

GE Energy

Smart Grid Cyber Security

John D. McDonald, P.E.
GM, T&D Marketing

IEEE PES Past President
IEEE Division VII Director
IEEE Fellow

The Smart Grid




POWERING POTENTIAL




What is a Smart Grid?

The integration of two infrastructures ... to provide customer value



Electrical infrastructure




Information infrastructure

Increases energy efficiency and operational productivity

Increases power system reliability and quality of service

Empowers everyone to meet environmental objectives

An Integrated 'Systems' Solution to a Complex Set of Challenges



The Power Delivery System of the Future Must Have Advanced Capabilities

To achieve benefits identified by stakeholders, the intelligent grid must be:

- Self-Healing** and **Adaptive** to correct problems before they become emergencies
- Interactive** with consumers and markets
- Optimized** to make best use of resources and equipment
- Predictive** rather than reactive, to prevent emergencies ahead rather than solve after
- Distributed assets and information** across geographical and organizational boundaries
- Integrated** to merge all critical information
- More Secure** from threats from all hazards

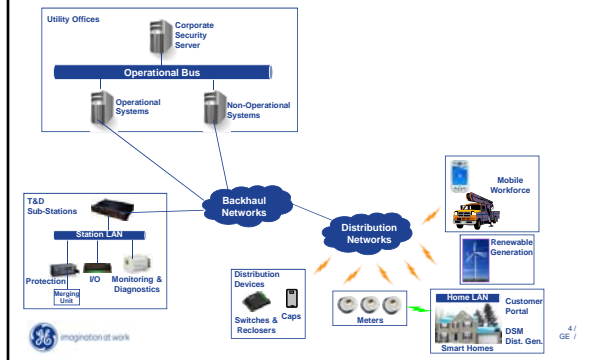


Enabling The Power Delivery System of the Future
Don Von Dollen - EPRI IntelliGrid, April 6, 2009





Smart Grid Simplified Architecture



Cyber Security Standards NERC CIP

"To reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets (computers, software and communication networks) that support those systems."



Network Security

NERC Cyber Security (Draft 4 approved)

- CIP-002-01 Critical Cyber Assets
- CIP-003-01 Security Management Controls
- CIP-004-01 Personnel & Training
- CIP-005-01 Electronic Security
- CIP-007-01 Physical Security
- CIP-008-01 Systems Security Management
- CIP-009-01 Incident Reporting and Response Planning

<http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html>





Secure Substation Architectures

Key NERC Security Requirements:

- Define Critical Cyber Assets
- Define & Create Electronic Security Perimeters
- Provide Support Dial-up and/or Wide Area Networks
- Track and Report Access by User – Audit Trail of Success or Failure
- Remove User Access (in 24 hours) for Termination for Cause
- Provide for User Access Rights – Gateway & IEDs
- Strong Two Factor User Authentication for Interactive Access
- Disable Unused Ports And Services
- Appropriate Use Banner
- Malicious Software Prevention

Other Common Security Requirements:

- Support access to SCADA and Non-SCADA Data
- Communication Line Encryption
- Support Centralized Security Management



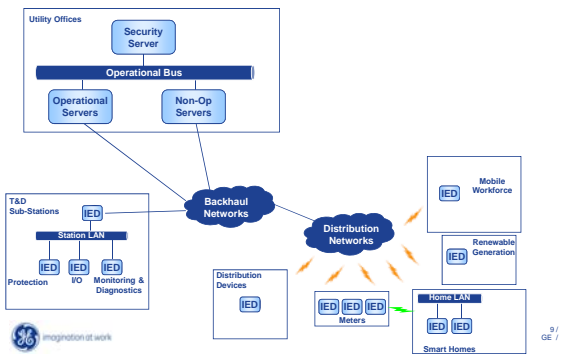
Failure Mode and Effects Analysis of Security

1. Function: Describe the function to be analyzed to secure against a specific cyber incident.
2. Failure Mode: Understanding the threat
3. Failure Causes: Understanding the types of attacks
4. Identify Failure Effects and Criticality: How serious are the consequences
5. Understand Solutions: What are the current methods of securing against the attack?
6. Match solution to analysis: Establish a Security system to match the analysis



8 / GE /

Simplified Smart Grid Architecture





Smart Grid Functionality

- Information & Data Access
- Device Control
- System or End Device Configuration
- Network Management and Performance
- Automation Systems
- Databases
- Data Calculations
- Cyber Security
- Physical Security



10 / GE /

Understanding the Threat

Protecting against -

- The Hacker
- The Vandal
- The Terrorist
- The Disgruntled Employee
- The Competitor
- The Customer
- The Security System

Types of attack -

- Eavesdropping
- Traffic Analysis
- Replaying
- Spoofing
- Cracking
- Social Engineering
- Denial of Service
- Destruction
- Reconfigure
- Malware



11 / GE /

Understanding Consequences and Risks

Analysis of Areas of Attack:

Control – Take control of switches (meters or substations)

Information – Interrupt or corrupt data flow

Configuration – Change configuration to open door for future action

Safety – Compromise safety of people or things



12 / GE /



Strong Security Techniques

- RADIUS server – Centralized security server with AAA – Authentication, Authorization and Accounting
- Extensible Authentication Protocol (EAP)- Transport Layer Security (TLS) – Commonly used in wireless systems
- X.509 is a standard for Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI)
- Ephemeral Cryptographic Key Management
 - DHE-DSS Diffie-Hellman Key Exchange - Digital Security Standard
- Secure Communication (message integrity, encryption, and replay protection)
 - Encryption / Hashing / Digital Signature



13 / GE /

Factors of Authentication

- 1. What You Know** – Passwords are widely used to identify a User, but only verify that somebody knows the password.
- 2. What You Have** – Digital certificates in the User's computer add more security than a password, and smart cards verify that Users have a physical token in their possession, but either can be stolen.
- 3. What You Are** – Biometrics such as fingerprints and iris recognition are more difficult but not impossible to forge.
- 4. What You Do** – Dynamic biometrics such as hand writing a signature and voice recognition are the most secure; however, replay attacks can fool the system.



NERC CIP: Two Factors required for Interactive Access

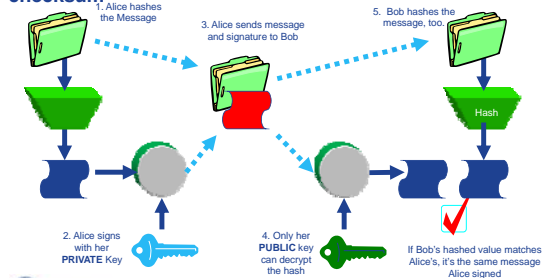


14 / GE /

Digital Signatures

Using asymmetric encryption for authentication

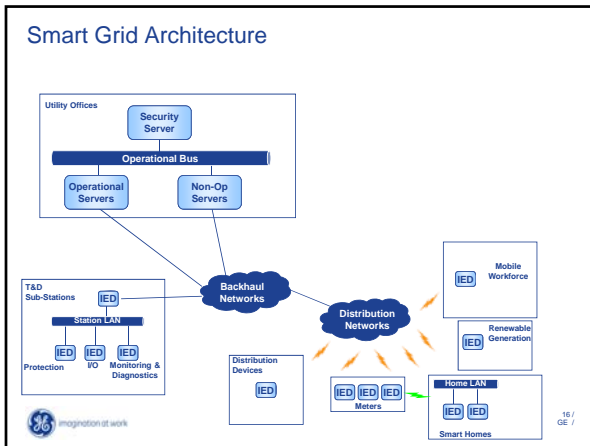
Uses a “one-way-hash” that is similar to a CRC or checksum



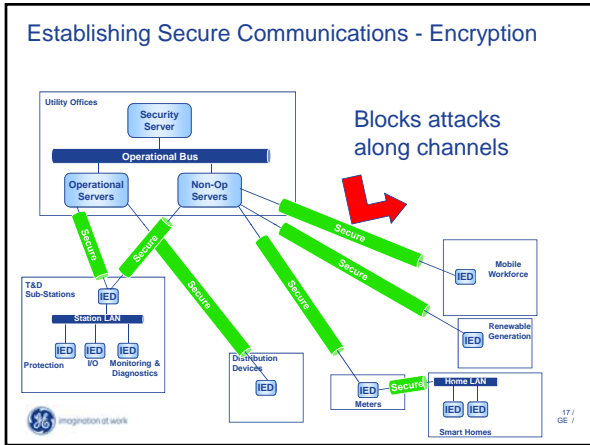
15 / GE /



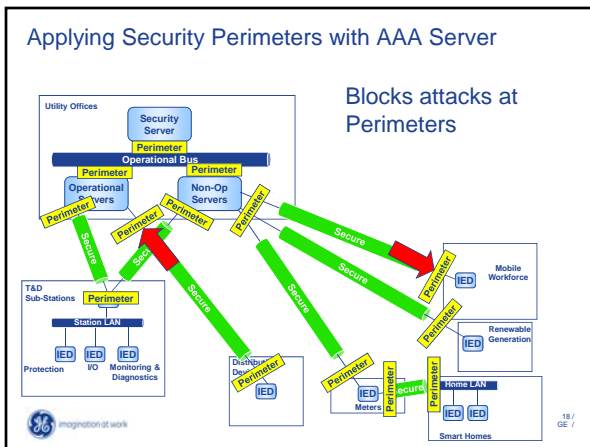
Smart Grid Architecture



Establishing Secure Communications - Encryption

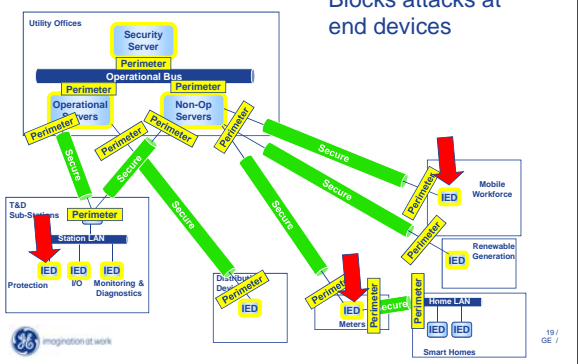


Applying Security Perimeters with AAA Server



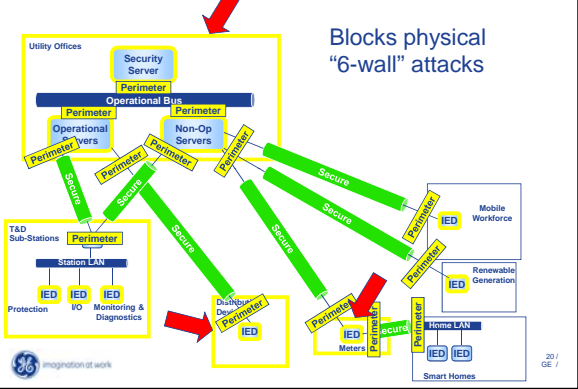


Secure the Devices with Private Keys and AAA Server



Blocks attacks at end devices

Physical Security



Blocks physical "6-wall" attacks

Summary

- NERC and Corporate Security Requirements
- Functions to Protect
- Understanding the threat
- Understanding the types of attacks
- How likely and serious are the consequences
- Current security methods
- Deploy a matching solution