Southern Company Generation

GENGuard™
Security by Design

Cyber Security for Process Control

Lessons Learned

Larry A. Spoonemore
SC Generation, Information Technology

January 2008

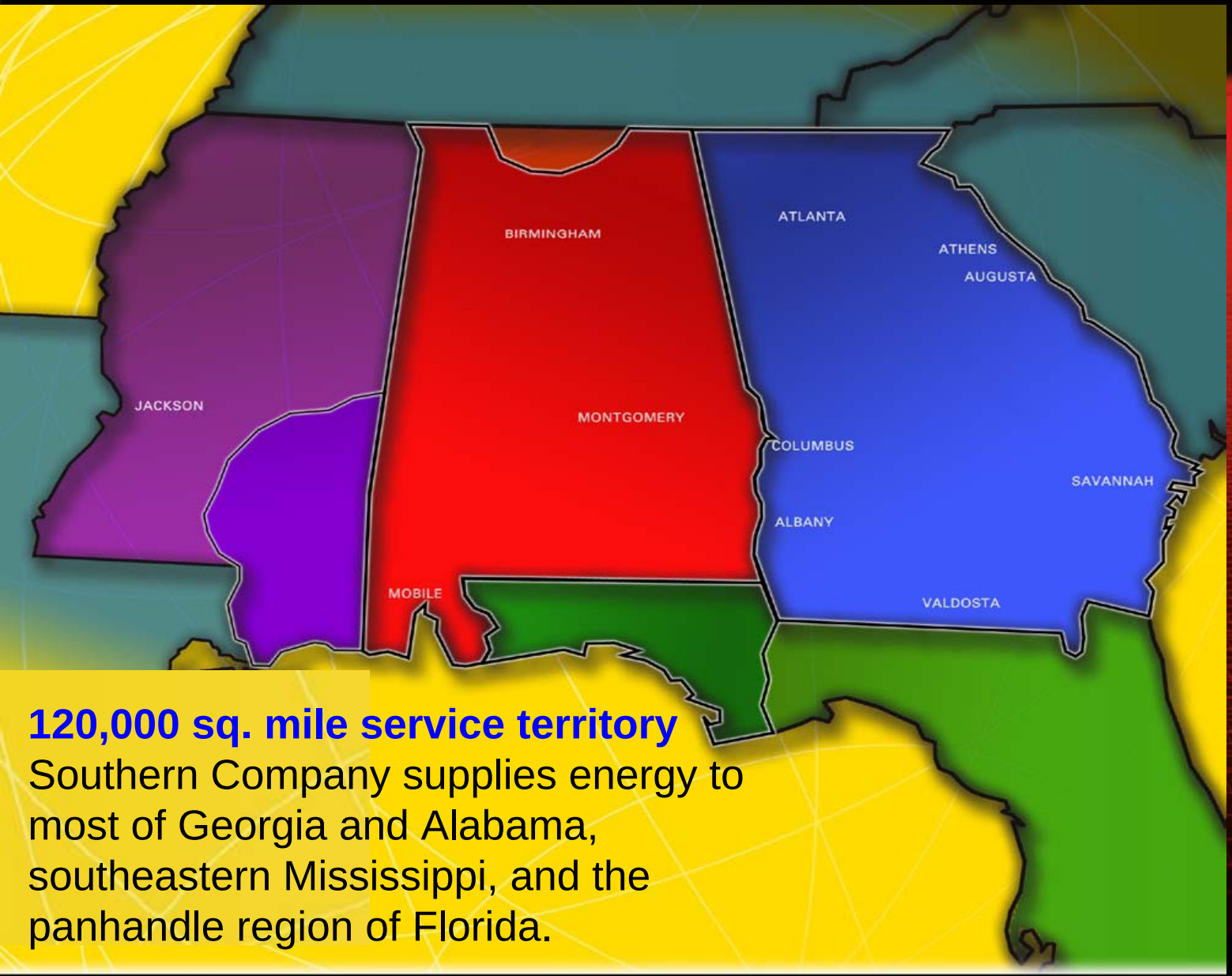
SOUTHERN COMPANY
Energy to Serve Your World®

INTRODUCTION

1. Who is Southern and What is GENGuard™?
2. The Challenges
3. Lessons Learned

Who is SOUTHERN COMPANY

One of the largest generators of electricity



120,000 sq. mile service territory

Southern Company supplies energy to most of Georgia and Alabama, southeastern Mississippi, and the panhandle region of Florida.

Plant Operations

The Southern Company operates more than **290** generating units in **72** plants with a combined capacity of over **46,000** megawatts.

SOUTHERN COMPANY

Energy to Serve Your World®

What is GENGuard™

GENGuard™...

A cyber security program for Electric Generating Plants.

Established to protect cyber assets from being vulnerable to malicious or unintentional cyber events.

The program consists of various components, including security policies, tools, technologies and processes to both enable and ensure on-going security of *essential cyber assets*.

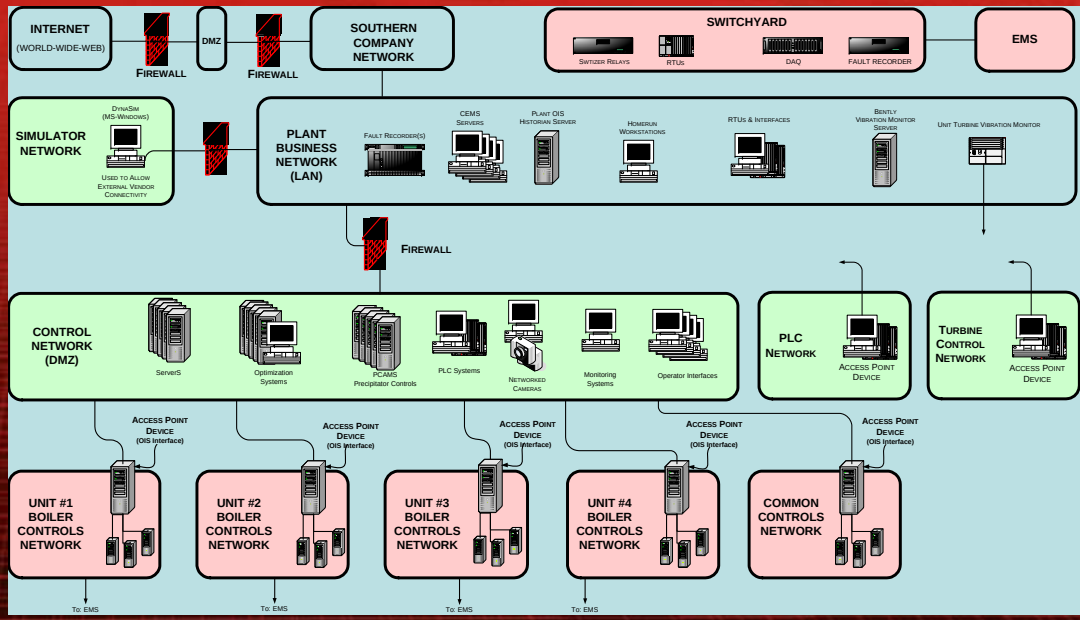
Business Drivers: The following business drivers exist that have made this program necessary.

- 9/11 and 2003 Northeast Blackout
- Regulatory compliance with FERC,NERC, DHS, & DOE (click here)
- Emerging threats with computer viruses, worms, and malicious attacks
- Security of Southern Company's Commercially Sensitive Data and Plant Process Control Systems
- Company Policy - Network Connectivity & Security (click here), Hardware Software Management (click here)

SECURITY FOCUS

Southern Company Generation

- Anti-virus
- Firewalls
- Intrusion prevention
- Penetration testing
- System patching
- Vulnerability testing



GENGuard™
Security by Design

SOUTHERN COMPANY
Energy to Serve Your World®

CHALLENGES

Southern Company Generation

Different Flavors of Cyber Security

Corporate IT

Manage the Business

1. IT Focuses on reliable networks and business applications
2. Common Hardware, OS, & Configuration
3. Dedicated IT Support Staff
4. Matured Policies, Standards, & Cyber Security Program

Energy Mgt System

Deliver the Product

1. Manages the reliable transmission of Electric Power to millions of customers
2. One Master System with similar sub-nodes
3. Dedicated Support Staff for IT systems
4. Matured Policies, Standards, & Cyber Security Program

Electric Power Plants

Produce the Product

1. Generate Electric Power reliably, at a low cost, & cleanly
2. 290 Generation Units w/various HW & OS types, configurations
3. Systems Support spread between local, corporate & vendor groups.
4. Cyber Security Program – under construction.


CHALLENGES
MONITOR / MEASURE
NEW ACQUISITIONS
REMOTE ACCESS
BUDGET
TOOL ADMINISTRATION
INDUSTRY STANDARDS
VENDOR MANAGEMENT
ACCESS MANAGEMENT
NON-IT MANAGED DEVICES
DOCUMENT MANAGEMENT
CERTIFICATION
COMPLIANCE AUDITS
ASSET MANAGEMENT
ANTI-VIRUS SOLUTION FOR PCS
AWARENESS & TRAINING
COMMUNICATIONS
DISASTER RECOVERY
INVENTORY
POLICIES
CHANGE MANAGEMENT
SECURITY UPDATES
INTELLECTUAL PROPERTY
HARDENING PCS
PHYSICAL SECURITY MGT
CONTRACTS-SOW's
ESCALATION POINT
INCIDENT RESPONSE
COMPLIANCE
BUSINESS CASES
VULNERABILITY MANAGEMENT
PORT MODEL DEVELOPMENT
RISK MANAGEMENT
PROJECT MANAGEMENT
NERC CYBER STANDARDS
COMPLIANCE w/REGULATION & POLICY
LIFECYCLE MANAGEMENT
REQUEST FOR REVIEW
LIAISON - IT SEC, VENDORS, PLANTS, CORP. SECURITY, ENGINEERING, EXECUTIVES, EXTERNAL
Allen Bradley
Metso
Proprietary OS
Woodward
Yokogawa
Solaris 10
Foxboro
Windows XP
Windows 2003
ABB/Bailey
General Electric
Honeywell
SOUTHERN COMPANY
Southern Company Generation

CHALLENGES

Change…It's what is happening all around you while your making your plans.

- The risk continues to change
  - Holes are found in yesterdays security solutions
- Your assets continue to change
  - New systems, upgrades, demand for increased connectivity
- Technology continues to change

Change is both the Challenge and the Opportunity…

LESSONS LEARNED

- Don't try to eat the whole elephant in one bite
  - Create a VISION of Milestones to achieve over time
    - This will guide your strategies and goal setting
      - Reference: Roadmap to Secure Control Systems in the Energy Sector
        - » http://www.controlsystemsroadmap.net/
  - Develop achievable & measurable goals
    - Examples
      - Inventory & Document all cyber assets
      - Measure & Access your Vulnerabilities
      - Develop & implement protective measures for your essential cyber assets
- Use change as an opportunity to make your vision a reality
  - Security by Design: To reduce the risk of introducing new vulnerabilities to a hardened environment, add cyber security specifications to procurement language.
    - Reference: Cyber Security Procurement Language for Process Controls
      - http://www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf
    - Security Certification

LESSONS LEARNED

- Don’t put all of your eggs in one basket
  - Segregate cyber assets that are most important to your operation
- Don’t Reinvent the Wheel

  - Adopt an Industry Standard (NERC Cyber Sec. Std.’s, NIST 853A, ISA 99)
  - Benefit from the collective efforts of industry and subject matter experts. Use this as a guide to assist with managing and communicating a complex issue.
- Tools are Your Friend
  - Even with the best defenses in place you still need to manage change, monitor operations, delay intruders, and Respond to Threats. These are significant challenges & require sophisticated tools.

LESSONS LEARNED

- Create Policies that state your security principles
  - Everyone must have a common understanding of what is acceptable.
- Focus on the Big Stuff
  - You can't secure it all. Classify your assets and focus on those things that are essential to your operation or business goals. Get the greatest benefit from your limited resources.
- Cyber Security is a People Problem, not a Technology Issue
  - Ensure that everyone understands the risk, the vision, and their responsibility.
  - Provide people with training and guidance on solutions to security risks.
  - Cyber Security is a sophisticated problem. Provide your people sophisticated tools.

CLOSING THOUGHTS

Cyber security is a journey…

The threat landscape, as well as technologies and processes to protect, are continually evolving.

There is no Silver Bullet.

Your best defense is a well informed and educated workforce.

Southern Company Generation

GENGuard™
Security by Design

SOUTHERN COMPANY
Energy to Serve Your World®