



The Challenges of Cyber and Physical Security Convergence

PCSF 2006 Spring Meeting

June 6, 2006

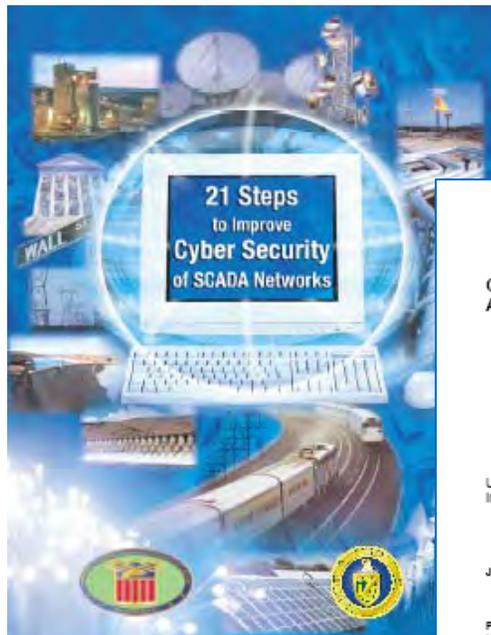
Margaret E. Grayson

AEP Networks, Inc.

“If there’s going to be a physical attack, there’s going to be a cyber-attack. They’re going to shut down your eyes and ears.”

- Joe Jarzombek, Director of Software Assurance, Department of Homeland Security, May 2006

SCADA and Cyber Security



Control Systems Cyber Security Awareness

US-CERT
Informational Focus Paper

July 7, 2006

Produced by:
United States Computer Emergency Readiness Team



SAND REPORT
SAND2005-7301 Unrestricted Release
Printed December 2005

Analysis of Operations and Cyber Security Policies for a System of Cooperating Flexible Alternating Current Transmission System (FACTS) Devices

Laurence R. Phillips, Mich Bryan Richardson, and Li

Sandia National Laboratories
Albuquerque, New Mexico 87185 and
Sandia is a multi-program laboratory managed by Lockheed Martin Corporation, for the U.S. National Nuclear Security Administration

Approved for public release; distribution is unlimited.

Sandia National



The impact of cyber security on SCADA systems is an emerging area of interest for critical infrastructure resilience.

Why cyber at all, rather than just physical?

- Low cost of required resources
- Low risk of casualties or retaliation
- Control of attribution and attribution timing
- Deniability
- Relatively precise control of what is destroyed
- Much greater destructiveness than physical attacks alone
- Technologically prestigious

Copyright © 2006 Scott Borg/U.S. Cyber Consequences Unit. All rights reserved.

Convergence Trends

- Technology
- Vendor
- Community
- Education
- Threats

Cooperation between physical and cyber security practices has increased since 911.

Source: CSO Magazine

Convergence Challenges

- Identity
- Information Sharing
- Governance
- Cost

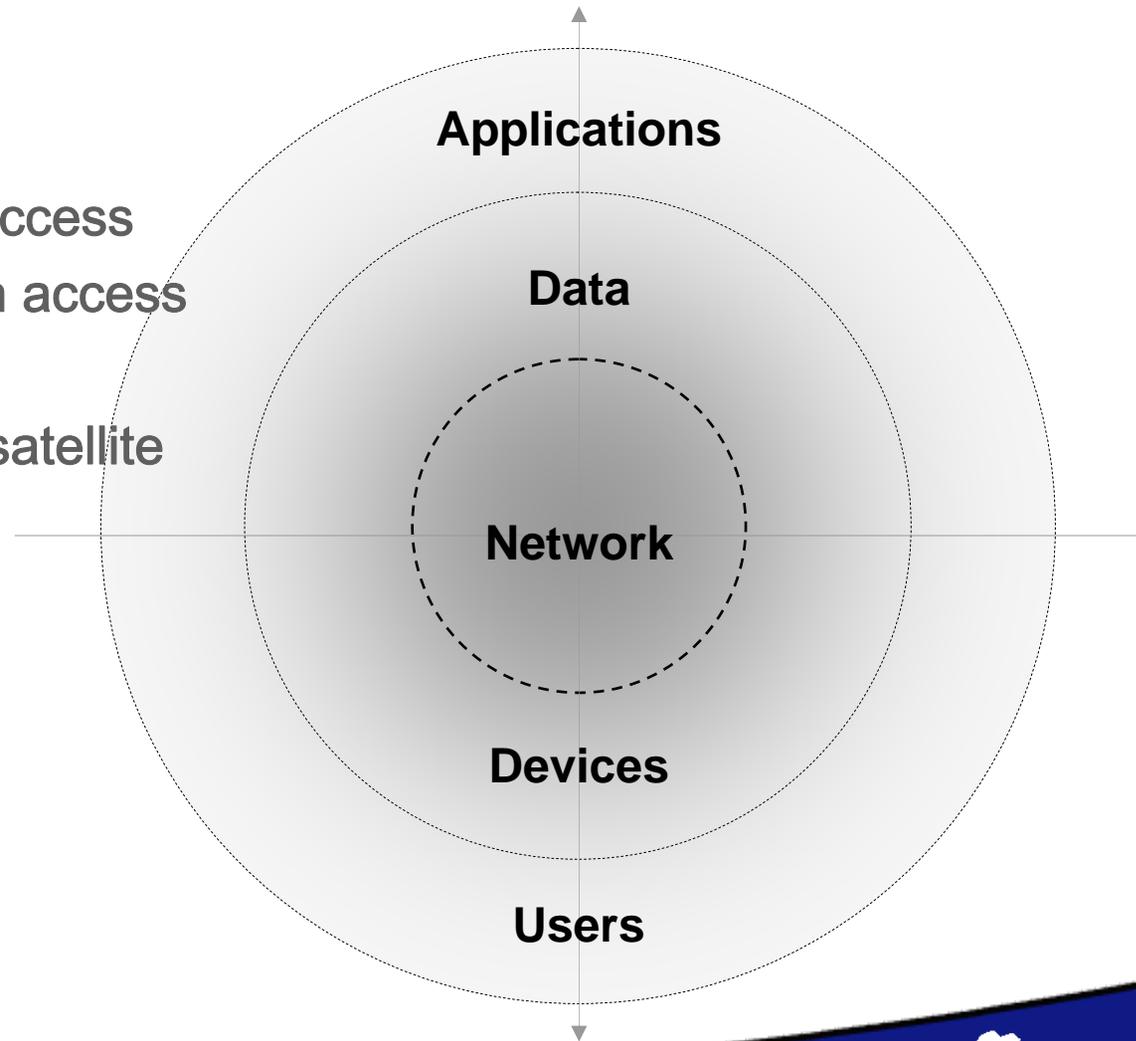


The Human Factor is Critical

Today's Reality

Requirements:

- Identity based user access
- Real time information access
- Legacy applications
- Wired, wireless and satellite



A Path Forward...

The Homeland Security Presidential Directive 12

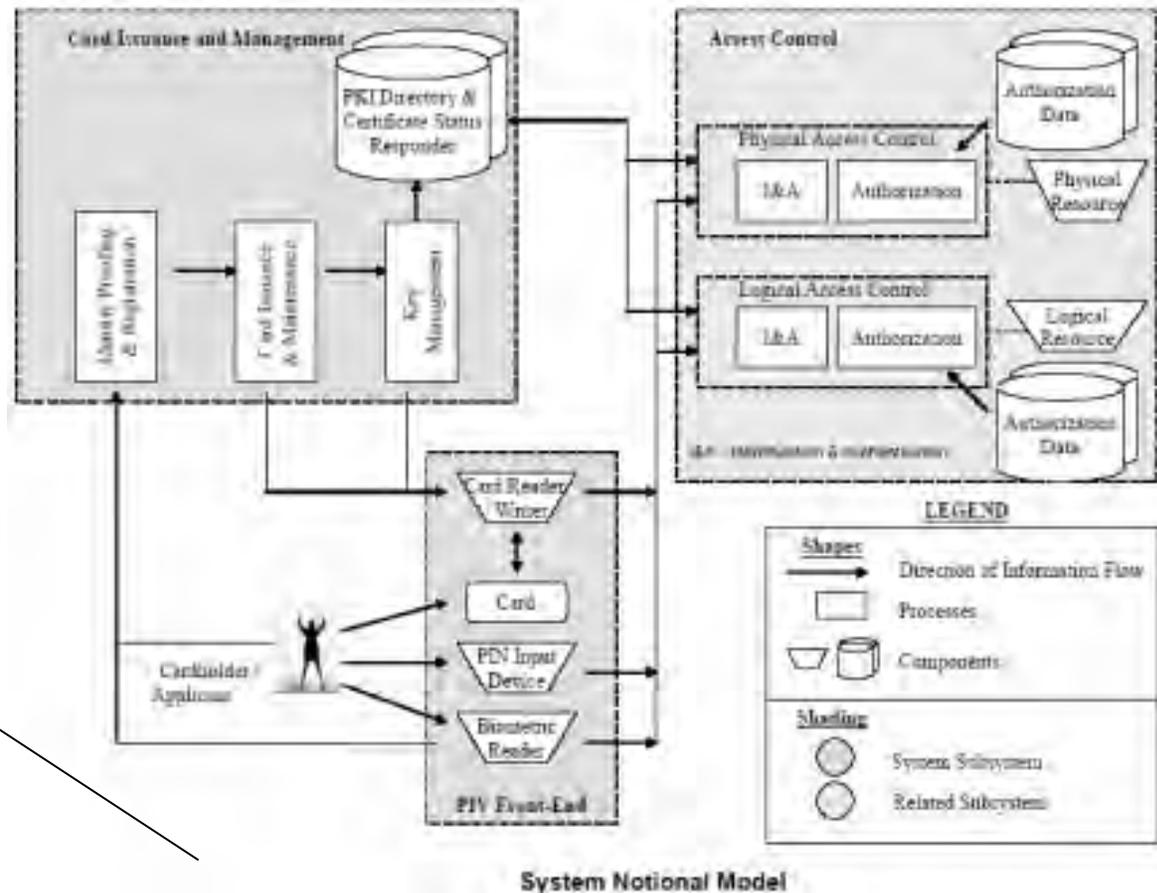
“The HSPD-12 standard will protect against a wide array of threats, including unauthorized access to government resources, identity theft and terrorism. By mandating a common identity standard ... HSPD-12 ushers in a new era of strong, multi-factor authentication that increases the security of networks, applications and data, while eliminating the risk of compromise due to poorly managed passwords. HSPD-12-compliant identification technologies will also improve efficiency when it comes to accessing data in highly secure environments.”

Source: The Impact of HSPD-12, a Novell white paper

Secure Identity Management

- **(HSPD-12) mandates a common identification standard** for all federal government agency employees and contractors, and establishes deadlines for adoption of the new identification mandate. Executive departments and agencies are required to use the standard for identification issued to federal employees and contractors to be used for both physical access to federally controlled facilities and logical access to federally controlled information systems.
- **In response to HSPD-12, FIPS 201** is the government-wide standard released by the National Institute of Standards and Technology (NIST) for reliable Personal Identification Verification (PIV) for government employees and contractors. Agencies are currently working toward PIV-II. FIPS 201 can provide a framework for local government and any corporation that requires secure identification. It provides a solid unified standard that can be adopted by local governments or by any corporation that requires strong identification of its employees.

FIPS 201 Architecture



System Notional Model

Source: Architecture diagram from SCB Solutions

SCADA Considerations

- Cyber Security as Enabler
- Skilled IT/Workforce Development
- R&D
- Risk Assessment/Risk Management

Information Sharing is Critical

The Basics of the ROI Calculation

Risk = Expected Loss = Threat x Consequence x Vulnerability

Reduction (Δ) in (Frequency of a Given Attack x Potential Consequence of That Attack x Probable Level of Damage from That Attack) = Loss Avoided = The Gain from the Counter-Measure Producing That Reduction

This “loss avoided” result needs to be compared with the cost of the counter-measure and assessed for confidence.

Whenever the gain from the counter-measure is hugely greater than the cost of the counter-measure, and the confidence level is appreciable, the implied ROI makes the need for the counter-measure obvious.

Copyright © 2006 Scott Borg/U.S. Cyber Consequences Unit. All rights reserved.

Convergence Themes

- A comprehensive security strategy
 - ...aligns security goals with organization goals.
- Security as a subset of Risk Management
 - ...supports cyber and physical security convergence requirements.
- Focus on the **consequences** of vulnerabilities in converged systems
 - ... recognizes that the impact of a failure can be disabling; i.e. Cyber security for SCADA and process control systems.

Best Practices

Four important questions...

1. How secure is secure enough?

Establishing cyber-trust is critical

Sensitive information sharing requires strong *integrated* security

Cyber and physical convergence demands security at the “intersection”

2. Is security available “on-demand”?

Choose self-provisioning solutions that support wide variety of user and operational environments, including mobile ones

3. Will the security features be used?

End-user transparency

Centralized/distributed policy management

4. Can I leverage my IT investment?

Federated authentication and identity extends across systems

Standards will evolve

Workforce development and cross-education

Trusted.
Certified.
Secure.

Thank You

AEP Networks

40 W. Gude Drive – Suite 100 – Rockville, MD 20850

1.240.399.1200

www.aepnetworks.com

gov.info@aepnetworks.com

