

## Secure Engineering Access in Power Substations: A Real-World Example



*Making Electric Power Safer, More Reliable, and More Economical®*

Copyright © SEL 2007

## Agenda

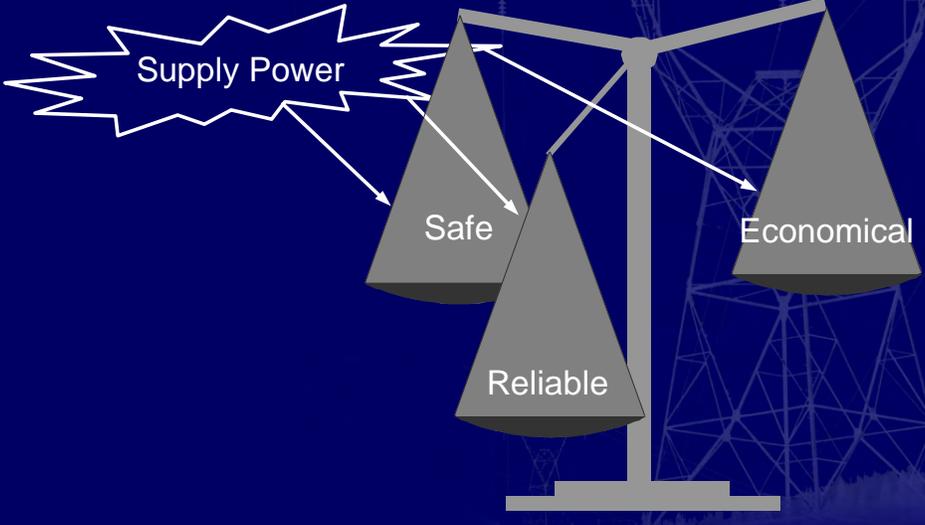
- The problems
- The methods
- Specific solution
- Best practices
- Questions

# Alabama Power



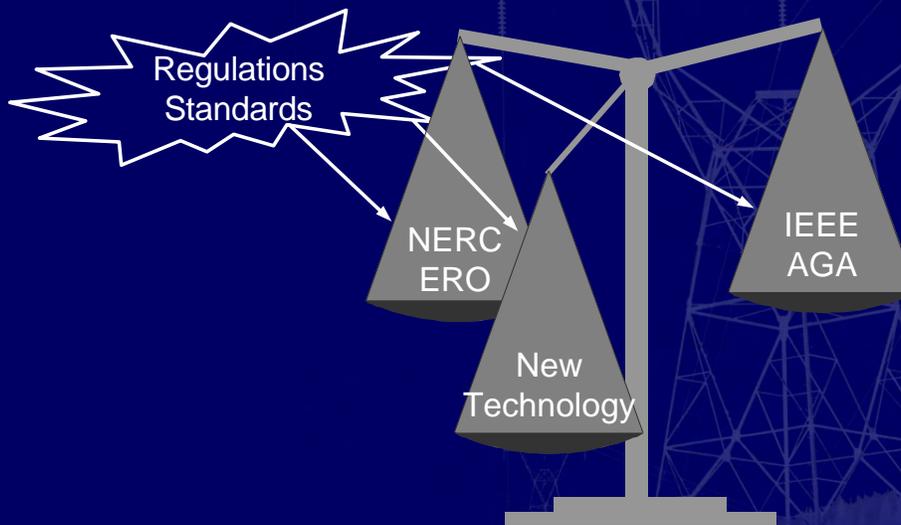
- Provides service to 1.3 million customers
- Maintains 78,000 miles of power lines
- Covers 44,500 miles of geography

## Improve Operations Bottom Line!



The diagram features a balance scale with three pans. The left pan is labeled 'Safe', the bottom pan is labeled 'Reliable', and the right pan is labeled 'Economical'. A jagged lightning bolt labeled 'Supply Power' points towards the 'Safe' pan. The background shows a power transmission tower.

## The Problem – Improve Operations



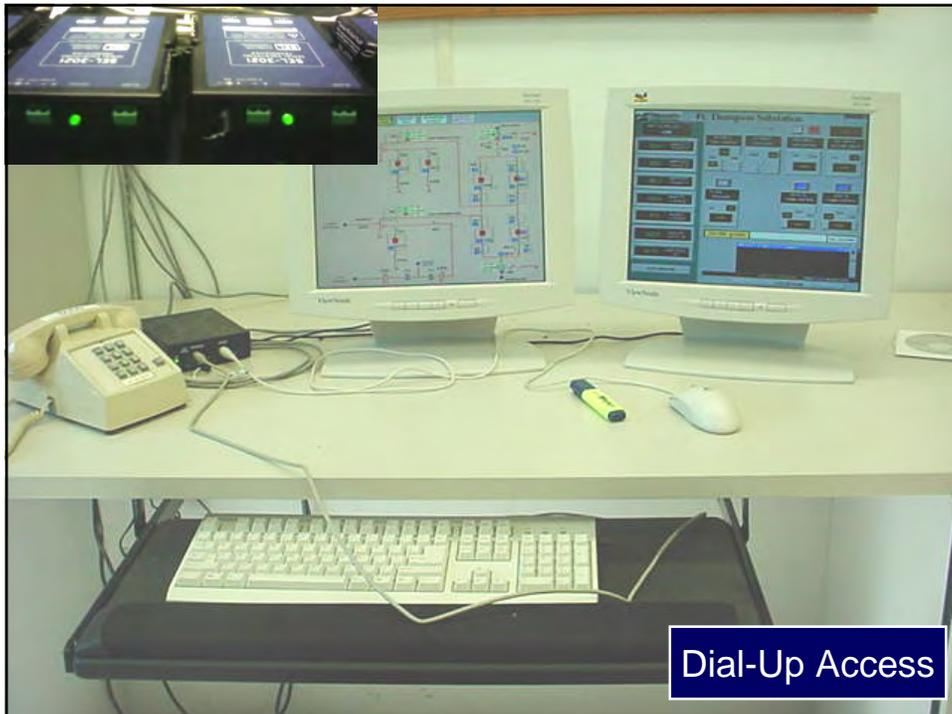
## The Problem With Security

- Consultants
- Regulations
- Media
- Management



## The Problem – Dealing With Fear, Uncertainty, and Doubt

- Has statute of limitations been reached for Queensland SCADA system hack in 2000
- How serious is problem if “experts” rely on same five-year-old incidents to prove point
- There are zero- and low-cost solutions





## Regulator Requirements

NERC / ERO

Critical Infrastructure Protection (CIP) standards

- Define roles and responsibilities
- Define electronic security perimeter
- Specifically, Section CIP 005 R2.3 – calls out that responsible entity must secure dial-up access to ESP (electronic security perimeter)

## Regulator Requirements

- From NERC CIP Workshop, Nov. 9, 2006
- Requirements
  - ◆ Effective password and user authorization control
  - ◆ Disabling of unused network services and ports
  - ◆ **Secure telecommunications and dial-up modem connections**
  - ◆ Use of firewall and IDS systems

## What Is at Stake? Financial Impact

- Blackouts are extremely expensive
  - ◆ Loss of power sales
  - ◆ Loss of productivity in affected areas
- August 2003 East Coast blackout
  - ◆ Affected some 50 million people in eight states and one Canadian province
  - ◆ Up to 40 hours to restore power
  - ◆ **Estimated \$10-billion financial impact**

## Attacker's Goal: Cause Significant Service Outage Maximize Affected Area / Length of Outage

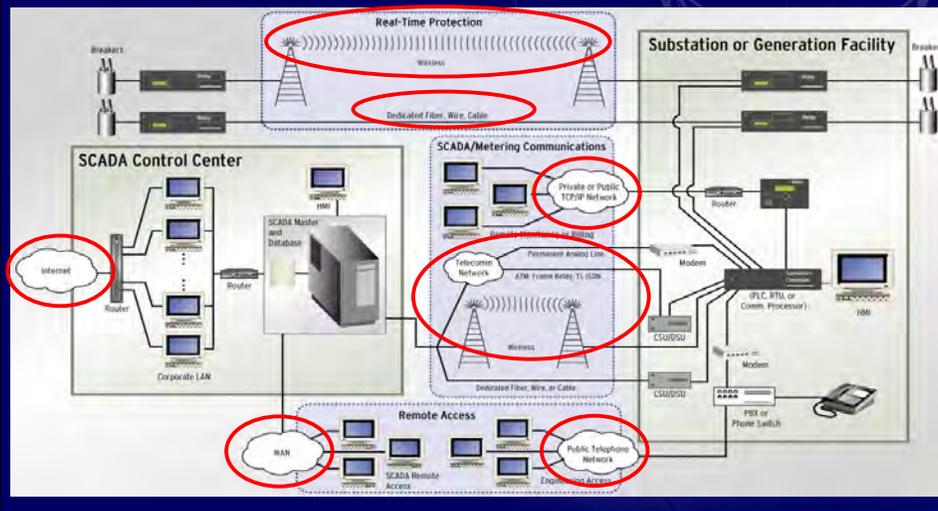


## The Sophisticated Attacker

- Attacker objectives
  - ◆ Obtain access to SCADA network
  - ◆ Remotely control power system equipment
- Motivations
  - ◆ Money – employment
  - ◆ Demonstration of skill set

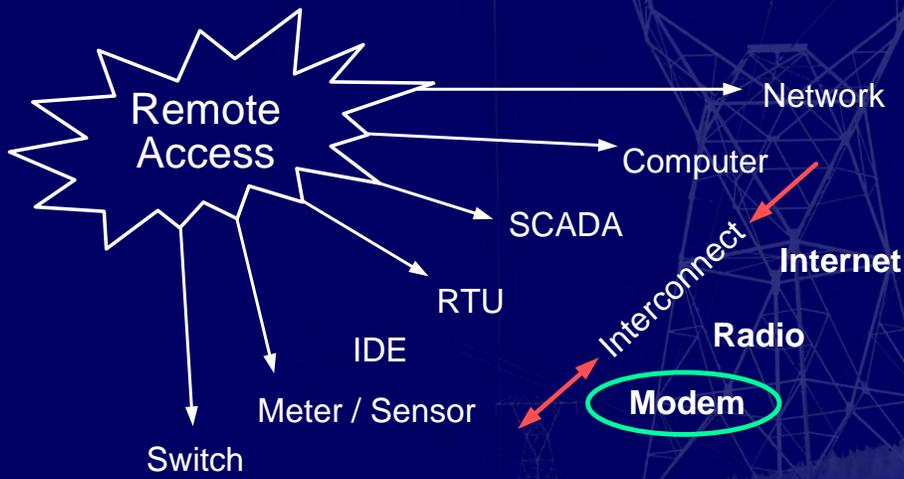


## SCADA Cybersecurity Unauthorized Access to Data Stream Areas of Concern

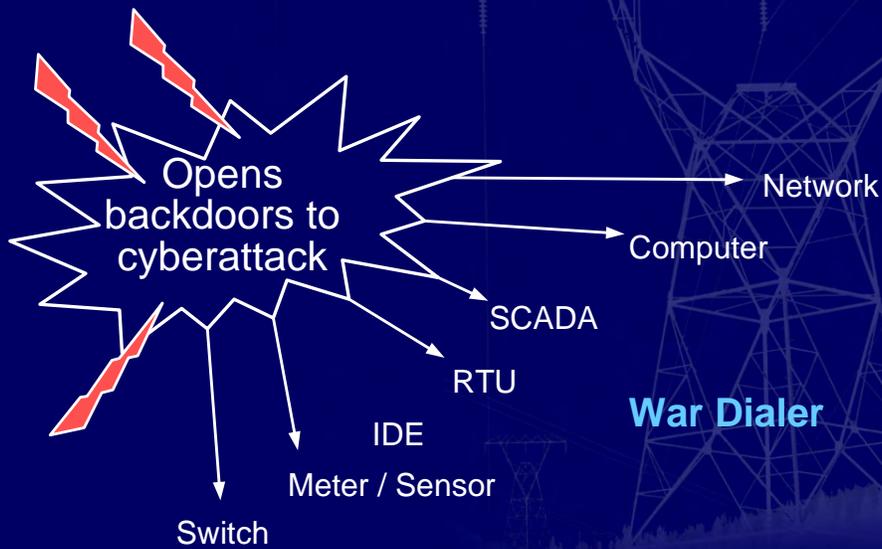


## Example – Remote Access

Faster Time to Identify / Address Problems!



## Example – Remote Access



## Attack Reconnaissance

- Attackers find corporate phone list in dumpster outside of field office
- List includes **unlisted** phone numbers to several large substations
- Calls reveal that numbers are voice lines connected to telephones (not modems)



## Modem Scanning

- Attackers know phone numbers are often assigned in contiguous blocks
- Attackers use War Dialer programs to search for modems at phone numbers “near” known voice numbers
  1. Program a range of target phone numbers
  2. Push “go”
  3. Come back later and analyze results

# Commercial War Dialer

Time	Modem	Number	Result	System ID	User ID	Password
2002-06-19 11:39	7	617-555-1637	CARRIER	PPP (MS-CHAP)		
2002-06-19 11:39	7	617-555-1305	CARRIER	PPP (MS-CHAP)		
2002-06-19 11:39	1	617-555-1459	BUSY			
2002-06-19 11:39	2	617-555-1381	BUSY			
2002-06-19 11:39	5	617-555-1272	BUSY			
2002-06-19 11:38	3	617-555-1859	BUSY			
2002-06-19 11:38	3	617-555-1973	CARRIER	PCAnywhere		
2002-06-19 11:38	7	617-555-1601	RING_TIMEOUT			
2002-06-19 11:38	4	617-555-1500	TONE			
2002-06-19 11:38	3	617-555-1265	CARRIER	PCAnywhere		
2002-06-19 11:38	2	617-555-1133	CARRIER	Unix (FreeBSD)		
2002-06-19 11:38	8	617-555-1547	CARRIER	PPP (MS-CHAP)		
2002-06-19 11:38	3	617-555-1982	TIMEOUT			
2002-06-19 11:38	6	617-555-1182	TONE			
2002-06-19 11:38	3	617-555-1238	BUSY			
2002-06-19 11:38	3	617-555-1559	BUSY			
2002-06-19 11:38	3	617-555-1144	TIMEOUT			
2002-06-19 11:38	7	617-555-1930	TONE			
2002-06-19 11:38	3	617-555-1834	TIMEOUT			
2002-06-19 11:38	7	617-555-1664	TIMEOUT			

# Descriptive Login Banners Help Attackers

GENERAL ELECTRIC CANADA, INC.

Welcome to the Paulson Hills Substations D20 RTU

LOGIN:

ENTER USER NAME: █

## Use Login Banners to Raise Security

Unauthorized access prohibited  
Illegal use will be prosecuted  
All calls are logged

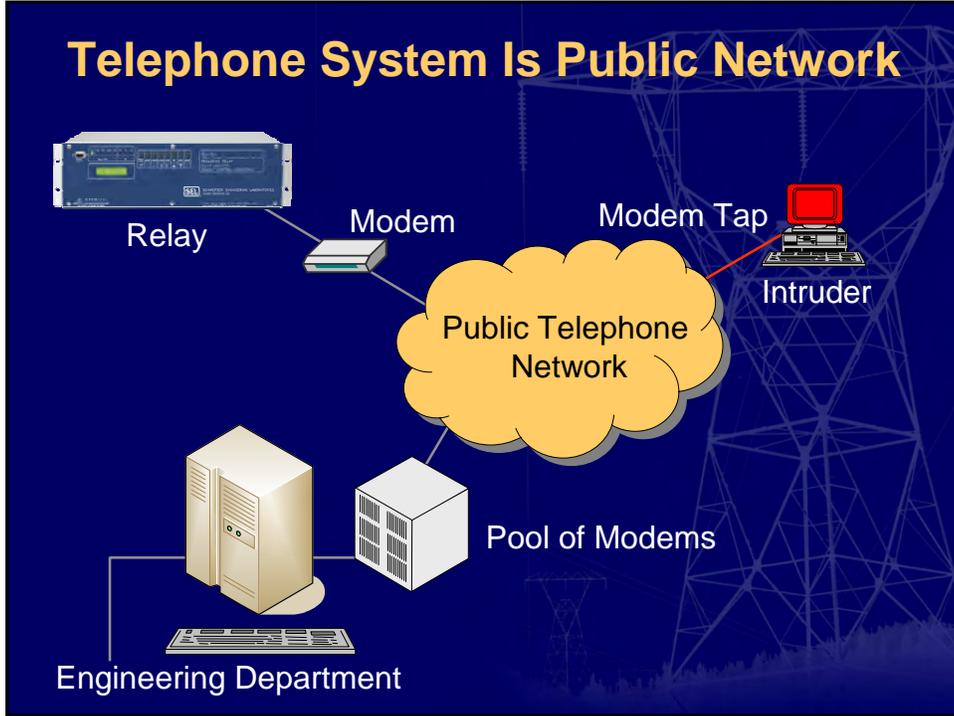
ENTER USER ID :

## Attacker Gains Access to SCADA Link by Wiretap

- Reads and saves commands and responses
- Uses data to identify protocol
- Saves access point for later attack



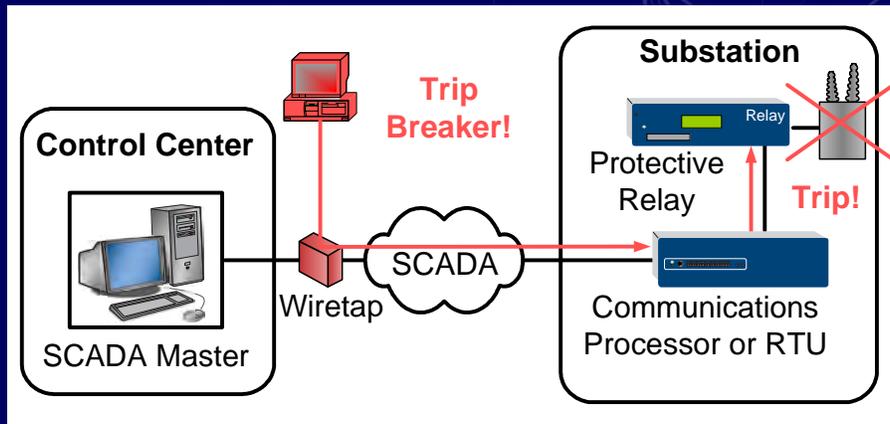
# Telephone System Is Public Network



# Modem-Tap Data Analyzer

```
EVENT #2: 10/07/04 13:27:48 CONNECT 1200 @175505039 103 bytes
<STX>12345687900987654321<FS>A4411660000091047-030410100
<ENQ>
00098100000<FS>665.42<ETX>n
<ACK><STX>RS01APPROVED 448968
<ACK> <SO> q-
<ETX><BEL> ,<CR>~U +
EVENT #3: 10/07/04 13:28:05 CONNECT 1200 @175505039 102 bytes
<STX>12345687900987654321<FS>A4411660000091047-030410100
<ENQ>
00098100000<FS>665.42<ETX>n
<ACK><STX>RS01APPROVED 448968
<ACK> . p
<ETX><BEL> <FF><CR>5r m
EVENT #4: 10/07/04 13:28:22 CONNECT 1200 @175505039 103 bytes
<STX>12345687900987654321<FS>A4411660000091047-030410100
<ENQ>
```

## Attacker Injects Commands to Trip DNP3, Modbus®, IEC 60870, You Name It!

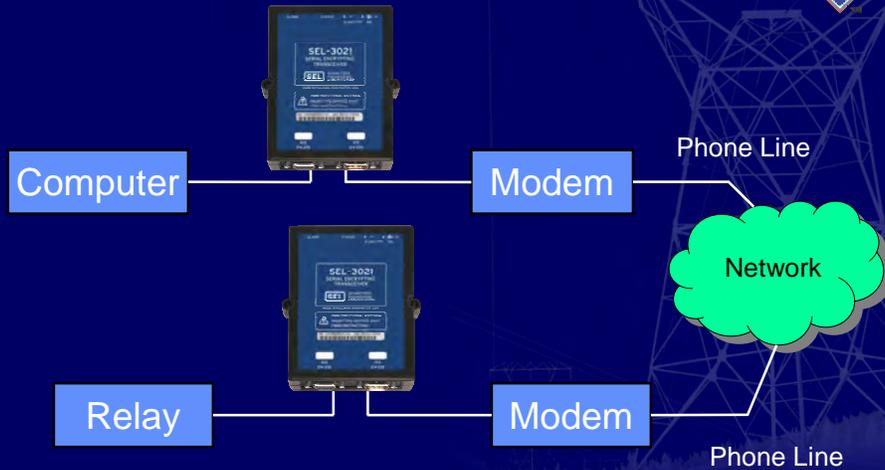


## A Simple Solution Is to Encrypt

- Confidentiality send messages over an unsecured medium without exposing contents
- Data authentication assures data were not altered in transit
- Session authentication unambiguously determines origin of communications session

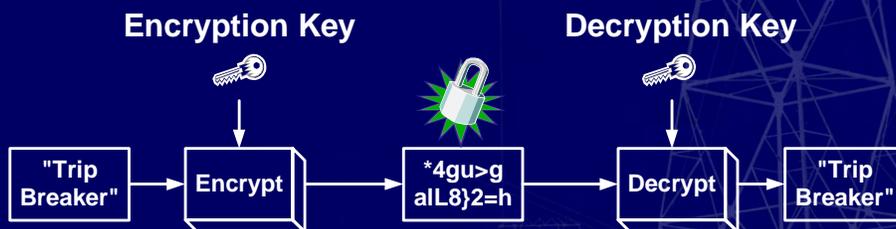
## How to Encrypt?

SEL-3021 Serial Encrypting Transceiver is a "bump-in-the-wire" solution

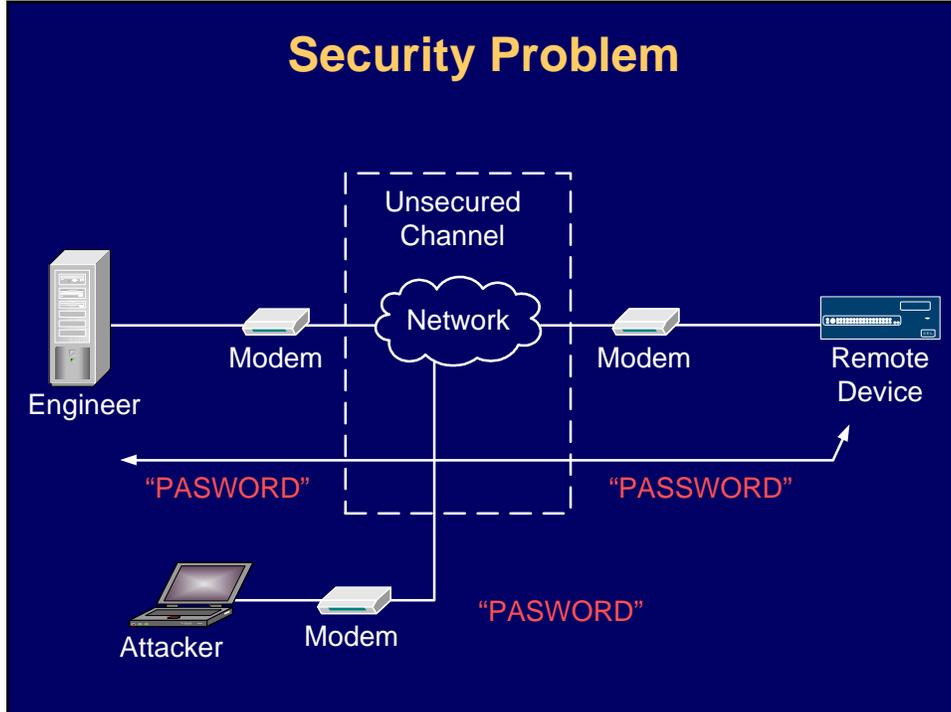


## How Does It Work?

Encryption functions scramble message in a way that is reversible



## Security Problem

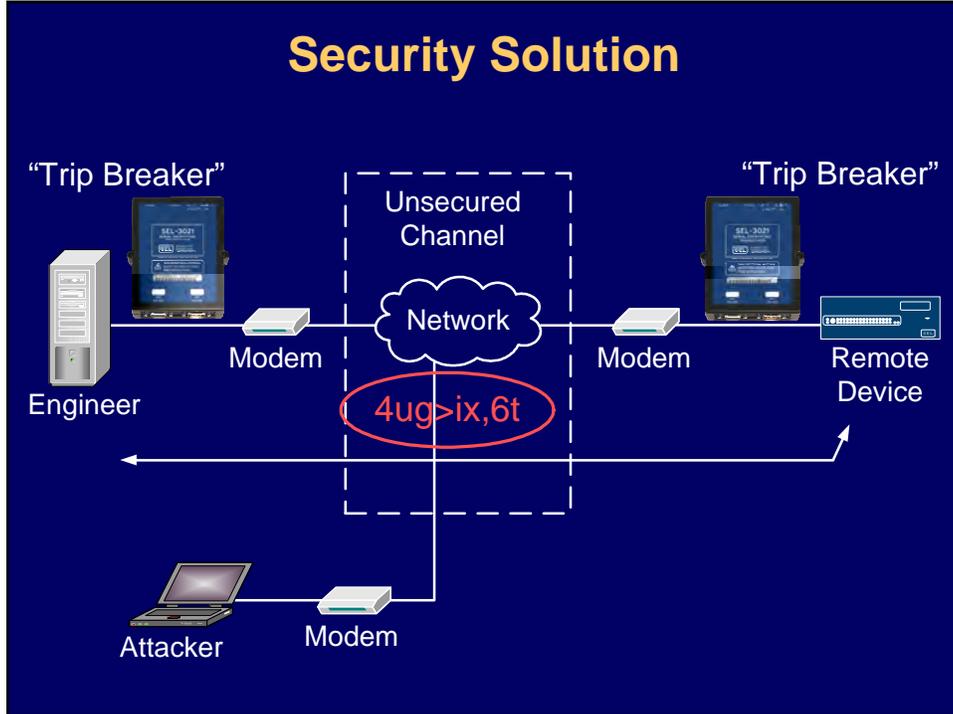


## SEL-3021-2 Provides Message Authentication Protocol (MAP)

- Offers four cipher protocol suites
- Provides data authentication
- Includes session authentication
- Supports mixed-mode operation
- Logs access attempts and settings changes



## Security Solution

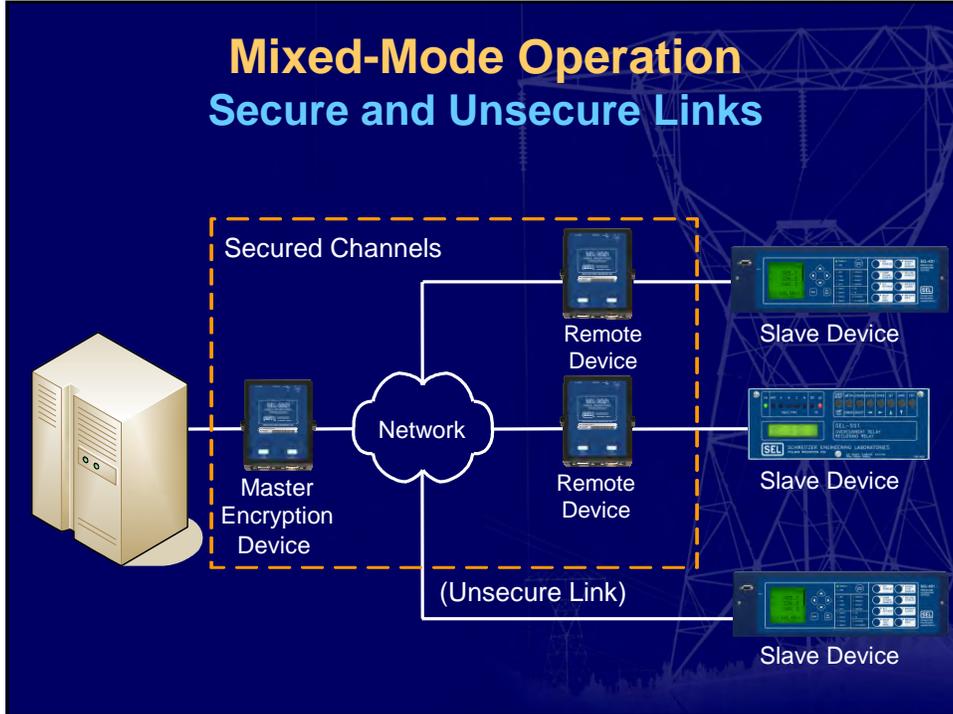


## Management Port Options

- New USB management port: simple, wired connection with AES encryption and HMAC SHA-1 authentication
- Standard 802.11b wireless management port



## Mixed-Mode Operation Secure and Unsecure Links



## Data Authentication HMAC / SHA-1 and SHA-256

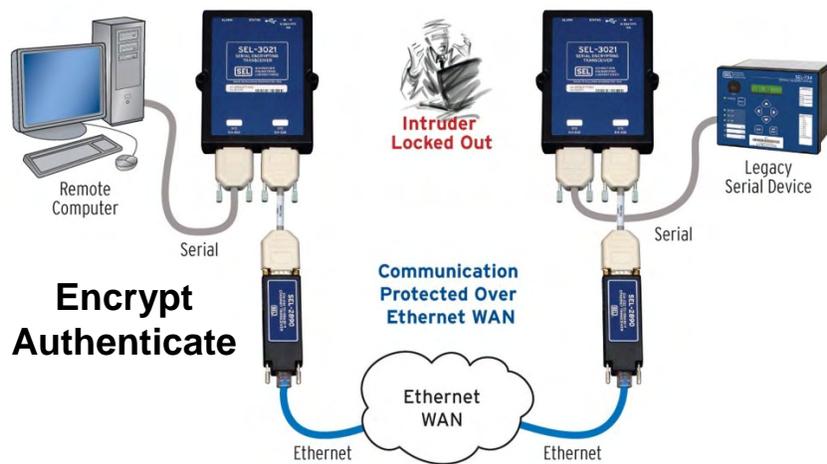
- Data authentication
- Data integrity

## Secure Ethernet for Serial Devices

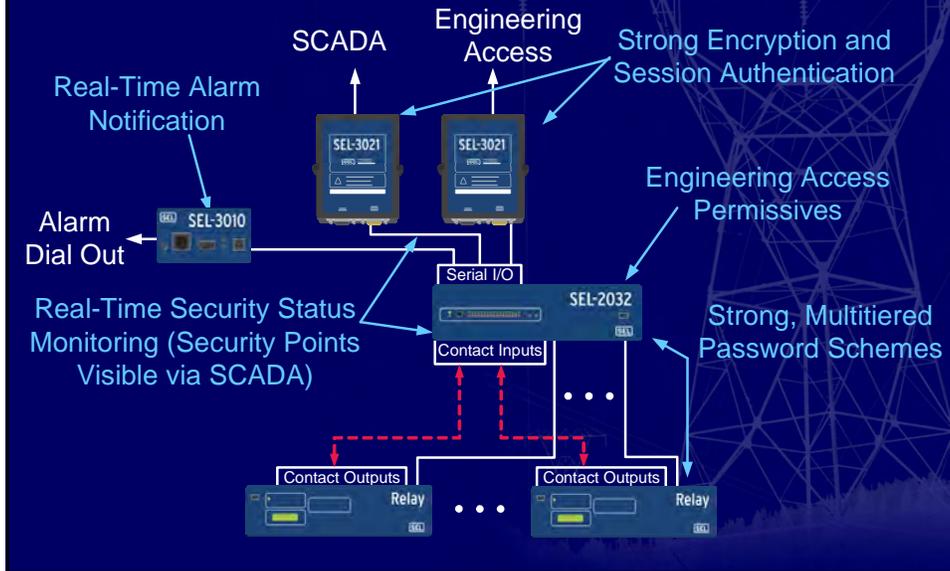
Use SEL-2890 Ethernet Transceiver and SEL-3021-2 for secure Ethernet communications for legacy devices



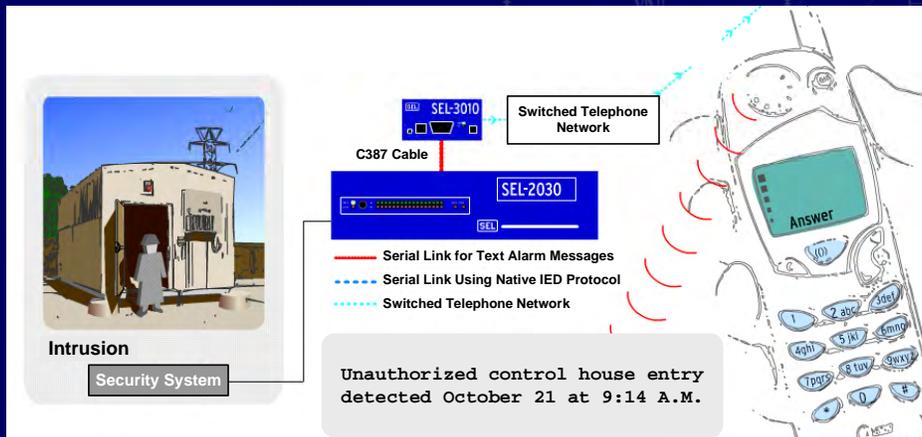
## SEL-2890 and SEL-3021-2



## Example: Defense in Depth

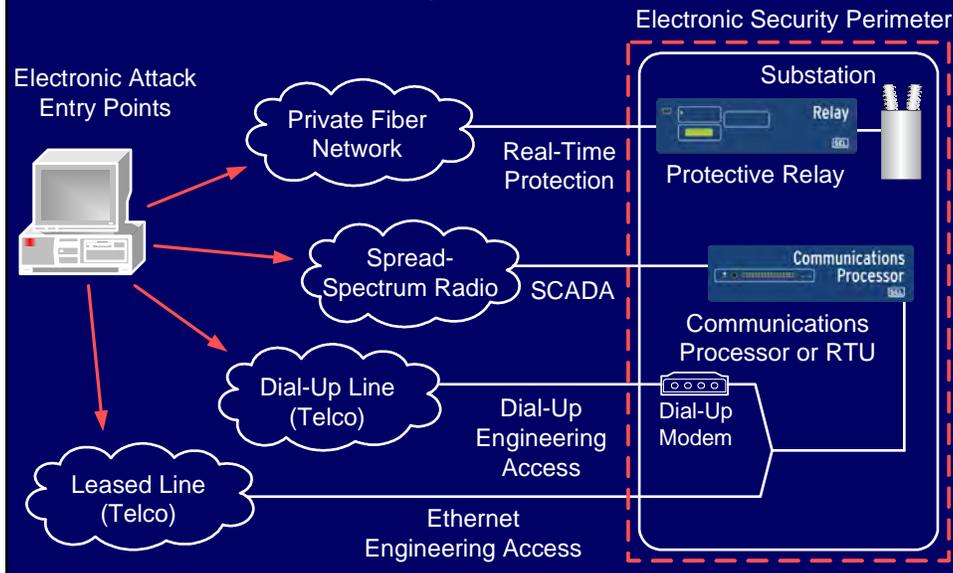


## SEL-3010 Event Messenger Delivers Station Alarms



SEL-3010 sends dynamic information to alert numbers you choose – not just canned messages!

# Identify and Defend Your Electronic Security Perimeter!



## Security Tips and Myths Edmund O. Schweitzer, III



**SCHWEITZER ENGINEERING LABORATORIES, INC.**  
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA  
Phone: 509.332.1890 • Fax: 509.332.7990  
www.selinc.com • info@selinc.com

### Twelve Tips for Improving the Security of Your Assets

Edmund O. Schweitzer, III  
August 25, 2006

From the very beginning of SEL, I have stressed the importance of the security of SEL relays, communications processors, meters, and other equipment. From our very first products, we have provided two levels of access with separate passwords, and alarm contacts which signal access failures. For many years, we have emphasized the importance of security in integrated systems, and have published many papers describing the threats, attack scenarios, and practical mitigation. In addition, SEL University offers a cybersecurity course, and SEL has several secure-communications products.

In recent years, cybersecurity has become increasingly important. Too many of us have had negative personal experiences, including identity theft, phishing, denial of service attacks, viruses, credit card fraud, and bank fraud.

## Conclusions

- Malicious attack opportunities may be numerous, but security can be implemented for zero or low cost
- Use strong pass-phrases
- NERC and FERC regulations recommend you define an electronic security perimeter
- Encryption devices can secure your current system
- Alabama Power is using SEL-3021 to secure remote engineering access rather than removing modems from substations

Questions?

