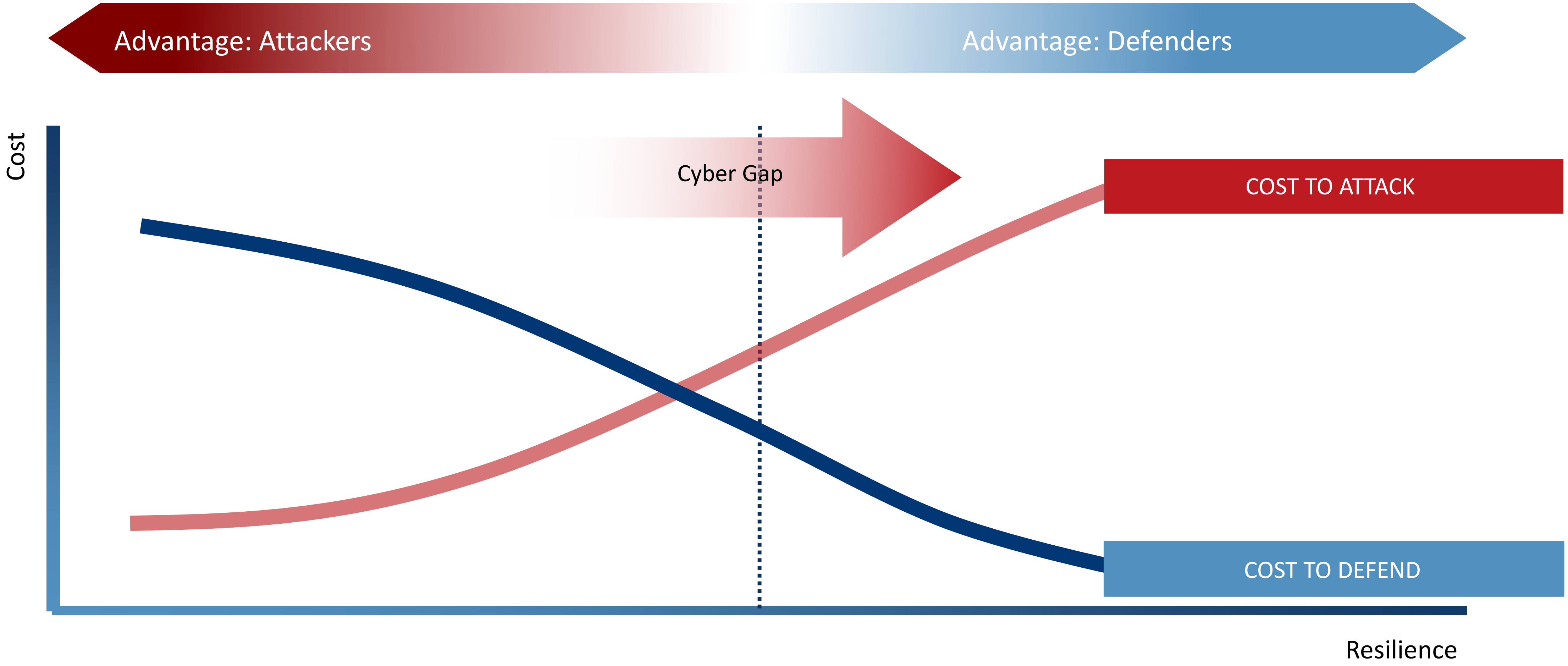


Duke Energy: keeping the lights on so you can sleep peacefully!

“Working to Secure the Grid, One Distributed Autonomous Function at a Time!”

Michael Murray – BlackRidge Technology

End Game: Resilient Architectures Require Economic Asymmetry



BlackRidge TECHNOLOGY

Homeland Security

US-CERT United States Computer Emergency Readiness Team

THE WHITE HOUSE
WASHINGTON

PRESIDENTIAL EXECUTIVE ORDER ON
STRENGTHENING THE CYBERSECURITY OF FEDERAL
NETWORKS AND CRITICAL INFRASTRUCTURE

Security Tip (ST18-001) Securing Network Infrastructure Devices

NCCIC encourages users and network administrators to implement the following recommendations to better secure their network infrastructure:

- ***Segment and segregate networks and functions.***
- ***Limit unnecessary lateral communications.***
- Harden network devices.
- ***Secure access to infrastructure devices.***
- ***Perform Out-of-Band network management.***
- Validate integrity of hardware and software.

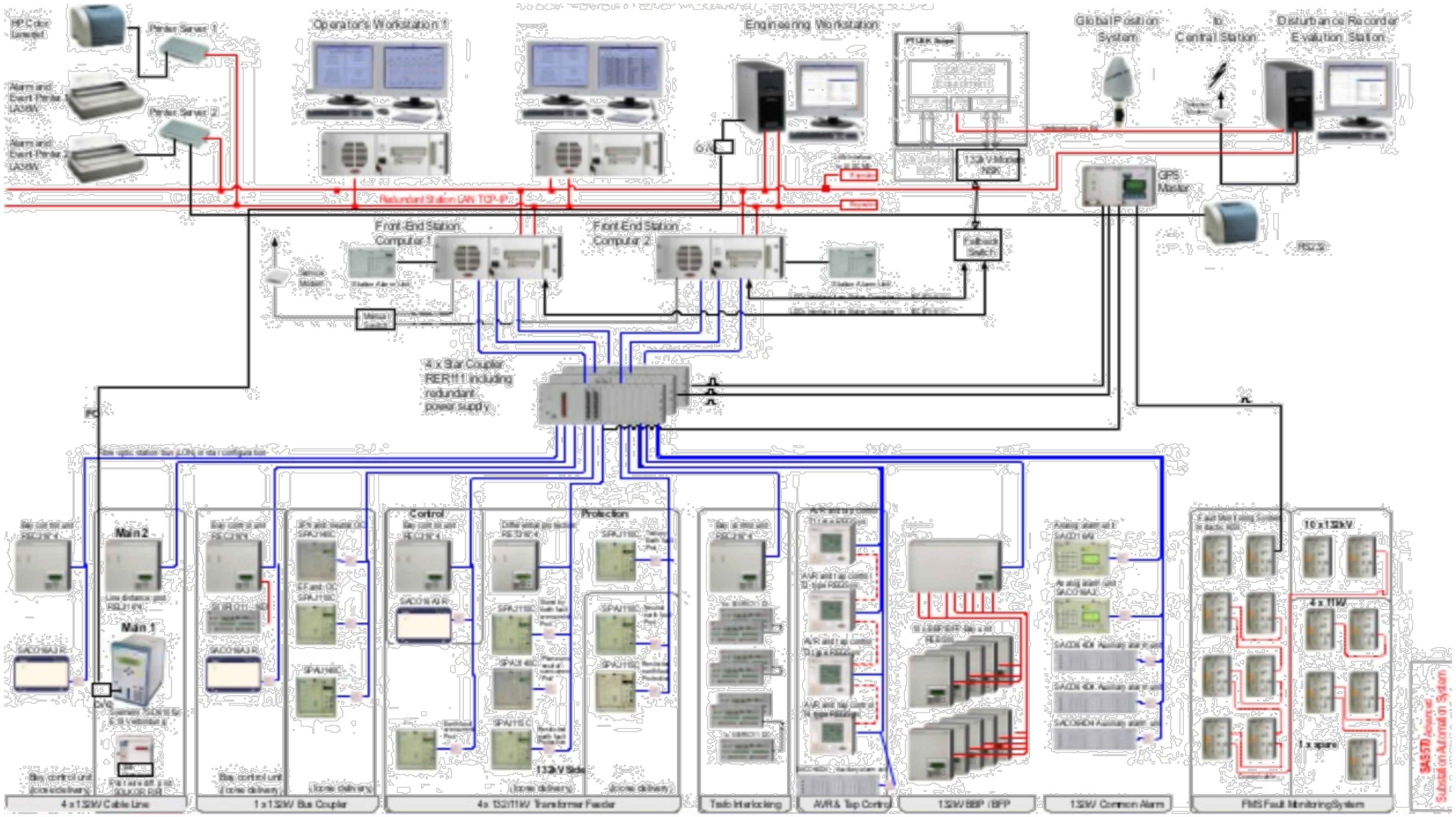
Segment and Segregate Networks and Functions

Security architects must consider the overall infrastructure layout, including segmentation and segregation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. On a poorly segmented network, intruders are able to extend their impact to control critical devices or gain access to sensitive data and intellectual property. Segregation separates network segments based on role and functionality. A securely segregated network can contain malicious occurrences, reducing the impact from intruders in the event that they have gained a foothold somewhere inside the network.

Technical Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

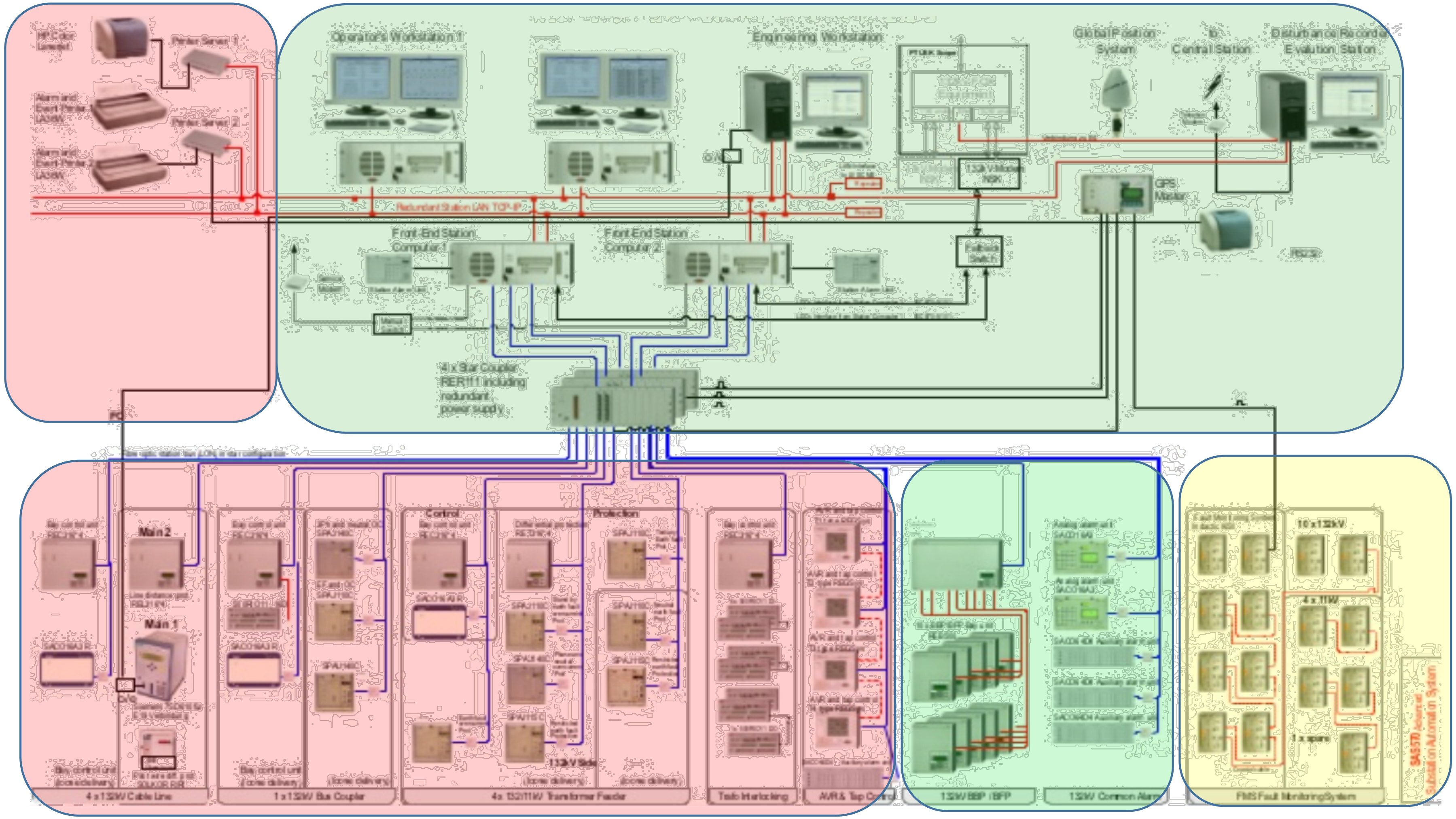
Segmentation / Segregation of Legacy 0,1,2 layers

Legacy Systems are a tapestry of older sensors, controllers and trust policies.



Segmentation / Segregation of all Layers

New Systems can exist with legacy systems through Segmentation and Segregation.



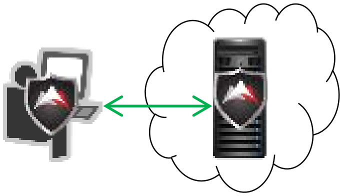
What Can the Community of Interest do to Respond?

Protect Critical Servers and Management Systems

- Protect high value servers and data (PII, algos, research, IP, ….)
- Protect Management Plane of IT networks and systems
- Data centers, IaaS cloud services, and IoT

Isolate and Protect Cloud Services

- Control access to IaaS cloud servers by all parties
- All access attempts logged for audit history with attribution
- No unauthorized awareness of public cloud services



Micro-Segmentation / Software-Based Segmentation / Compliance

- Infrastructure independent and supports heterogenous environments
- Separates security policy from network topology
- Addresses compliance, risk and regulatory requirements

Identity-Based Networking

- Identity Based Policy and Network Access
- Topology Independent Networking

BlackRidge TECHNOLOGY

Candace Suh-Lee – EPRI

Cybersecurity and Grid Modernization

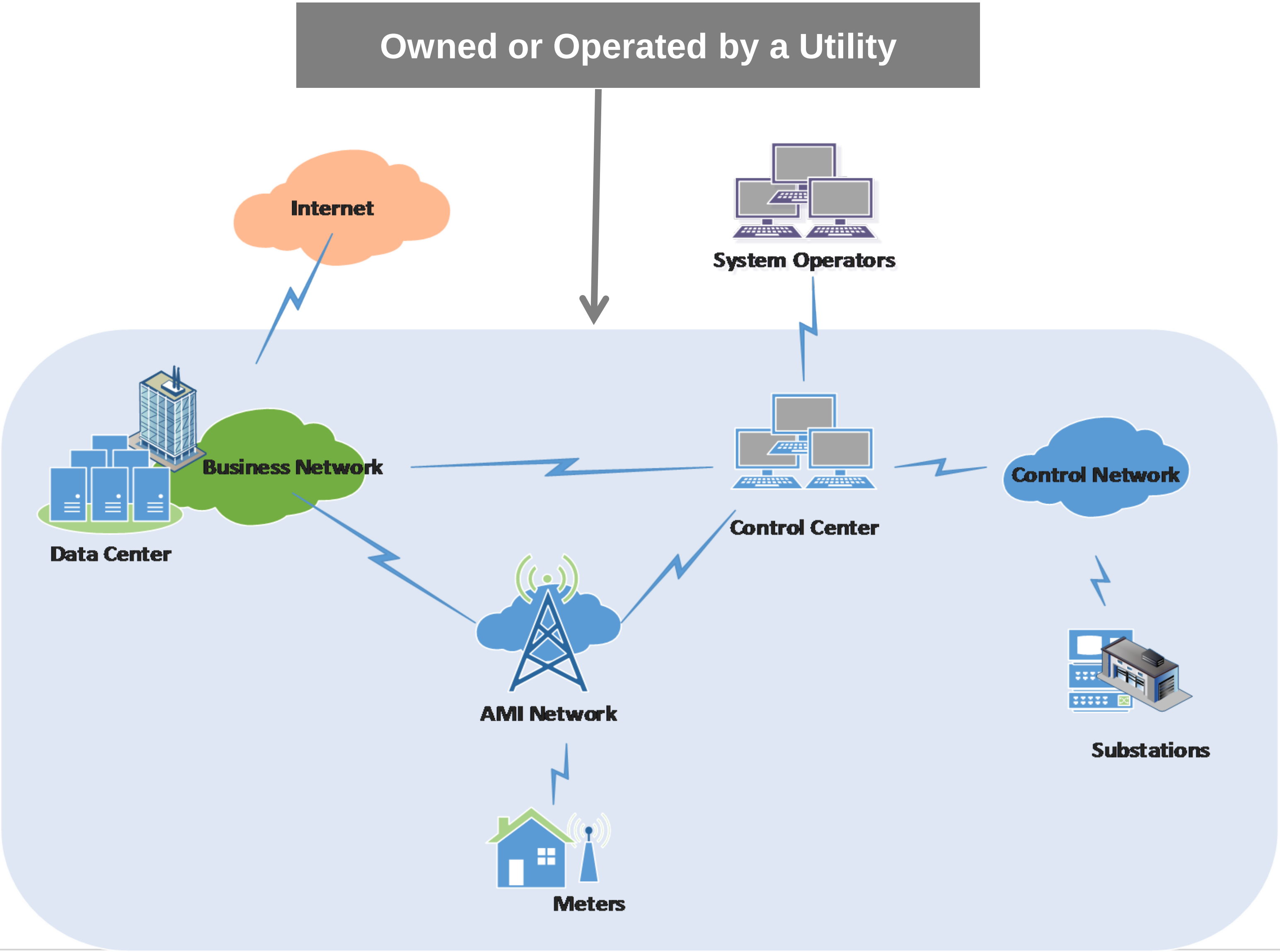
Challenges and Urgent Needs

Candace Suh-Lee, CISSP, CISA
Principal Technical Leader

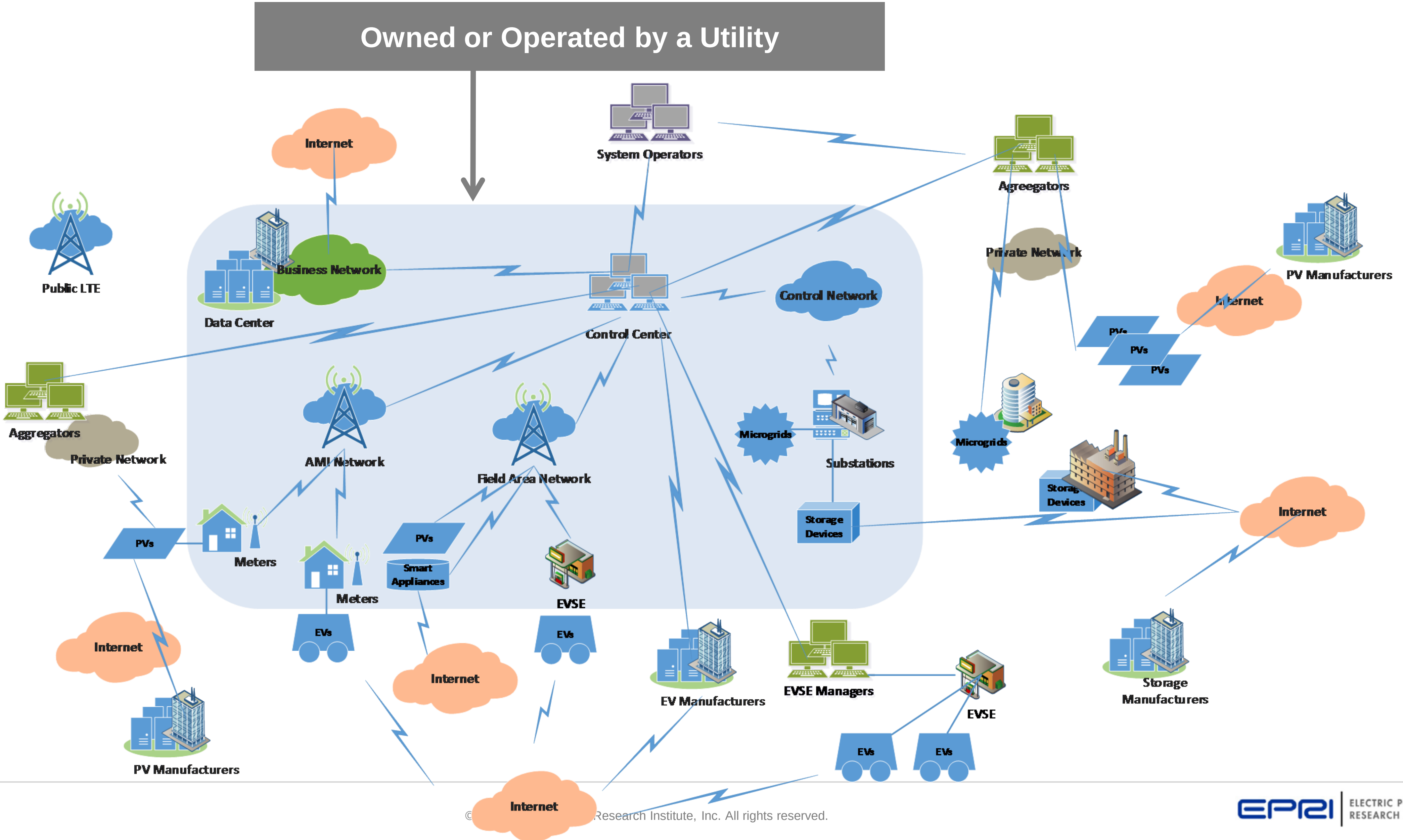
Workshop on Smart Grid Interoperability and Cybersecurity, NCCoE

November 13-14, 2018

Utility Communications – Recent Past



Smart Grid Communications – Near Future



Owned or Operated by a Utility

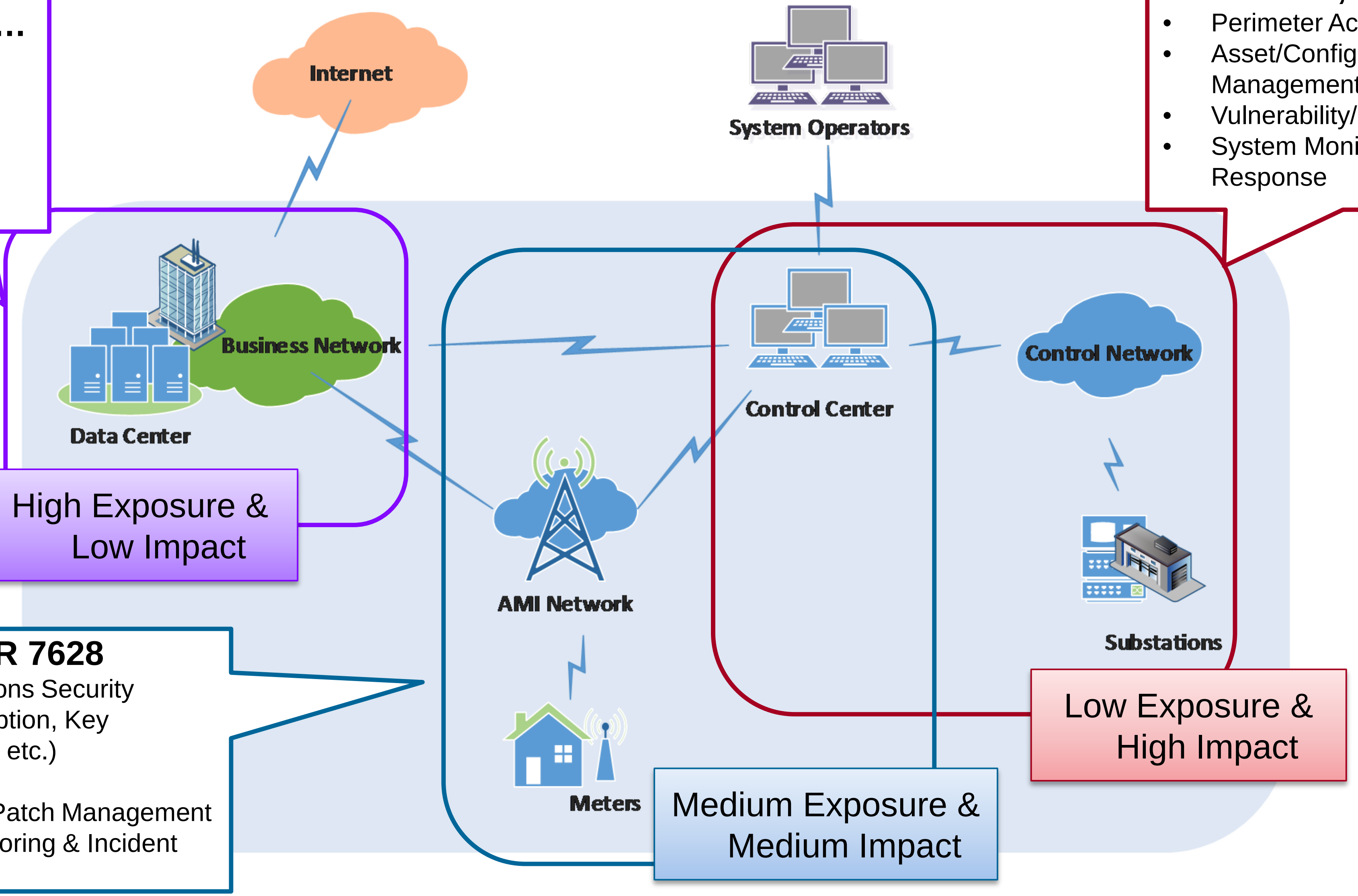
Risk Profile & Security Requirements – Recent Past

PCI, ISO27001/2, …

- Threat monitoring & Incident Response
- Vulnerability/Patch Management
- Perimeter & End-point Protection

ISA99, NERC CIP

- Perimeter Access Controls
- Asset/Configuration/Change Management
- Vulnerability/Patch Management
- System Monitoring & Incident Response



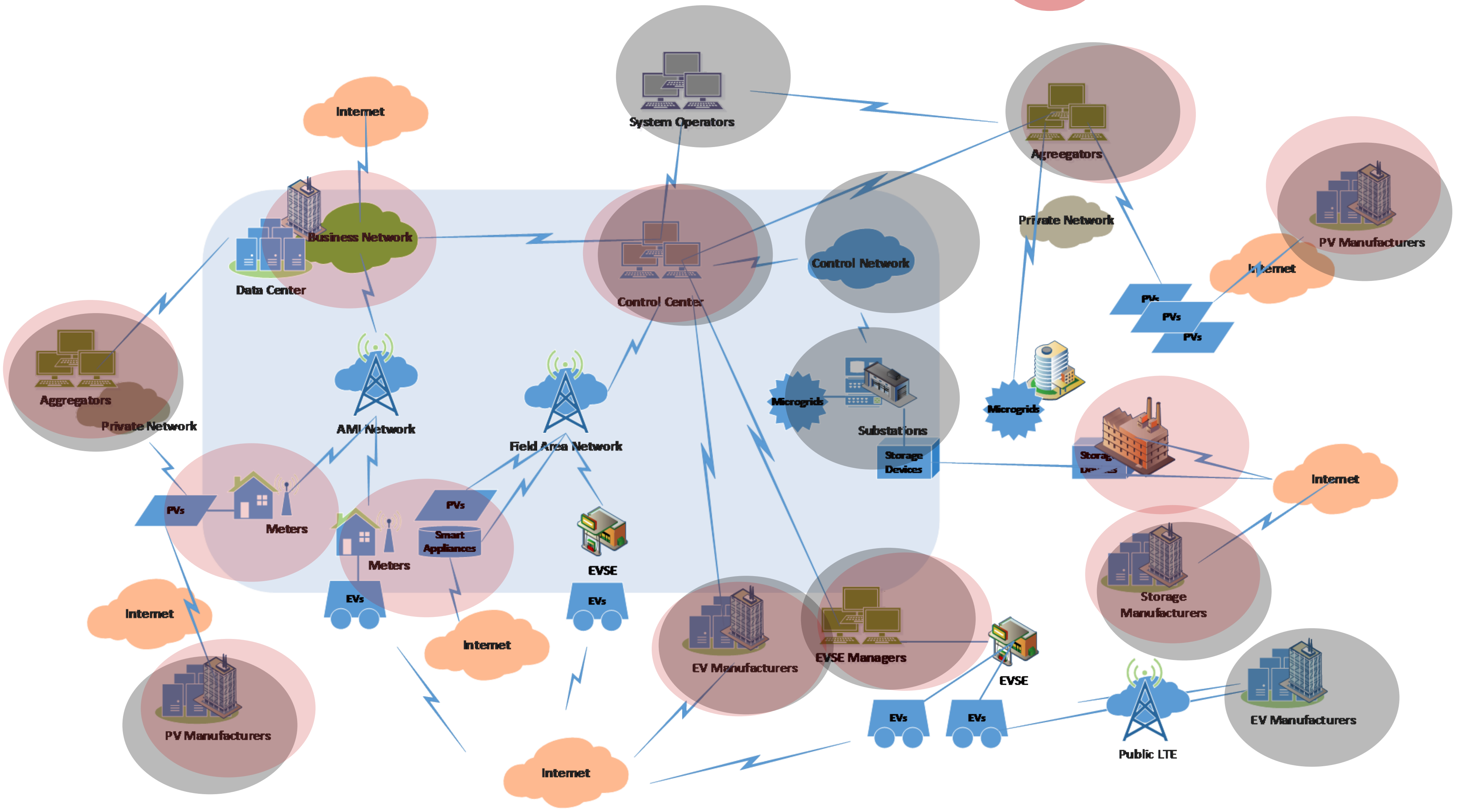
NISTIR 7628

- Communications Security (Traffic Encryption, Key Management, etc.)
- Privacy
- Vulnerability/Patch Management
- System Monitoring & Incident Response

Risk Profile – Near Future

High Impact (Customer Data or Grid Reliability)

High Exposure (Internet)



New Cybersecurity Considerations

- **Multi-party Grid**
  - Customers, 3-rd parties have increasing influence in how the power is generated and delivered
  - Devices / energy sources not owned by utility are connected to the grid
  - Who is responsible for cybersecurity?

- **Securing Emerging Technology**
  - Smart devices, sensors, smart appliances, IoT, EVs etc.
  - Not enough guidelines for **engineering cybersecurity** into these technologies

- **Securing the Ecosystem**
  - Securing things within the boundary of ownership may not be enough
  - Need to consider the risk that our assets or actions pose to the ecosystem
  - Security standards should capture the **cybersecurity responsibilities to the ecosystem**

Together…Shaping the Future of Electricity

Breakout Sessions

Main Room

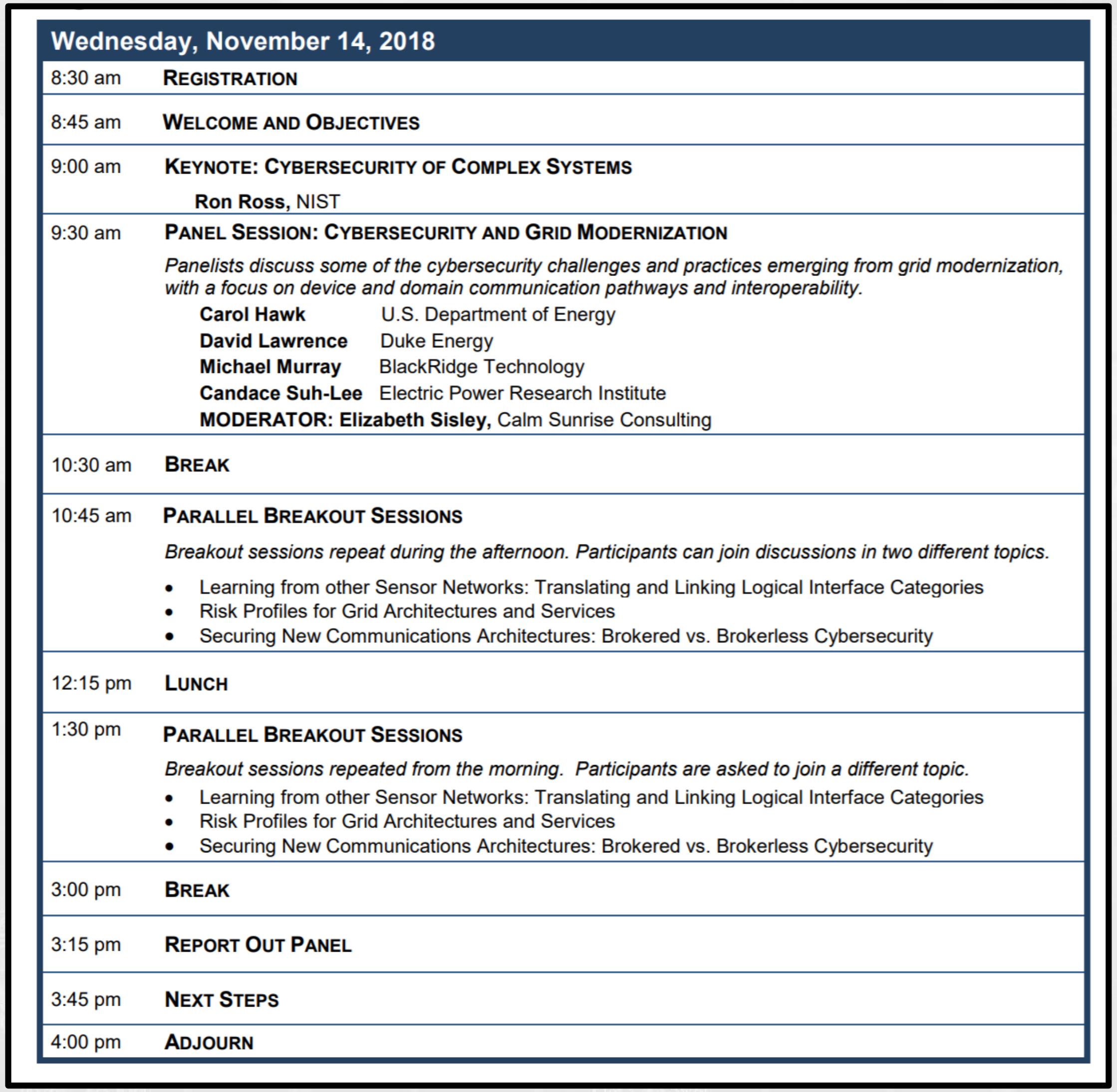
Breakout 1:
Learning from other Sensor Networks
-and-
Translating and Linking Logical Interface Categories

Middle Room

Breakout 3:
Securing New Comms Architectures, Brokered vs. Brokerless

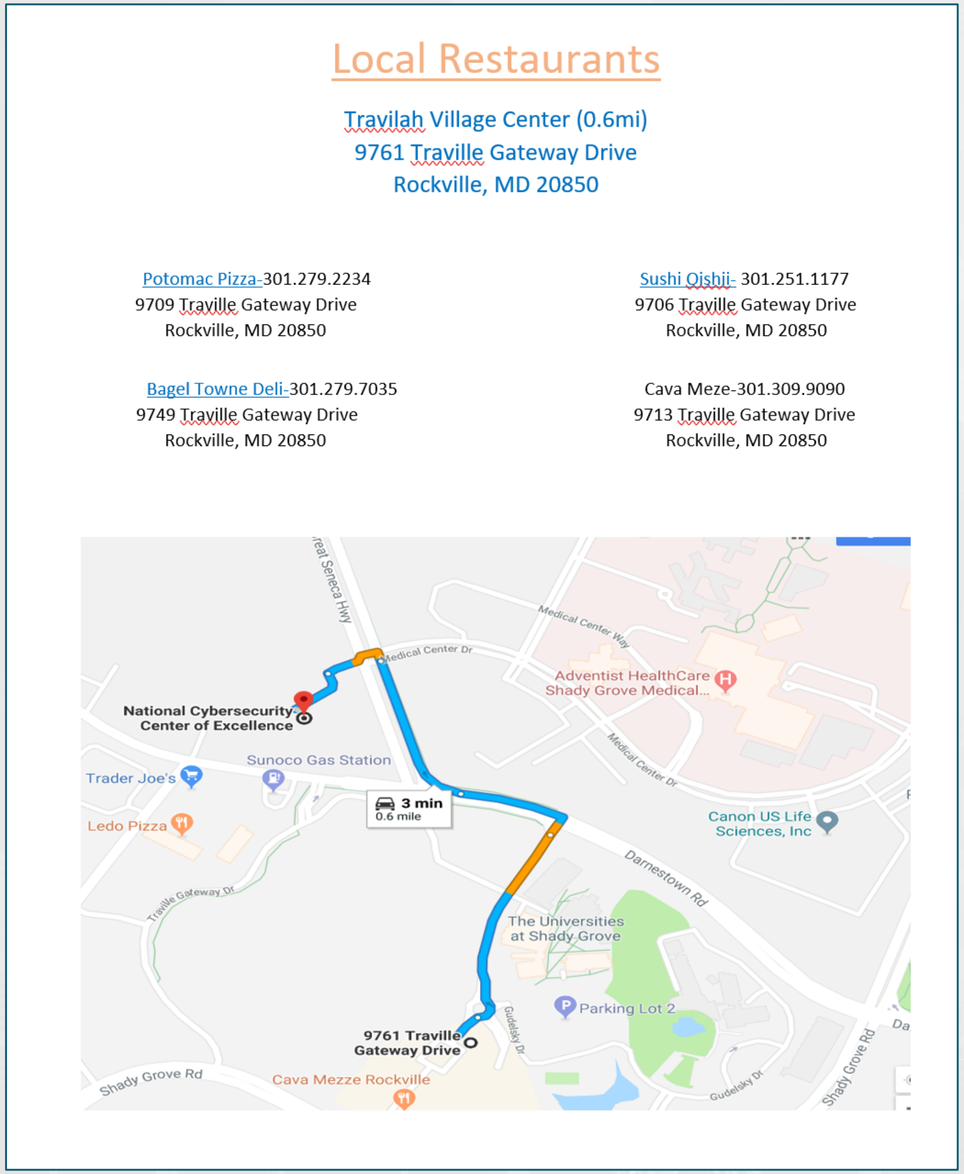
Far Room

Breakout 2:
Risk Profiles for Grid Architectures & Services



Wednesday, November 14, 2018	
8:30 am	**Registration**
8:45 am	**Welcome and Objectives**
9:00 am	**Keynote: Cybersecurity of Complex Systems** **Ron Ross**, NIST
9:30 am	**Panel Session: Cybersecurity and Grid Modernization** *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	**Break**
10:45 am	**Parallel Breakout Sessions** *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	**Lunch**
1:30 pm	**Parallel Breakout Sessions** *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	**Break**
3:15 pm	**Report Out Panel**
3:45 pm	**Next Steps**
4:00 pm	**Adjourn**

Lunch: 12:15-1:30



Local Restaurants

Travilah Village Center (0.6mi)
9761 Traville Gateway Drive
Rockville, MD 20850

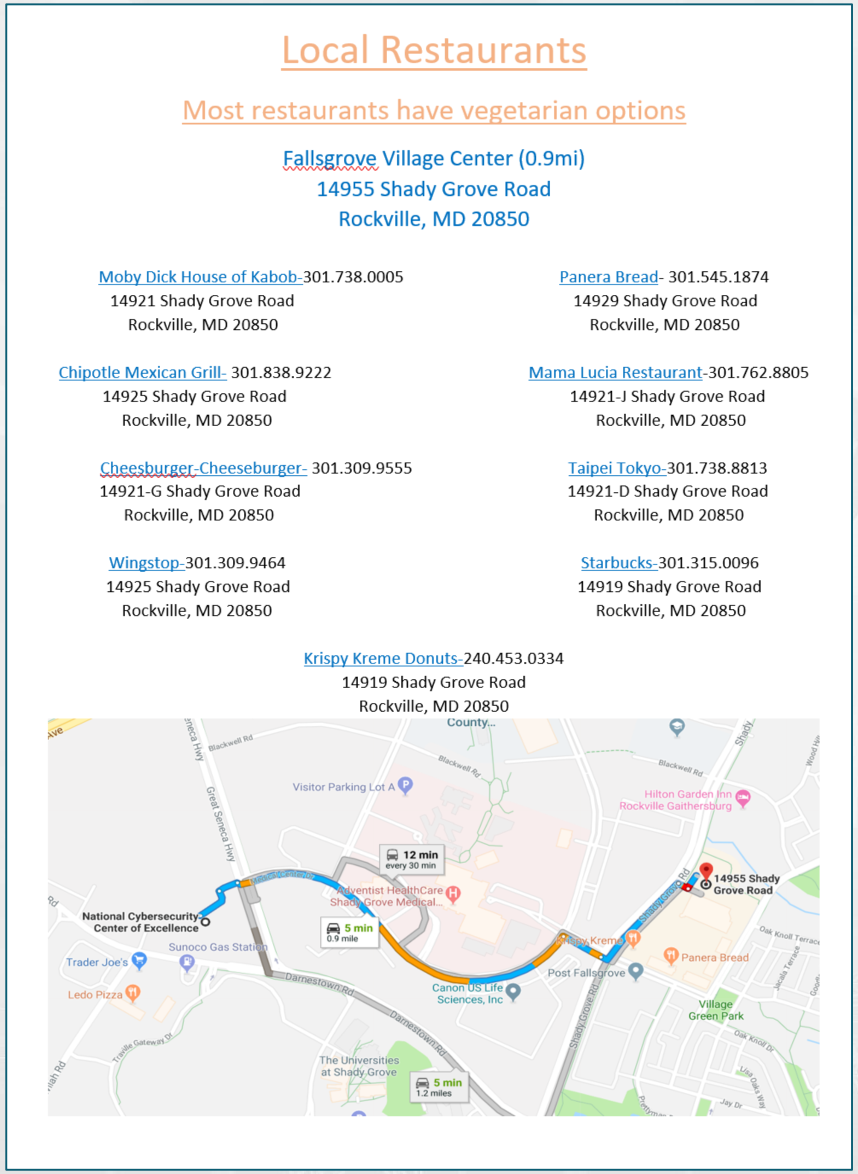
Potomac Pizza-301.279.2234
9709 Traville Gateway Drive
Rockville, MD 20850

Bagel Towne Deli-301.279.7035
9749 Traville Gateway Drive
Rockville, MD 20850

Sushi Qishii- 301.251.1177
9706 Traville Gateway Drive
Rockville, MD 20850

Cava Meze-301.309.9090
9713 Traville Gateway Drive
Rockville, MD 20850

Great Seneca Hwy
Medical Center Dr
Medical Center Way
Adventist HealthCare Shady Grove Medical...
National Cybersecurity Center of Excellence
Sunoco Gas Station
Trader Joe's
Ledo Pizza
3 min
0.6 mile
Medical Center Dr
Canon US Life Sciences, Inc
Darnestown Rd
Traville Gateway Dr
The Universities at Shady Grove
Parking Lot 2
Gudelsky Dr
9761 Traville Gateway Drive
Shady Grove Rd
Cava Mezze Rockville
Gudelsky Dr
Shady Grove Rd



Local Restaurants

Most restaurants have vegetarian options

Fallsgrove Village Center (0.9mi)
14955 Shady Grove Road
Rockville, MD 20850

Moby Dick House of Kabob-301.738.0005
14921 Shady Grove Road
Rockville, MD 20850

Chipotle Mexican Grill- 301.838.9222
14925 Shady Grove Road
Rockville, MD 20850

Cheesburger-Cheeseburger- 301.309.9555
14921-G Shady Grove Road
Rockville, MD 20850

Wingstop-301.309.9464
14925 Shady Grove Road
Rockville, MD 20850

Panera Bread- 301.545.1874
14929 Shady Grove Road
Rockville, MD 20850

Mama Lucia Restaurant-301.762.8805
14921-J Shady Grove Road
Rockville, MD 20850

Taipei Tokyo-301.738.8813
14921-D Shady Grove Road
Rockville, MD 20850

Starbucks-301.315.0096
14919 Shady Grove Road
Rockville, MD 20850

Krispy Kreme Donuts-240.453.0334
14919 Shady Grove Road
Rockville, MD 20850

Afternoon breakouts begin at 1:30pm

Breakout Sessions

Main Room

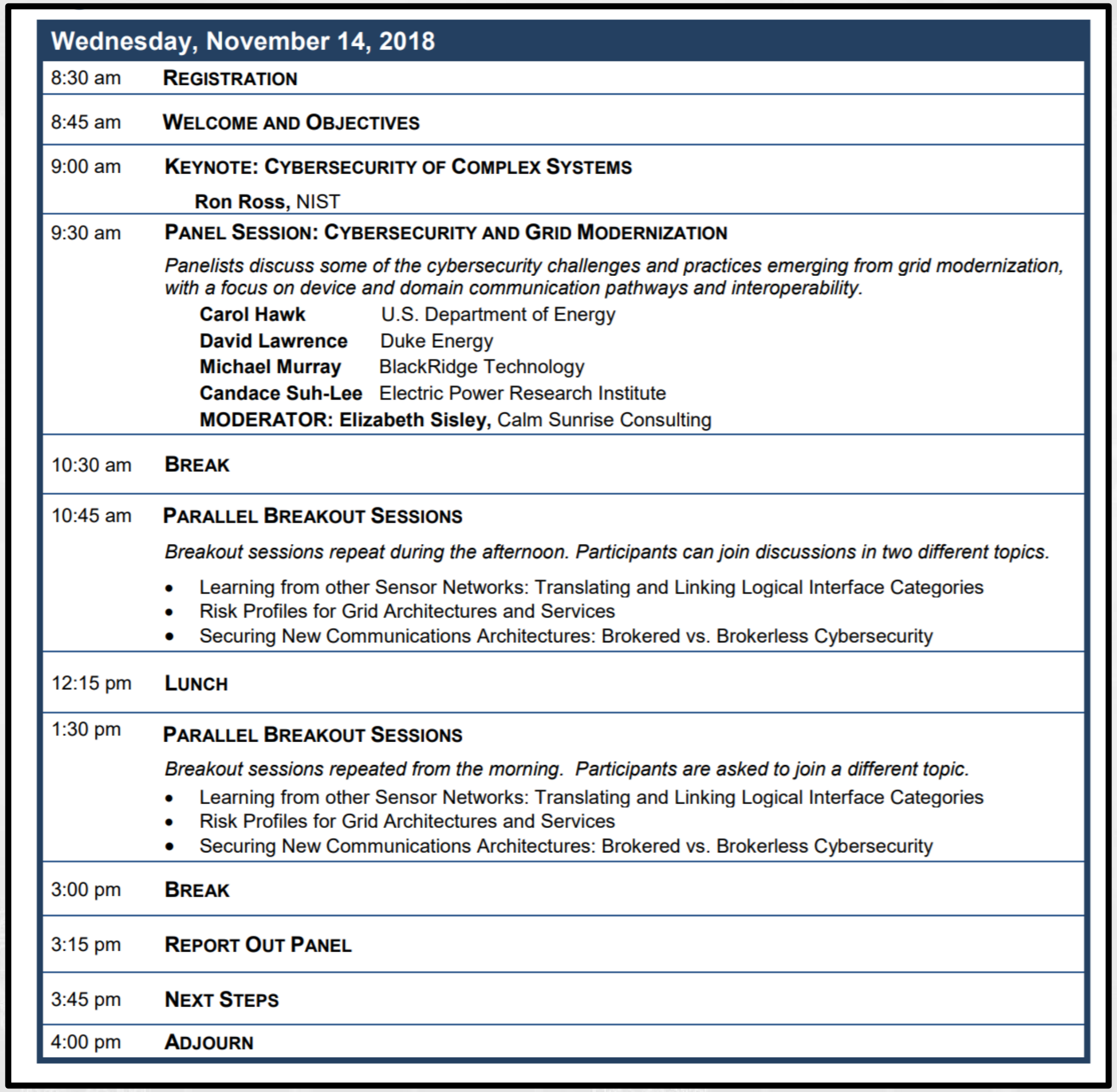
Breakout 1:
Learning from other Sensor Networks
-and-
Translating and Linking Logical Interface Categories

Middle Room

Breakout 3:
Securing New Comms Architectures, Brokered vs. Brokerless

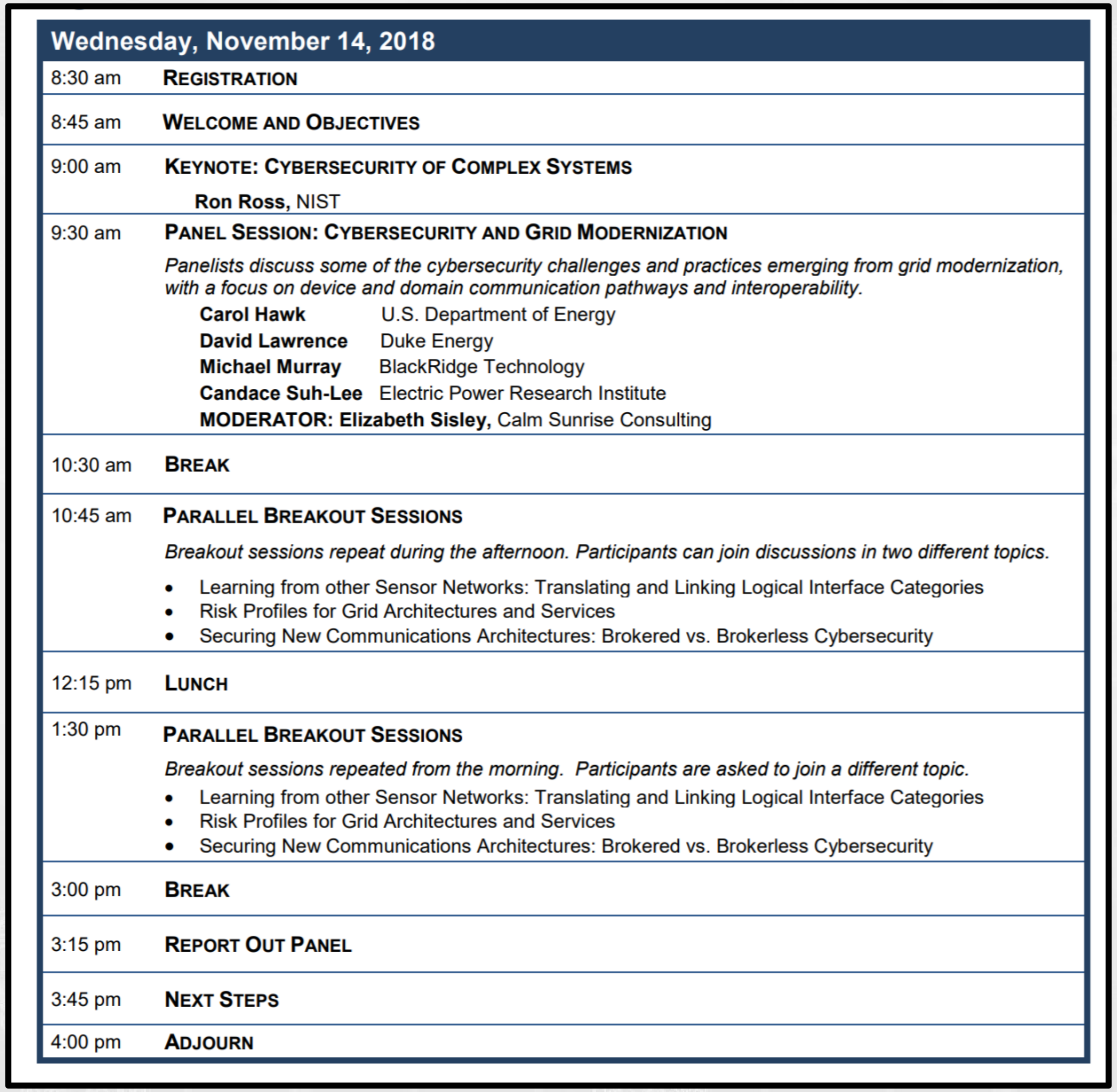
Far Room

Breakout 2:
Risk Profiles for Grid Architectures & Services



Wednesday, November 14, 2018	
8:30 am	**Registration**
8:45 am	**Welcome and Objectives**
9:00 am	**Keynote: Cybersecurity of Complex Systems** **Ron Ross,** NIST
9:30 am	**Panel Session: Cybersecurity and Grid Modernization** *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	**Break**
10:45 am	**Parallel Breakout Sessions** *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	**Lunch**
1:30 pm	**Parallel Breakout Sessions** *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	**Break**
3:15 pm	**Report Out Panel**
3:45 pm	**Next Steps**
4:00 pm	**Adjourn**

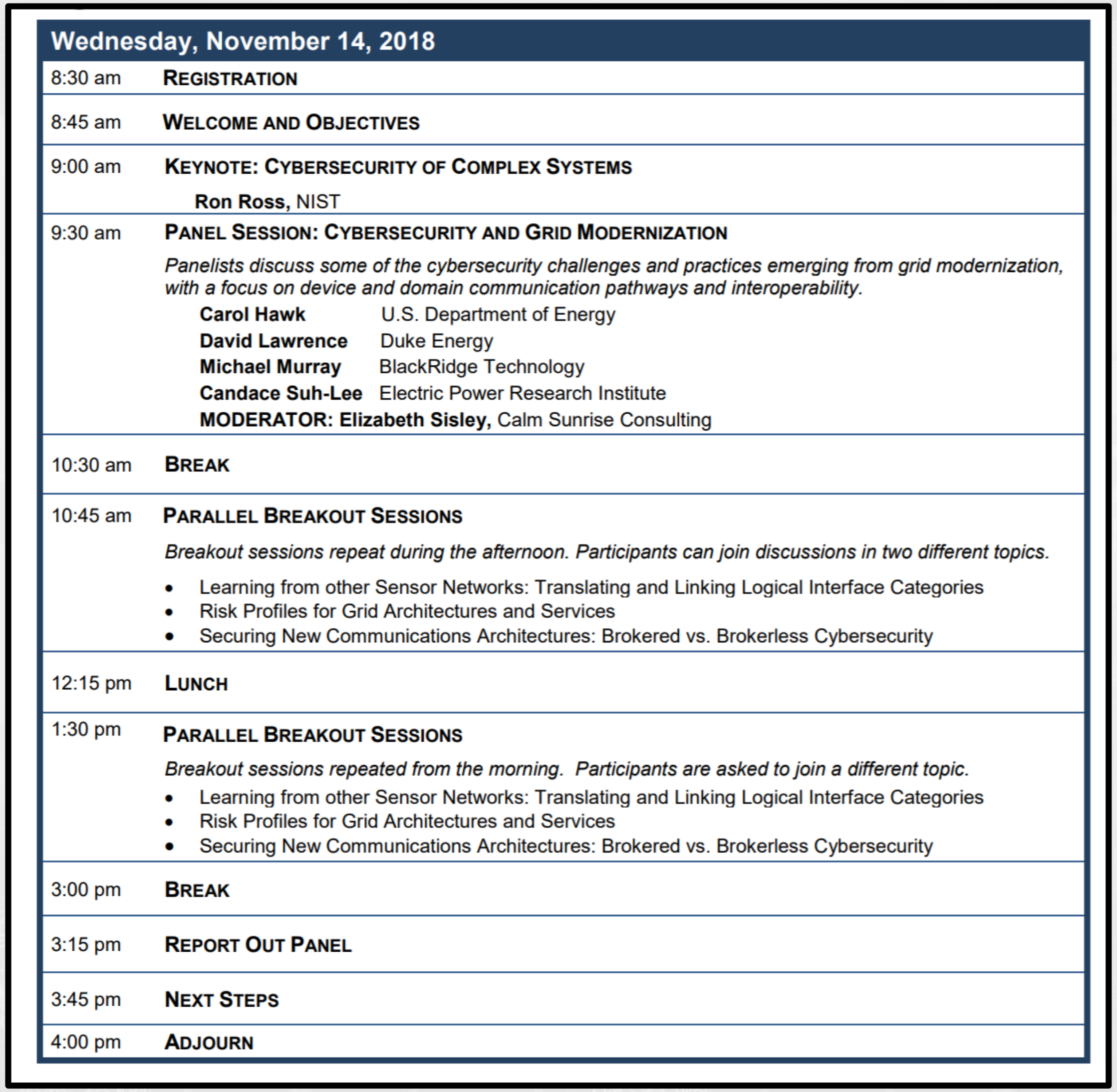
Report Out Panel



Wednesday, November 14, 2018

8:30 am	**Registration**
8:45 am	**Welcome and Objectives**
9:00 am	**Keynote: Cybersecurity of Complex Systems** **Ron Ross,** NIST
9:30 am	**Panel Session: Cybersecurity and Grid Modernization** *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	**Break**
10:45 am	**Parallel Breakout Sessions** *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	**Lunch**
1:30 pm	**Parallel Breakout Sessions** *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	**Break**
3:15 pm	**Report Out Panel**
3:45 pm	**Next Steps**
4:00 pm	**Adjourn**

Next Steps



Wednesday, November 14, 2018	
8:30 am	**Registration**
8:45 am	**Welcome and Objectives**
9:00 am	**Keynote: Cybersecurity of Complex Systems** **Ron Ross,** NIST
9:30 am	**Panel Session: Cybersecurity and Grid Modernization** *Panelists discuss some of the cybersecurity challenges and practices emerging from grid modernization, with a focus on device and domain communication pathways and interoperability.* **Carol Hawk** U.S. Department of Energy **David Lawrence** Duke Energy **Michael Murray** BlackRidge Technology **Candace Suh-Lee** Electric Power Research Institute **MODERATOR: Elizabeth Sisley,** Calm Sunrise Consulting
10:30 am	**Break**
10:45 am	**Parallel Breakout Sessions** *Breakout sessions repeat during the afternoon. Participants can join discussions in two different topics.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
12:15 pm	**Lunch**
1:30 pm	**Parallel Breakout Sessions** *Breakout sessions repeated from the morning. Participants are asked to join a different topic.* • Learning from other Sensor Networks: Translating and Linking Logical Interface Categories • Risk Profiles for Grid Architectures and Services • Securing New Communications Architectures: Brokered vs. Brokerless Cybersecurity
3:00 pm	**Break**
3:15 pm	**Report Out Panel**
3:45 pm	**Next Steps**
4:00 pm	**Adjourn**

Please provide written feedback

- Updated Conceptual Model:
  - https://www.nist.gov/document/draftsmartgridconceptualmodelupdatev3pdf
- Developing an Ontology for the Grid:
  - https://www.nist.gov/document/draftontologyforthesmartgridv2pdf
- Smart Grid Cybersecurity Risk Profile:
  - https://www.nist.gov/document/draftcsfsmartgridprofilepdf
- Logical Interface Categories for High-DER Scenario:
  - https://www.nist.gov/document/draftinterfacecategoriesassessmentpdf
- Overview of Pub/Sub Communications and Security Concerns:
  - https://www.nist.gov/document/draftpubsubsecurityaspectspdf
- Interoperability Profiles:
  - https://www.nist.gov/document/draftinteroperabilityprofiledescriptionfinalpdf
- Testing & Certification Landscape for Smart Grid Standards
  - https://www.nist.gov/document/drafttclandscapeevaluationfinalpdf

USE THIS EMAIL ADDRESS: smartgridframework@nist.gov

And more…

Upcoming Regional Roundtables:

- Providence: November 29, 2018

Additional documents will be posted soon:

https://www.nist.gov/engineering-laboratory/smart-grid/smart-grid-framework