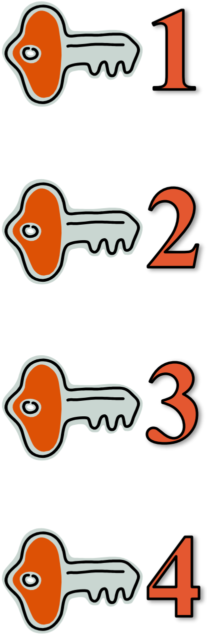
Power System Engineering, Inc.



Utility Cyber Security

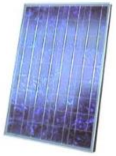
4 Key Areas You Need to Address

Jim Weikert
Jeff Simdon
Power System Engineering, Inc.
Web Site: www.powersystem.org

Agenda

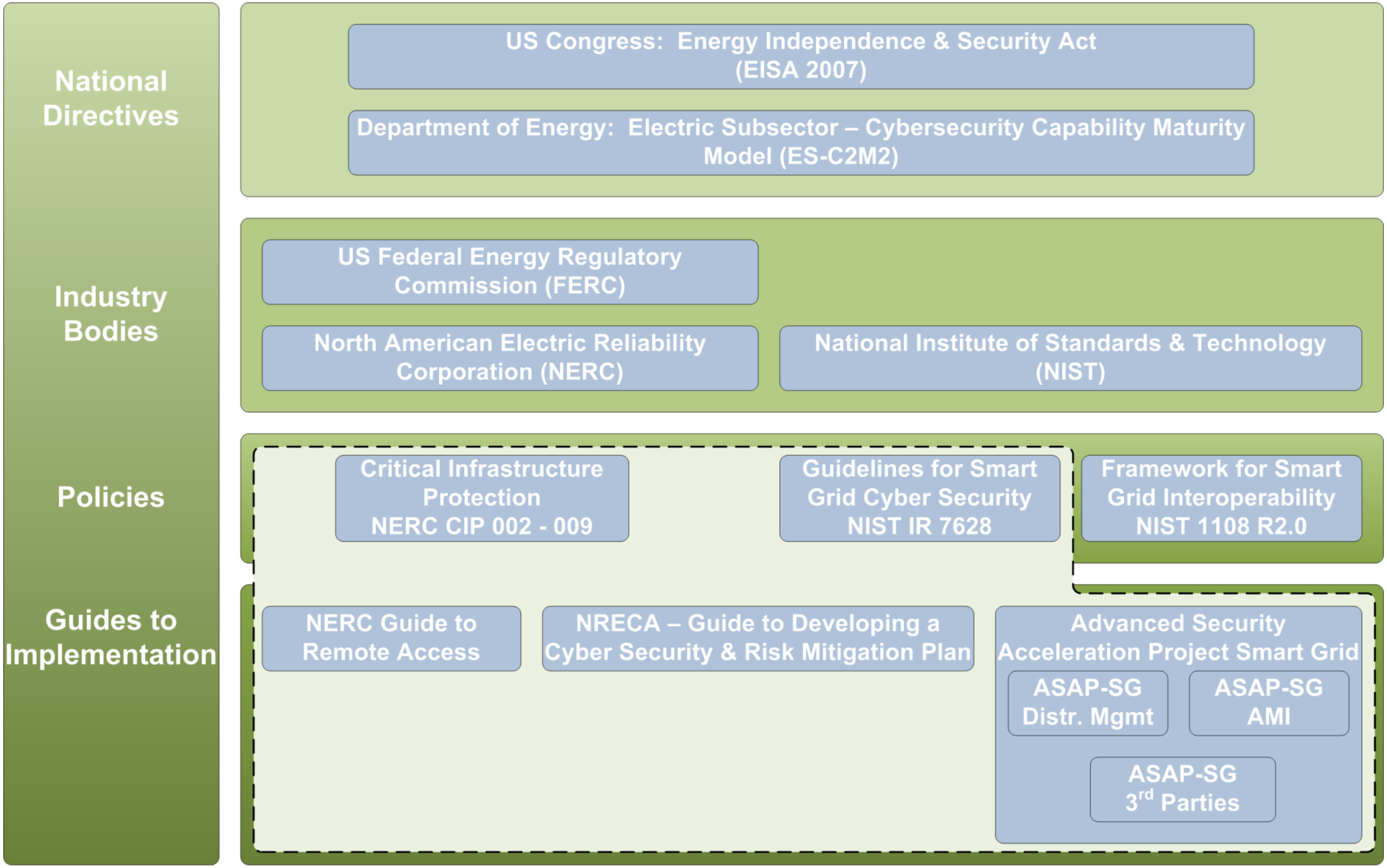
#	Topic
1	Introduction
2	1 Control System Security
3	2 Metering, MDM and Customer Information Security
4	3 Corporate System Security
5	4 Communications Infrastructure Security
6	Applying this to Your Utility

Increasing Role of Automation

Category	Scenarios	Category	Scenarios
AMI	Meter Reading, Prepaid Usage, Outage Detection…	Plug-in Electric Vehicle	Optimized Charging, Charging w/ DR, Price Signals…
Demand Response	Critical Peak Pricing, Real-time pricing, Net Metering…	Distributed Resources 	Customer Controlled, Utility DR controlled
Customer Interfaces	IHD Usage Info, Historical Data, View Pricing Info…	Transmission Operations	Real-time SCADA, Network Analysis, Synchro-phasors…
Electricity Market	Bulk Power Market, Retail Power, Carbon Trading…	RTO/ISO	Management of generation and storage.
Distribution Automation	Feeder Switching, Power Flow Analysis, FLISR…	Asset Management	Equipment Loading, Asset Replacement

Security is all about managing information flow.

Utility Sector Cyber Security Standards



National Directives

US Congress: Energy Independence & Security Act (EISA 2007)

Department of Energy: Electric Subsector – Cybersecurity Capability Maturity Model (ES-C2M2)

Industry Bodies

US Federal Energy Regulatory Commission (FERC)

North American Electric Reliability Corporation (NERC)

National Institute of Standards & Technology (NIST)

Policies

Critical Infrastructure Protection NERC CIP 002 - 009

Guidelines for Smart Grid Cyber Security NIST IR 7628

Framework for Smart Grid Interoperability NIST 1108 R2.0

Guides to Implementation

NERC Guide to Remote Access

NRECA – Guide to Developing a Cyber Security & Risk Mitigation Plan

Advanced Security Acceleration Project Smart Grid

ASAP-SG Distr. Mgmt

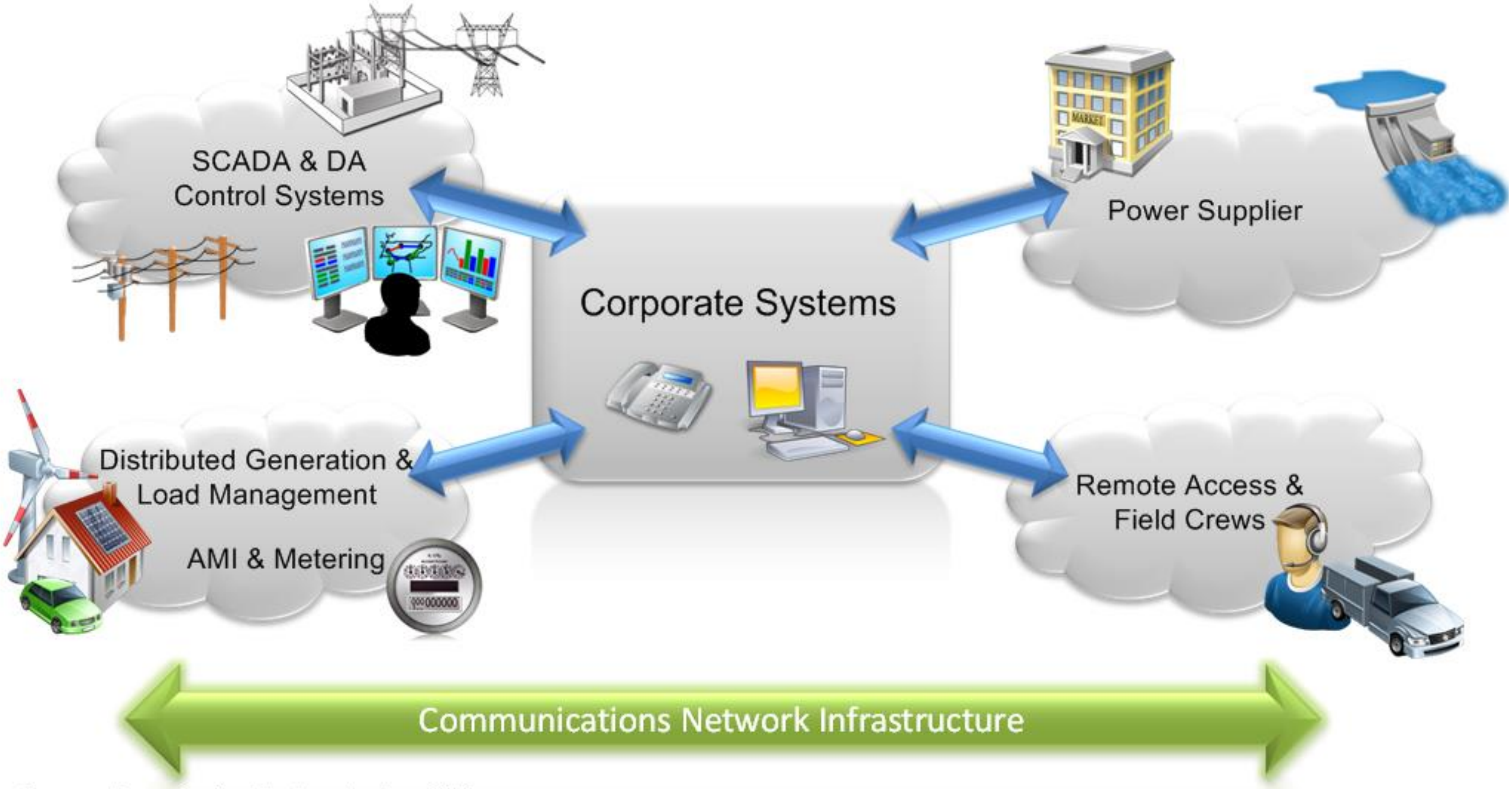
ASAP-SG AMI

ASAP-SG 3rd Parties

Source: Power System Engineering, Inc. 2012

Utility Cyber-Security Model

Each utility has to consider how these aspects of the Smart Grid intersect with its organization.



Source: Power System Engineering, Inc. 2012

NIST Cyber-Security Objectives

- ***Availability*** is generally considered the most critical security requirement, although the time latency can vary:
  - 4 milliseconds for protective relaying
  - Sub-seconds for transmission wide area situational awareness
  - Seconds for substation and feeder SCADA
  - Minutes for monitoring noncritical equipment and some market pricing
  - Hours for meter reading and longer term market pricing information
  - Days/weeks/months for collecting long-term data such as power quality
- ***Integrity*** is generally considered the second most critical security requirement
  - Data has not been modified without authorization
  - Source, time-stamp and quality of data is known and authenticated
- ***Confidentiality:*** least critical for power system reliability, but important for privacy:
  - Customer, electric market, and general corporate information

Security is centered around how information is handled.

Differing System Objectives

C	Confidentiality
I	Integrity
A	Availability

Category	Interface Category		Example	Impact		
				C	I	A
Control Systems and Equipment	1	High availability and with compute and/or BW constraint	SCADA feeder monitoring & control	L	H	H
	2	Not high availability, but with compute and/or BW constraint	Analyze system faults or devices	L	H	M
	3	High availability, but without compute and/or BW constraint	Direct Transfer Trip or Substation control	L	H	H
	4	Not high availability and without compute and/or BW constraint	Low priority data gathering	L	H	M
	5	Control systems within an organization	SCADA & Generation DCS	L	H	H
	6	Control systems in different organizations	G&T and Co-op SCADA or SCADA and ISO/RTO	L	H	M
Corporate	7	Back office systems under common mgmt.	CIS and MDMS Interface	H	M	L
	8	Back office systems under differing mgmt.	MDMS and 3rd party billing	H	M	L
	9	Business to business financial systems	Energy market transactions	L	M	M
Control and Corporate	10	Control & Corporate system interface	Work management system and GIS interface	L	H	M
Sensors	11	Sensors & collectors for measurement	Transformer temp. sensor	L	M	M
	12	Sensor networks and control systems	SCADA to sensors	L	M	M
Metering and Customer Information	13	Systems that use the AMI network	Meters and MDMS or Load Management and Customer	H	H	L
	14	AMI network systems with high availability	DRMS and Customer Distributed Energy Resources SCADA and DA over AMI	H	H	H
	15	Systems using customer networks (HAN)	Customer Appliances	L	M	M
	16	External systems & customer site	Energy provider & DER Customer and CIS website	H	M	L
Inter-system Connections	17	Mobile Field Crew Interfaces	OMS, GIS, SCADA…	L	H	M
	18	Between metering equipment	Meters & MDMS, Field Crews, DER…	L	H	L
	19	Operations decision support systems	WAMS & ISO/RTO	L	H	M
	20	Engineering and Control Systems	Relay settings, Oscillography	L	H	M
	21	Control systems and vendors	Vendor Remote Access	L	H	L
	22	Network Management Systems	SNMP to network devices	H	H	H

Each system has unique requirements.

Beyond Electronic Security

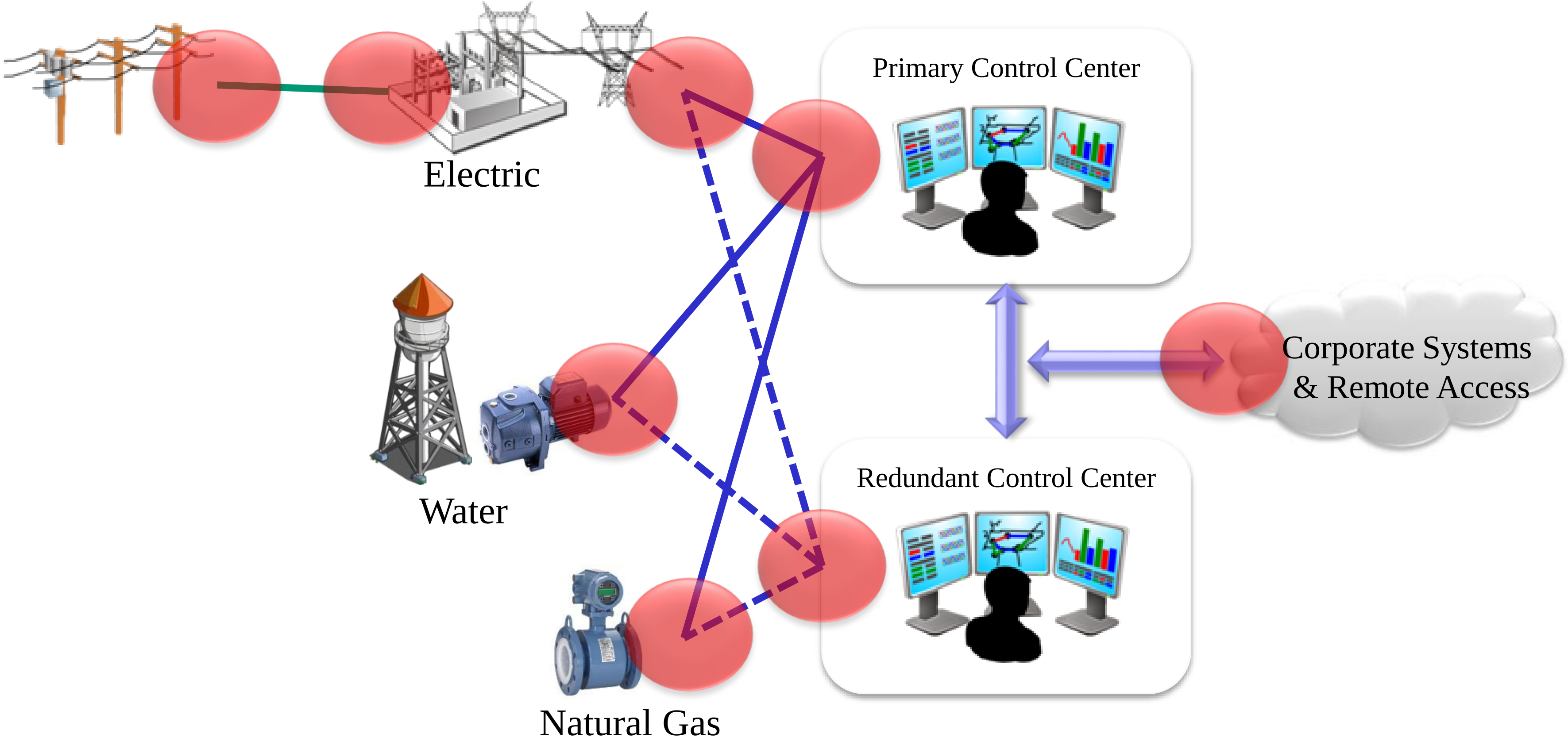
Tools	Addresses
Training	Awareness of how to use security measures
Social Engineering	Avoid inadvertent personnel mistakes
Contingency Planning and Incident Response	Plans for what to do when something goes wrong.
Physical Access Control	Limit those who have physical access
Contractor and Vendor Access	Avoid others compromising your system
Information Mgmt. and Protection	Keeping settings, passwords, and info safe
Patch Management	Test changes carefully to avoid compromises
Logging of activity	Keeping track of possible incidents

Cyber security does not rely solely on electronic tools.

Agenda

#	Topic
1	Introduction
2	🔑1 Control System Security
3	🔑2 Metering, MDM and Customer Information Security
4	🔑3 Corporate System Security
5	🔑4 Communications Infrastructure Security
6	Applying this to Your Utility

System Components and Exposure Points



Distributed Resources

Stations

Control Centers

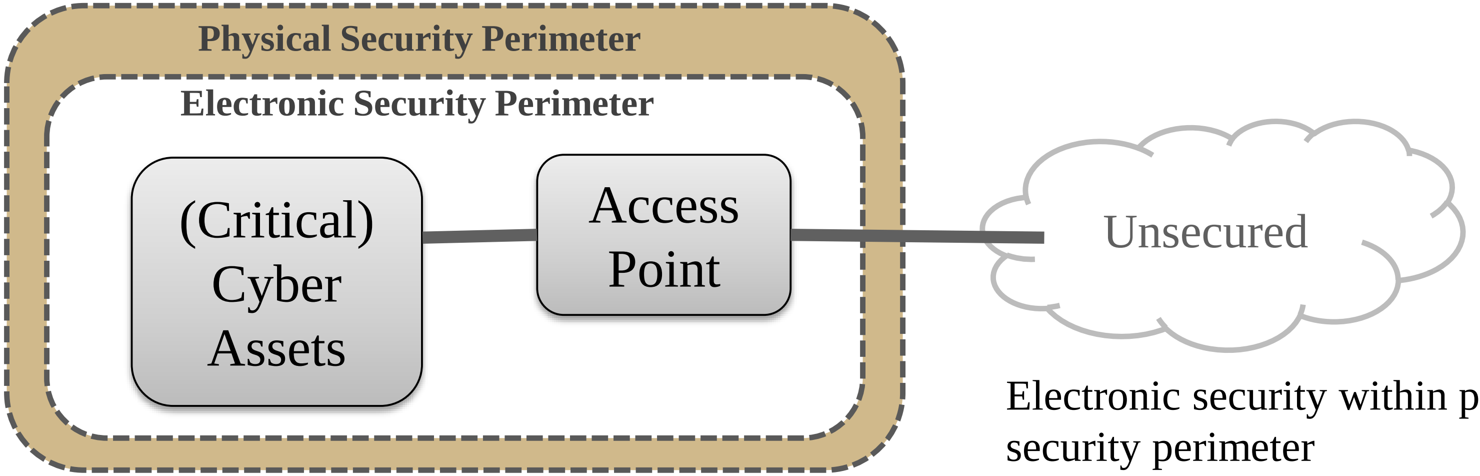
The system has many components and exposure points.

Control System Security Objectives

- Control as opposed to information
  - Availability and Integrity: Main objective is system performance
  - Information: Low impact of disclosure of information
- Security at all levels
  - Prevention: Encryption and Authentication prevent access
  - Detection: Monitor boundaries and alert system operators
  - Contain: Limit extent of control if access is gained
  - Repair: Pre-define processes to restore or manually operate
- Inter-system
  - Interfaces to OMS and AMI are critical to secure well

Prevention is not the only step to maintaining availability.

Substation ESP Security



Confidentiality:	L
Integrity:	H
Availability:	H

Electronic security within physical security perimeter

Protection	Description	Tool
Traffic Limitation	Only allow specific types of packets	Firewall
Packet Inspection	Monitor traffic for viruses and malware	
Unroutable	Prevent access from this substation to another	Tunnel
Encryption	Scramble bytes to prevent someone from reading	VPN
Integrity	Detect if any of the bits are changed or replayed	
Authentication	Make sure only allowed users / computers access	

Many options to layer for substation security.

Distribution Automation Security

Confidentiality:	L
Integrity:	H
Availability:	H

- DA Sites pose unique challenges
  - Outside of physical security of substations
  - Openings to system
  - Limited capability devices lack strength of substation ESP devices

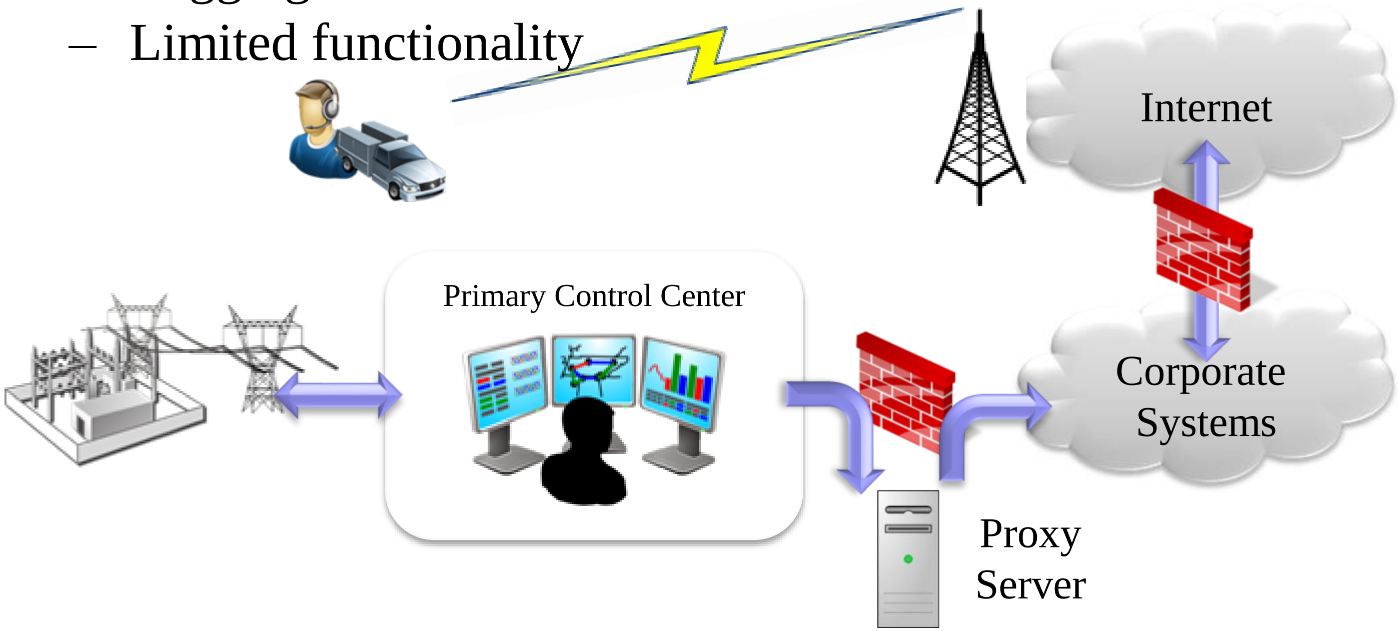
- Solutions
  - Tunnels: back to system to limit access to other resources
  - Authentication: in device to prevent unintended activation or modification
  - Authentication: run VPN tunnel or DNP 3 v5 to require authentication to host
  - Traffic Inspection: at collector to avoid injected viruses, etc.
  - Device limitation: at DA site and collector, simple measures to limit devices which can connect

Close the back door on your security system.

Corporate and Remote Access

Confidentiality:	L
Integrity:	H
Availability:	M

- Worker access to information requires careful design.
  - Public networks (i.e. cellular) for data access
  - Layer protection through corporate and public networks
  - Strong authentication of remote users
  - Protection of control system through proxy servers
  - Logging of access
  - Limited functionality



Extend your system to the field with care.

Steps to Securing your Control System

- **Electronic** measures
  - ESPs inspect incoming traffic and secure outgoing traffic
  - Inspect traffic to DA sites and limit system exposure
  - Crews receive remote access through a controlled manner
- **People and procedural** measures
  - Senior manager in charge of security around your SCADA system
  - Inventory of equipment and access rights for personnel
  - Operators trained on disaster recovery plans
  - Test system updates before deploying them
  - Physical security to control center, substations and DA points
  - Background checks on contractors before allowing access
  - Maintenance crews given restricted access

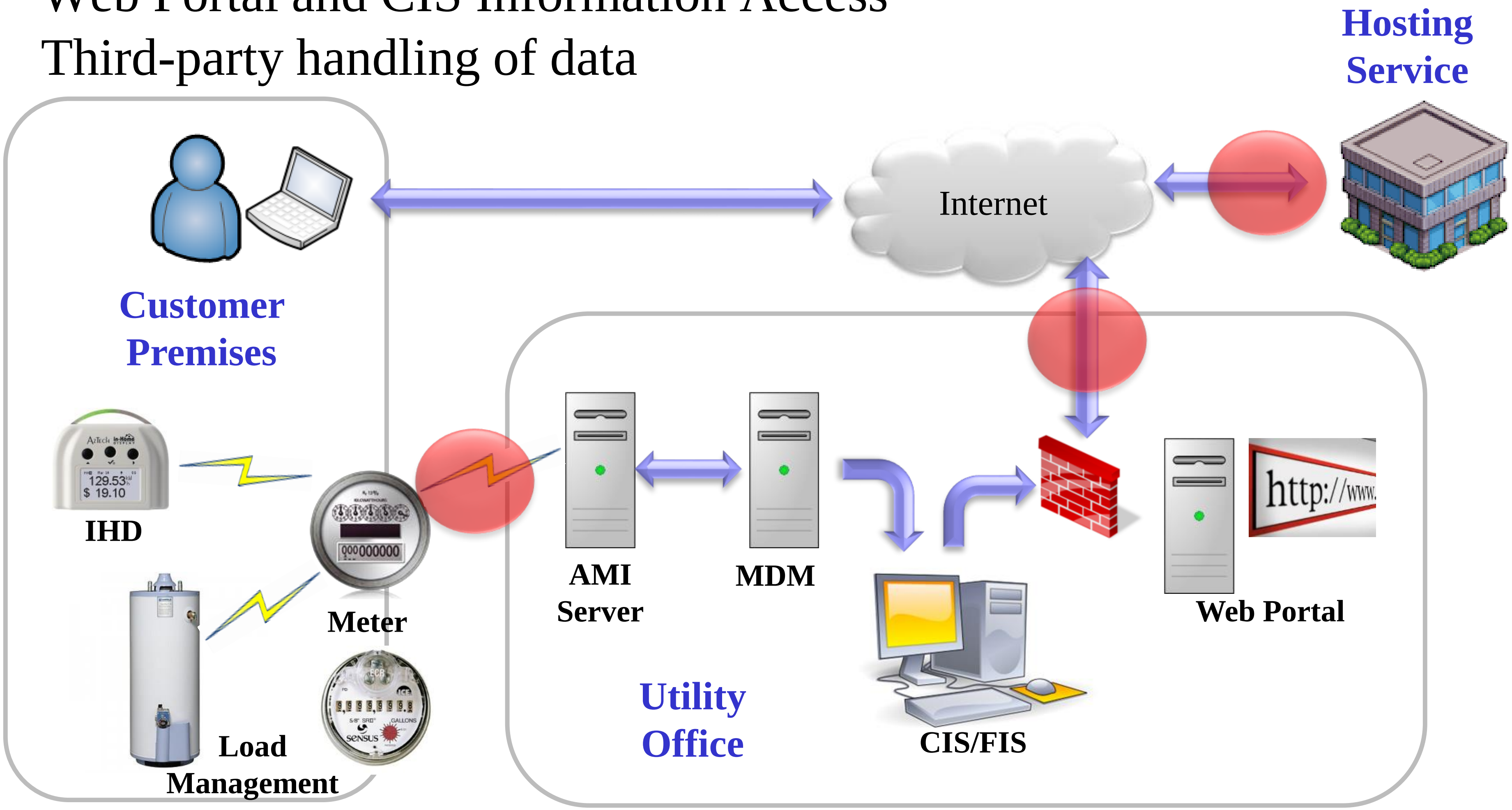
Foundational measures are an important first step.

Agenda

#	Topic
1	Introduction
2	1 Control System Security
3	2 Metering, MDM and Customer Information Security
4	3 Corporate System Security
5	4 Communications Infrastructure Security
6	Applying this to Your Utility

Metering, MDM, and CIS System Components

- Meter and AMI Infrastructure
- Web Portal and CIS Information Access
- Third-party handling of data



Metering and In-home Displays

Confidentiality	H
Integrity	H
Availability	L

- Metering Data gathered into the AMI
  - Integrity: Trustworthiness of data
    - Use for billing (both from customer tampering as well as others)
    - Use MDM VEE (validate, edit, evaluate) to filter for missing, erroneous reads
  - Confidentiality: as information is gathered, meter identification shouldn't identify customer by GPS, street address or name
  - Availability: Metering data can typically be gathered as available
- Customer usage information to IHDs
  - Confidentiality concern as billing information is relayed back to customer premises
- Security Activities

Tool	Addresses
Encryption	Interception of meter data
MDM and VEE	Erroneous data into CIS
Meter seals	Physical meter tampering
Authentication	Restricted changes to meters
Firewall	Protect corporate network
AMI Server Configuration	Denial of Service

Trust the data from your AMI and keep it confidential.

Load Management

Confidentiality:	L
Integrity:	H
Availability:	M

- Sometimes through AMI network, sometimes through separate network
- Primary concern is secure control
  - Confidentiality: Low
  - Integrity: High
    - Avoid turning off customer equipment
    - Re-enabling customer equipment can incur significant peak charges or overload the distribution or transmission systems
  - Availability:
    - Important to avoid charges, but known outages can be addressed
- Security Activities

Tool	Addresses
Encryption	Interception of meter data
Status Information	Verification of switch status
Firewall	Protect corporate network

Protect both re-enabling as well as disabling of loads.

Web Portal & Customer Access

Confidentiality:	H
Integrity:	M
Availability:	L

- Information confidentiality is the biggest concern
  - Customer usage information
  - Customer bill-pay (credit and banking information)
- Often 3rd parties are involved for customer data and billing
  - Choose vendors carefully and understand their security policies.
- Security activities

Tool	Addresses
Web Logging and Review	Detect attempted breaches or misuse
Secure Socket Layer	Secure web transactions
Password Management	Avoid password abuse (guess or discovery)
Vendor analysis	Secure hosting of web data
Internal Logging & Review	Detect attempted breaches or misuse
Proxy Server	Prevent access to CIS and FIS systems

Secure transactions to protect financial and usage information.

Steps to Securing your Metering System

- **Electronic** measures
  - Meters aren’t identified by customer information.
  - External access to the AMI server is restricted.
  - MDM checks for erroneous data before it enters CIS.
  - Load Management activities are monitored.
  - Secure web portal for customer access.
- **People and Procedural** measures
  - Senior manager in charge of security around your metering system.
  - Inventory of equipment and access rights for personnel.
  - Operators trained on disaster recovery plans.
  - Test system updates before deploying them.
  - Physical security to meters, collectors, and servers.
  - Background checks on contractors before allowing access.
  - Maintenance crews given restricted access.

Foundational measures are an important first step.

Agenda

#	Topic
1	Introduction
2	🔑1 Control System Security
3	🔑2 Metering, MDM and Customer Information Security
4	🔑3 Corporate System Security
5	🔑4 Communications Infrastructure Security
6	Applying this to Your Utility

Corporate Network Considerations

Confidentiality:	H
Integrity:	M
Availability:	L

- Corporate network has more interfaces to different segments with different security requirements
- Corporate network has more connections to the Internet making it harder to secure
- Increasing customer demand for access to information increases risk exposure
- Segmentation and management of traffic is important to managing traffic between interfaces

Customer Information (CIS)	Financial System (FIS)
Telephone	Interactive Voice (IVR)
Geographic Information (GIS)	Engineering Analysis
Work Order Management	Mobile Workforce Mgmt. (MWM)
Automatic Vehicle Location (AVL)	

Greater number of systems makes confidentiality a challenge.

Principles of Network Security

- Network security is insuring that all activity is desired and originates from authorized entities
  - An accounting for 100% of all activity on 100% of the devices
- Grant "least privilege" to users and applications
  - Give entities no more than the minimum access they need to accomplish the task to prevent unintended accesses
- Use a "defense in depth" strategy
  - Design your strategy around a series of layers to prevent one exploit to compromise the whole
- Use the technique of "resource isolation"
  - Compartmentalization of resources so that activities can be isolated and tracked

Balance between layered security and impeding productivity.

Isolation & Segmentation Methods

- Physical segmentation is the most secure but not always practical
  - Each system is on its own physical connection
  - TCO for infrastructure is high
  - Mobility requirements
- Virtual segmentation (VPN) involves cryptology management and updates
  - Use of encryption to pass the traffic through less secure environments
- Logical segmentation (VLAN) can decentralize the management of your networking devices
  - Use of encapsulation to separate traffic in the same environment

Each technology offers different benefits.

Embedded Application Security

- Traffic isolation and management is important, but not the whole story.
- Applications have their own set of security concerns
  - Authentication
  - Data storage (data at rest)
  - Remote access
- Many have mechanisms for secure remote access
  - HTTPS and SSL
  - Not all do

Start by utilizing the security tools offered by the software.

Managing Access to Insecure Applications

- Securing applications that may not be inherently secure:
  - VPNs
  - Proxy Devices
  - Terminal Services
- Legacy MWM example:
  - By leveraging Terminal Services through a VPN, a legacy application can be given secure mobility.

Use additional tools to complement software as needed.

Steps to Securing your Corporate Systems

- **Electronic** measures
  - Utilize security measures inherent in applications
  - Create “Defense in Depth” using multiple security mechanisms jointly.
  - Apply “Least Privilege” principles to restrict access to many systems.
- **People and Procedural** measures
  - Senior manager in charge of security around your corporate system.
  - Inventory of equipment and access rights for personnel.
  - Operators trained disclosure of information.

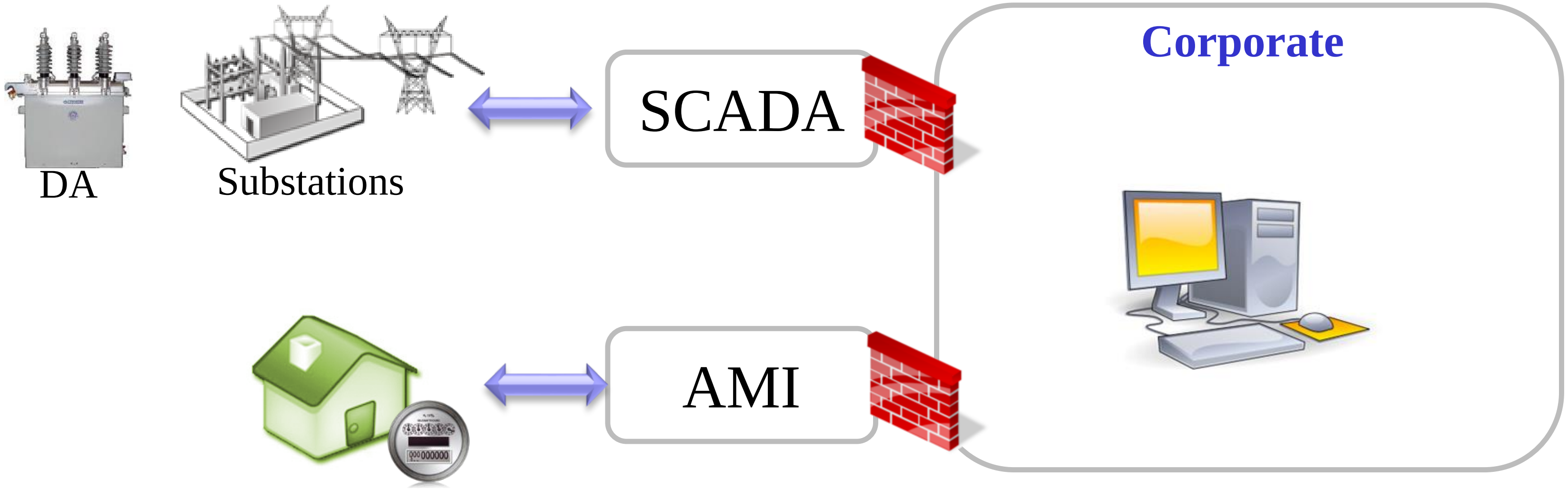
Corporate systems are the hub to all automation programs.

Agenda

#	Topic
1	Introduction
2	🔑1 Control System Security
3	🔑2 Metering, MDM and Customer Information Security
4	🔑3 Corporate System Security
5	🔑4 Communications Infrastructure Security
6	Applying this to Your Utility

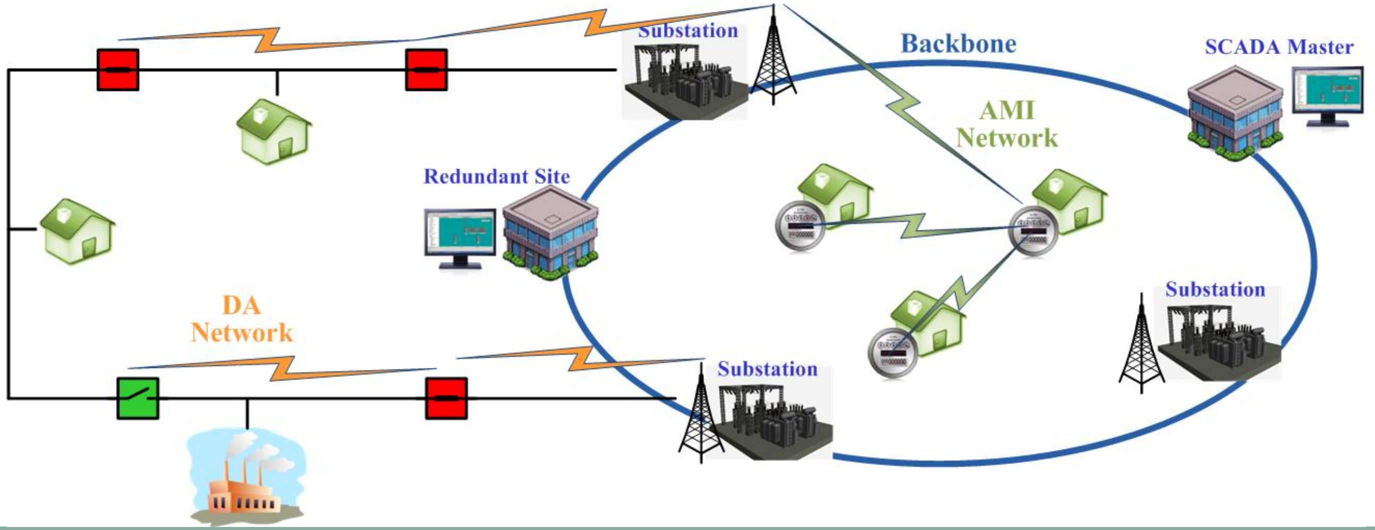
Segmentation Principles

- Isolate traffic between systems: corporate, SCADA & DA, AMI
  - Physical segmentation: physical connections
  - Virtual segmentation: VPN or similar encryption tunnel to segment
  - Logical segmentation: VLAN or similar packet tagging to segment
- Restrict, authenticate and monitor traffic at access points
  - Follow “least access” principle for restriction
  - Users restricted to certain networks and devices
  - Access points monitored



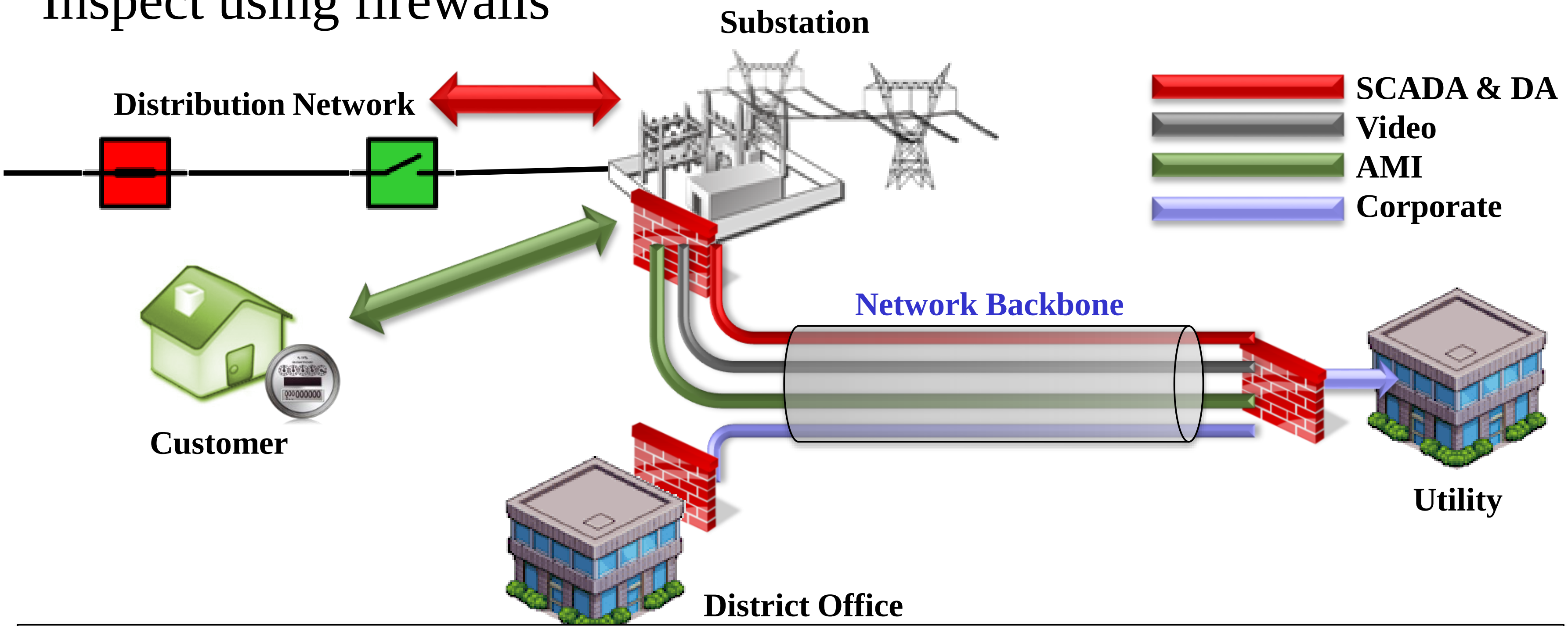
Multi-Tier Infrastructure

Tier		Description	Speed	Coverage	Redundancy
1	Backbone	Connect offices and most substations	High speed 10-100+ Mbps	Ring	Critical
2	Backbone Extension	Connects remote substations	Medium speed 10+ Mbps	Point-to-point	Preferable
3	DA Network	Connect field DA equipment to each other and to a collection point to the SCADA system.	Lower speed 50 kbps to 1 Mbps	Wide-area	Preferable
4	AMI Network	Connect meters to each other and to a collection point.	Lower speed <50 kbps to 1Mbps	Wide-area	Preferable



Multiple Systems

- Different systems operate over common network backbone
- Need to follow principle of “least access” to avoid cross-system access
- Segment using VLANs or VPNs
- Inspect using firewalls



Maintain security end-to-end even over a common backbone.

Agenda

#	Topic
1	Introduction
2	🔑1 Control System Security
3	🔑2 Metering, MDM and Customer Information Security
4	🔑3 Corporate System Security
5	🔑4 Communications Infrastructure Security
6	Applying this to Your Utility

4 Key Area Summary

1 **Control System**: Secure field points as well as substations, wells and control centers. Carefully manage system updates to avoid adding system weaknesses.

2 **Metering & Customer Information**: Don’t expose corporate networks through insecure AMI server and web portal access.

3 **Corporate Systems**: Layer security embedded in applications with good network structure and personnel access.

4 **Communications Infrastructure**: Maintain network security and segmentation from the corporate office to the field devices.

Applying this to Your Utility

- Assess your network and procedures
  - A good cyber security program starts with knowing what you have and accounting for all activity
- Identify gaps and weaknesses
- Assess the risk
- Prioritize remediation
- Monitor the results and periodically reassess

PSE’s Utility Cyber Security Assessment Methodology

Step 1: Discovery

- Request for Information
  - Hardware Inventory
  - Network Diagrams
  - Software Systems
  - Security Questions
- Interview
  - Overall Program
  - Policies and People
  - Processes
  - Technology
- Investigation
  - Network Settings
  - Platforms (Servers, …)
  - Devices (IEDs, …)
  - Logging (Detection)
  - Test for holes (staff and equipment)

Step 2: Assessment

- Assessment
  - System Security Model

    (Functional groups, data flow, interfaces, control, logging)
  - Risk Assessment

    (Risk tolerance of utility, impact of loss)

Step 3: Plan

- Recommendations
  - Prioritize initiatives
  - Propose system changes and guidelines
  - Propose recommendations by security area
  - Provide budget for recommended plan
  - Provide a schedule for the recommended plan

Thank You

Power System Engineering, Inc.

Jim Weikert
Lead Utility Automation Consultant
Direct: 608-268-3556
Mobile: 608-206-3753
Email: weikertj@powersystem.org

Jeff Simdon
IT & Security Consultant
Direct: 608-268-3561
Mobile: 608-443-8337
Email: simdonj@powersystem.org

www.powersystem.org