

Applications of InfoSec to Protect the Electric Power Grid

Information Survivability Workshop

Panel Presentation*

March 18-20, 2002, Vancouver, BC Canada

Paul W. Oman

Schweitzer Engineering Laboratories, Inc.

*Portions of this work were funded by grant #60NANB1D0116 from the National Institute of Standards and Technology, U.S. Dept. of Commerce.

Examining Cascading Failures

1996 West Coast Blackouts

- Portland, Seattle, and California Drawing From Columbia Hydroelectric System
- Transmission Lines Heavily Burdened
- 3 Cascading Failures
- Worst Was August 10, 1996
 - ◆ 7.5 Million customers in 14 states, 2 Canadian provinces, & Baja Mexico
 - ◆ \$1.5 Billion lost in production & services
 - \$166 million per hour
 - \$2.7 million per minute

August 10, 1996 Post-Mortem



14:01:00 BigEddy-Ostrander
500kV line sags into a tree

14:52:37 JohnDay-Marion
500kV line sags into a tree

14:52:37+ Marion-Lane 500kV
line forced offline due to out
of service breaker

15:42:37 Keeler-Allston 500kV
line sags into a tree and
trips

15:42:37+ Keeler-Pearl 500kV
line also lost due to breaker
and transformer service

August 10, 1996 Post-Mortem



- Several hundred MVAR reactive power lost
- Other lines now overloaded
- Hanford voltage depressed from 527 to 506kV
- McNary reactive power increased to maximum

15:47:29 Merwin-St.Johns
115kV line trips on mis-op

15:47:36 Ross-Lexington
230kV line sags into a tree

15:47:36+ 207MW generation
lost on Ross-Lexington line

August 10, 1996 Post-Mortem



- Seven lines out
15:47:36+ McNary reactive output above maximum
15:47:40-44 Six McNary generators trip
- Frequency drops to 59.9 Hz at McNary
- McNary generator exciter circuits erroneously detect phase imbalance from drop in frequency
15:47:49-15:48:12 Three more McNary generators trip

August 10, 1996 Post-Mortem



- McNary generation drops to 350MW
- Grand Coulee, Chief Joseph, and John Day increase generation
- Frequency oscillation grows to ~ 0.224 Hz as generation is dropped and replaced
- 15:48:21 PDCI RAS inserts Malin (g.3) shunt capacitors
- Voltage increases
- 15:48:21+ PDCI begins fluctuating

August 10, 1996 Post-Mortem



15:48:47 Two more McNary generators trip

15:48:51 Malin records 1,000MW and 60kV peak-to-peak; RAS inserts Malin (g.4) shunt capacitors

15:48:51+ RAS inserts series capacitors on all three 500kV lines south of Grizzly

15:48:51+ Buckley-Grizzly 500kV line relays on Zone 1 protection

- Voltage on Malin's 500kV bus drops to 315kV

August 10, 1996 Post-Mortem



15:48:52 Malin-Round Mtn.
500kV COI #1 and #2 lines
trip on switch-into-fault logic

15:48:52+ RAS inserts Chief
Joseph Dynamic Brake

15:48:52+ JohnDay-Grizzly
500kV #1 and #2 lines trip

15:48:52+ Meridian-Capt.Jack
500kV NCOI trips

15:48:52+ Grizzly-Malin 500kV
NCOI trips

15:48:52+ Capt.Jack-Olinda
500kV COI trips

August 10, 1996 Post-Mortem



15:48:52+ 500kV COI
Separation Complete

15:49:00 Final two McNary
generators trip

- 15 lines out of service
 - 5 lost in first 100 minutes
 - 10 lost in last 2 minutes
- West Coast islanding continues ~ 30 minutes
- Island frequencies ranged from 58.3 to 61.3 Hz

Cascading Failure Vulnerability

- Generation Not Near Load
- T&D Pushed to Critical
- Failures by
 - Weather
 - Maintenance issues
 - Relay mis-operations
 - Frequency oscillations

Conclusions:

- Electric Power Vulnerable
- Cascading Failure Can be Induced by Physical or Electronic Sabotage



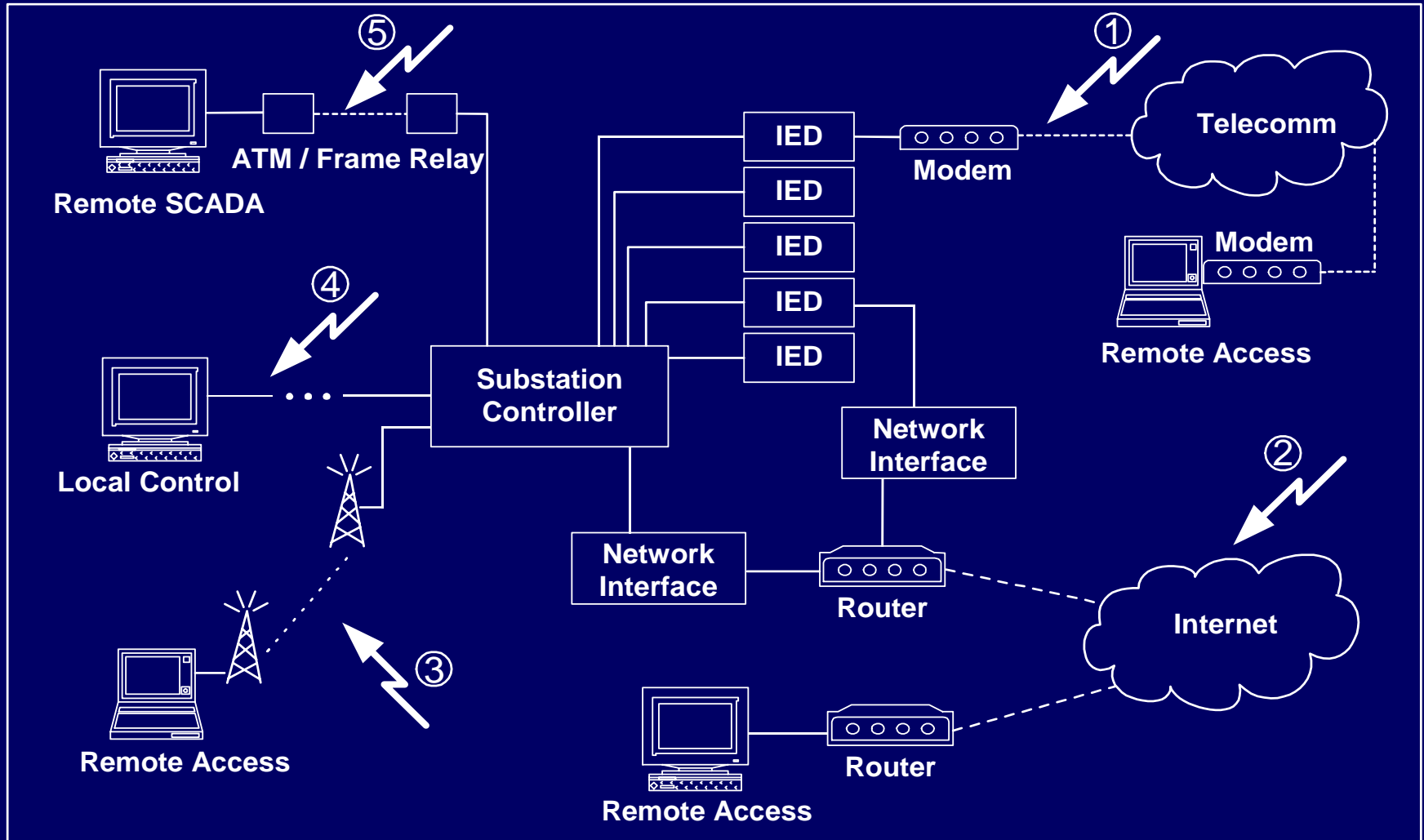
Attack Scenarios

1. Terrorism and Acts of War
2. Industry Instability Creates Disgruntled Employees
3. Deregulation and Reorganization Creates Disgruntled Customers
4. Increased World Trade Resistance
5. Increased Electronic Theft and Fraud
6. Increased Nuisance Hacking and Hacktivism

Cyber Attacks Against Electric Utilities

- Several Attacks on Utility Financial Systems
- Environmentalists Caught Hacking Utility's IT System
- Recreational Hackers Took Over Utility's Server to Play Games
- Insider Threat Against Texas Power Grid
- Insider Caught Hacking Nuclear Power Station Controls
- Cal-ISO Servers Hacked via China Telecom

Electronic Access Vulnerabilities

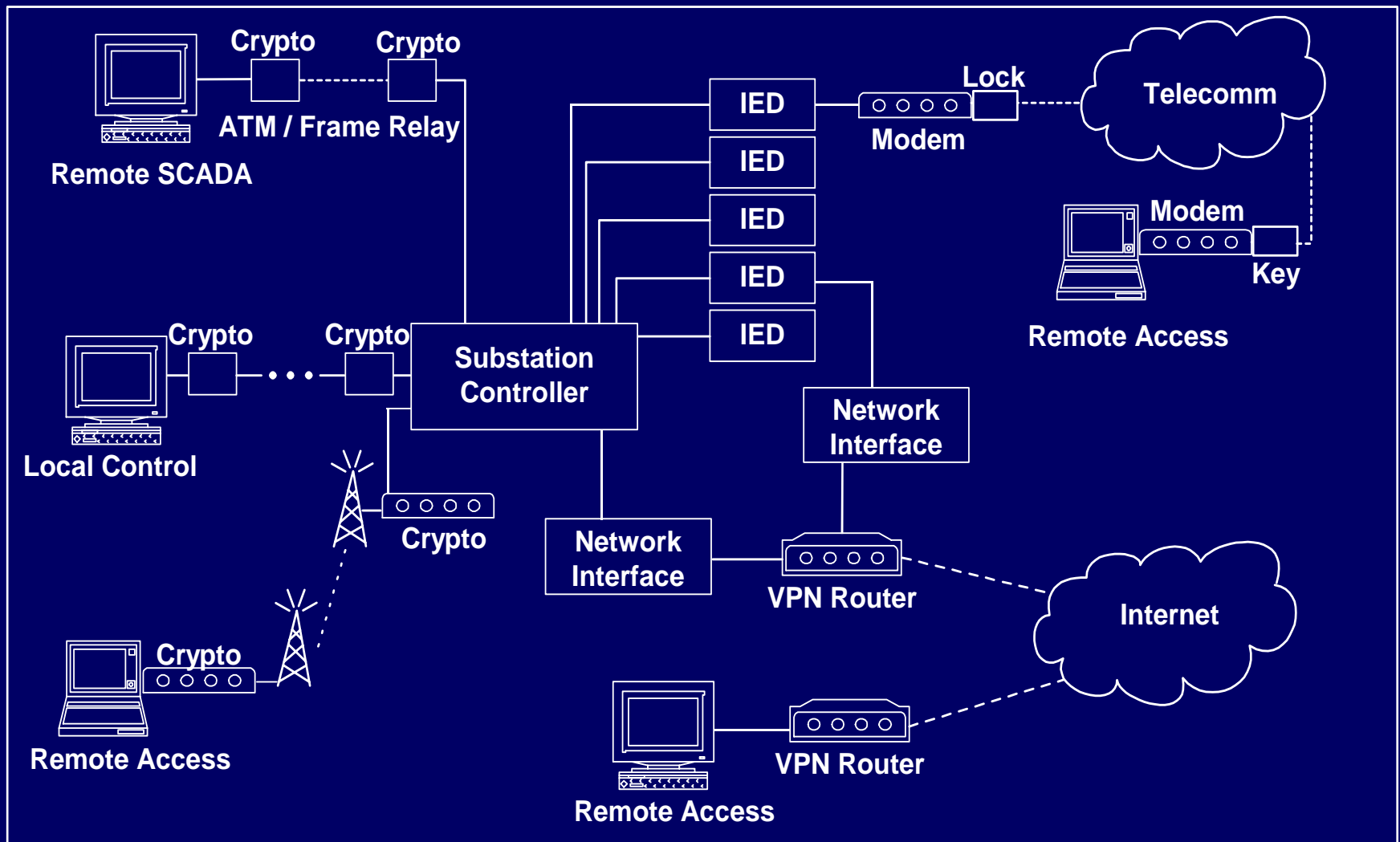


NIST Critical Infrastructure Protection Grant (SEL+WSU+UI)

Industrial Applications of Information Security to Protect the Electric Power Infrastructure

- 1. Hardening Substations Against Unauthorized Remote Access**
- 2. Applications of IPSec to Control Center and Substation Communications**
- 3. In Situ Security and Survivability Assessments**
- 4. A Prototypical Secure Information Infrastructure for Power Grid Status Data**
- 5. Foster InfoSec Awareness and Education Within the Electric Power Industry**

Securing Substation Communications



Related Publications

1. Concerns About Intrusions Into Remotely Accessible Substation Controllers and SCADA Systems (www.selinc.com)
2. Safeguarding IEDs, Substations, and SCADA Systems Against Electronic Intrusions (www.selinc.com)
3. Protecting the Grid From Cyber Attack
(*Utility Automation*, Nov. 2001 & Jan. 2002)
4. Tools for Protecting Electric Power Systems From Electronic Intrusions (www.selinc.com)

Related Publications

5. Low Cost Authentication Devices for Secure Modem and Network Connections
(www.selinc.com, AG2001-10)
6. Barriers to a Wide-Area Trusted Network Early Warning System for Electric Power Disturbances (*HICSS*, Jan. 2002)
7. Obstacles to Self-Healing Reliable Complex Control Systems (*ISW*, Mar. 2002)

Impediments to Survivability of the Power Grid

1. No Wide-Area Communications Infrastructure
2. Telecommunications Infrastructure Fragility
3. Lack of Network QoS Guarantees
4. Immaturity and Fragility of Trust Frameworks
5. No Below-Threshold Disturbance Data
6. Various Substation Communication Protocols
7. Socio-Economic and Political Resistance