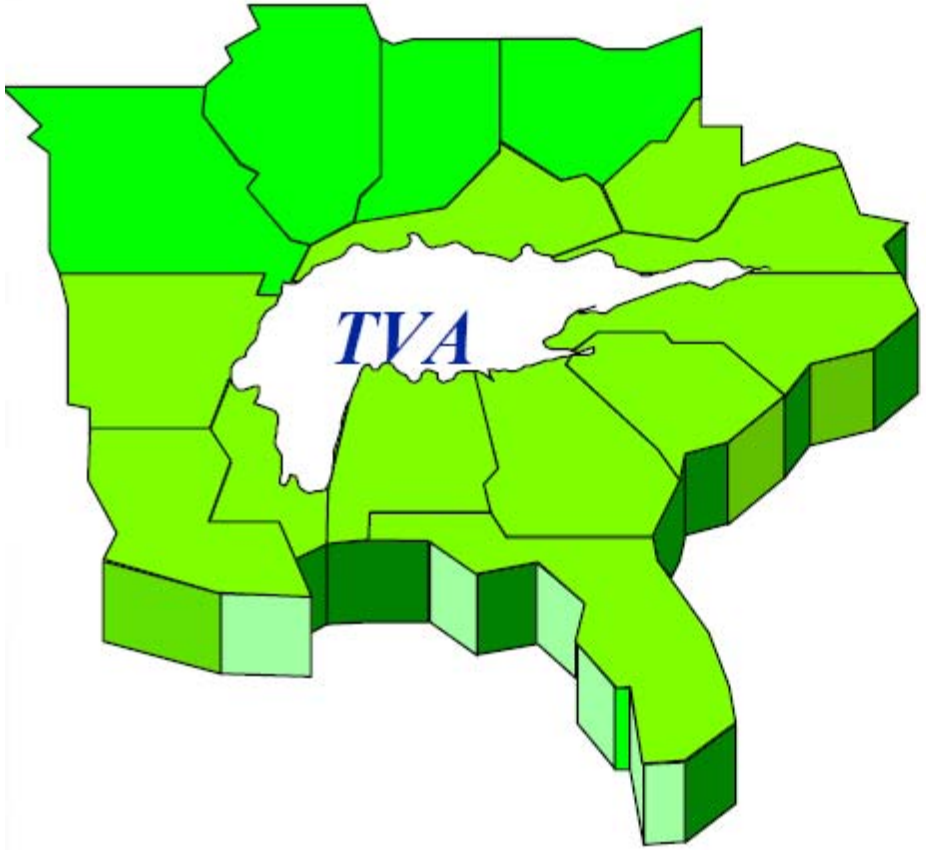
# Applying NIST SP 800-53 to Control Systems

**Cynthia Hill-Watson**
**James Tosh, III**

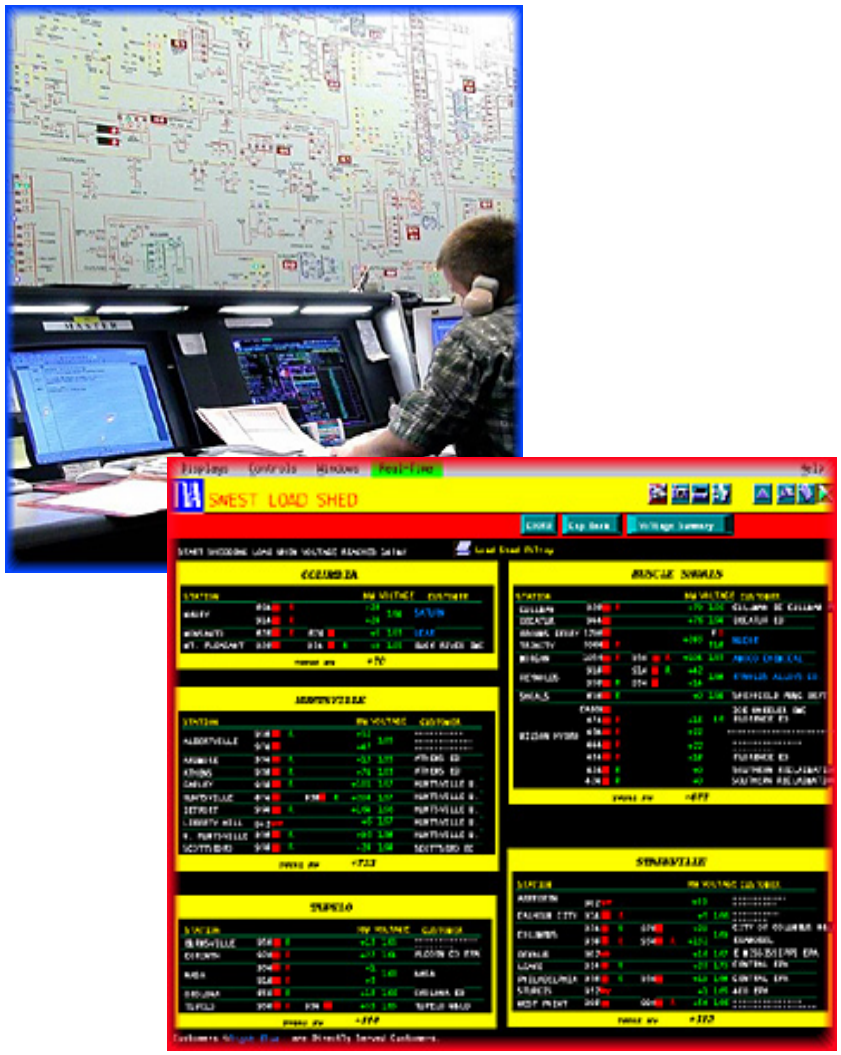
**August 16, 2007**
**Knoxville, TN**

# TVA Power System




- 80,000 Square Miles
- 7 States
- 57 Interconnections
- 17,000 Miles of Transmission Line
- 15 Balancing Area / Transmission Operator Interfaces

# SCADA




- Siemens PowerTG System on a Unix platform (migrating to Linux)
- Client software runs on Unix and Windows 2003/2000 platforms
- 114 Workstations (172 Monitors)
- 450 Remote Terminal Units
- 2,684 display screens
- DMZ – File Transfer, Dataware
- Interconnections
  - ICCP
  - Remote Vendor Support
- Maintained and supported by dedicated Control Systems IT and SCADA EMS support staff

# NIST Risk Management Framework

***Starting Point***

**FIPS 199 / SP 800-60**

**Security Categorization**

Define criticality /sensitivity of information system according to potential impact of loss

**FIPS 200 / SP 800-53**

**Security Control Selection**

Select minimum (baseline) security controls to protect the information system; apply tailoring guidance as appropriate

**FIPS 200 / SP 800-53 / SP 800-30**

**Security Control Refinement**

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

**SP 800-18**

**Security Control Documentation**

Document in the security plan, the security requirements for the information system and the security controls planned or in place

**SP 800-70**

**Security Control Implementation**

Implement security controls; apply security configuration settings

**SP 800-53A**

**Security Control Assessment**

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

**SP 800-37**

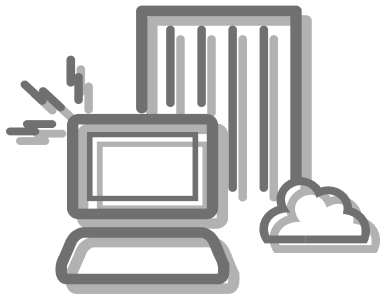
**System Authorization**

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

**SP 800-37 / SP 8800-53A**

**Security Control Monitoring**

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



TVA's IT Security and Privacy Program follows NIST Risk Management Framework

# Challenges Applying Some Controls

- **SCADA (Major Application)**
  - HIGH Overall Security Rating
  - NIST SP 800-53 HIGH baseline
- **Some controls from the following families are not implemented due to the potential adverse impact to business operations**
  - AC – Access Control
  - SI - System and Information Integrity
  - SC - System and Communications Protection
- **Compensating controls used to minimize risks**

**Following slides lists controls where weaknesses/deficiencies were identified*

# RISK ASSESSMENT

- **AC-07 Unsuccessful Login Attempts -** The information system enforces a limit of defined number of consecutive invalid access attempts by a user during a time period. System automatically locks user account/node.
- **AC-12 Session Termination –** The information system automatically terminates a remote session after a defined time period of inactivity.
- **SI-03 Malicious Code Protection -** The information system implements malicious code protection.
- **IA-07 Cryptographic Module Authentication and SC-12 Cryptographic Key Establishment and Management**

# Security Certification and Accreditation

- **AC-05 SEPARATION OF DUTIES –** The information system enforces separation of duties through assigned access authorizations.

- **AC-10 CONCURRENT SESSION CONTROL –** The information system limits the number of concurrent sessions for any user to a defined number of sessions.

- **AC-11 SESSION LOCK –** The information system prevents further access to the system by initiating a session lock after a defined time period of inactivity. (shared accounts)

# Security Certification and Accreditation

- **AU-06 AUDIT MONITORING, ANALYSIS, AND REPORTING –** The organization regularly reviews/analyzes information system audit records for indication of inappropriate or unusual activity, investigates activity or suspected violation, reports findings to appropriate officials, and take necessary actions. Control Enhancements:
  - (1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
  - (2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

# Security Certification and Accreditation

- **AU-09 PROTECTION OF AUDIT INFORMATION -** The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

- **CM-06 CONFIGURATION SETTINGS** Control Enhancement 1 - Automated controls have not been implemented to provide for the management of configuration settings.

- **CM-07 - LEAST FUNCTIONALITY –** The organization configures the information system to provide on essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services.

# Security Certification and Accreditation

- **IA-02 USER IDENTIFICATION AND AUTHENTICATION –** The information system uniquely identifies and authenticates users.

- **IA-07 CRYPTOGRAPHIC MODULE AUTHENTICATION -** The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

- **SC-03 SECURITY FUNCTION ISOLATION** - The information system isolates security functions from nonsecurity functions.

# Security Certification and Accreditation

- **SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT -** When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

- **SI-03 MALICIOUS CODE PROTECTION -** The information system implements malicious code protection.

- **SI-06 SECURITY FUNCTIONALITY VERIFICATION -** The information system verifies the correct operation of security functions upon system startup and restart, upon command by user with appropriate privilege, periodically every defined time-period and notifies system administrator, shuts the system down, restarts the system when anomalies are discovered.

# System Authorization

| Risk Management Forms | Open | Closed |
|---|---|---|
| Risk Assessment | 1 | 3 |
| Security Test & Evaluation | 1 | 8 |
| Plan of Action and Milestones | 2 | 11 |

**Authorization to Operate System**

Note: Each weakness identified in the Risk Assessment and ST&E reports and its mitigation plan (accept risk, mitigate risk, avoid risk, transfer risk) are described on a risk management form. Plan of Action and Milestones measures implemented or planned milestones to correct weaknesses or minimize risks.

Two “Open” items pertain to Malicious Code—mitigation planned by Sept. 2007.

# QUESTIONS

**For more information…**

**Cynthia Hill-Watson**
**Office Phone: 423-751-6747**
**Email: chwatson@tva.gov**

**James Tosh III**
**Office Phone: 423-751-4492**
**Email: jttosh1@tva.gov**