Utility and Substation Physical Security
Who is WESCO/CSC

• **WESCO Distribution, Inc**
  – WESCO is a leading distributor of electrical construction products and electrical and industrial maintenance, repair and operating (MRO) supplies

• **Utility Solutions Division**
  – WESCO also provides sourcing, supply, and materials management for maintenance and power plant operations. WESCO the optimum choice for streamlining procurement practices.
    • Investor-Owned Utilities (IOUs)
    • Municipals (Munis)
    • Rural Electric Co-Operatives (Co-Ops)

• **Communication Supply Corp (CSC)**
  – Founded in 1972, Communications Supply Corporation is a leading nationwide distributor of low-voltage network infrastructure and industrial wire and cable products. Through a network of 32 branch offices, CSC distributes a full range of products to support advanced connectivity for voice and data communications, access control, security surveillance, building automation, and video distribution
What We’ll Cover Today

• Regulations, mandates
• Physical Security – what it is and isn’t
• Your security goals and how to meet them
• Overview of technologies that can help
• Tying it all together is the key
In 2006, the Federal Energy Regulatory Commission (FERC) approved the Security and Reliability standards proposed by NERC, making the CIP (Critical Infrastructure Protection) Cyber & Physical Security Standards mandatory and enforceable across all users, owners and operators of the bulk-power system.

NERC – North American Electric Reliability Corporation

http://www.NERC.com
NERC – CIP 005 and 006

NERC-CIP 005-2
Standard requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter.

NERC–CIP 006-2
Standard is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

• IP Cameras
• IR Cameras
• NVR’s
• Monitors

• Alarm Cable
• Control Cable
• Access Control
• Perimeter Protection

Critical Infrastructure Protection (CIP) guide the protection of both Physical & Electronic Cyber Assets have mandatory compliance dates no later than December 2010.
Preparation for “Life under NERC – CIP”

- NERC CIP is not complete
- Plan to improve security of systems / procedures
- Basic implementation
  - Identity critical Cyber Assets
  - Establish a secure perimeter
  - Identify, screen and restrict personnel accessing info via Access Management System
  - Install video to track access in and out
- Success = tools and processes that are not burdensome on operations and easy to maintain
Beyond NERC - CIP

• Don’t do it just for compliance reasons
• Conduct a threat level assessment
• Define the critical assets
• Define the area where the assets reside
Security 101
Making Your Grid Smart & Secure
## What is Physical Security?

**Physical Security**

**Goals:**
- Keep bad guys out of facility and off of property – safety concerns
- Physically keep them away from the network and computers
- Track/Log who came in and out

**Tools:**
- Video Surveillance
- Card, Biometric Authentication
- Perimeter Detection
- Notification – Alerts, lights, horns

## Logical/Cyber Security

**Goals:**
- Keep bad guys off network and computer systems
- Hackers, Viruses, SPAM, Denial of Service Attacks, Stolen logins
- Access logs, audit trails

**Tools:**
- Firewalls
- Access Control Lists (ACLs)
- Authentication tokens
- Encryption
Overlap

Physical and Logical Security systems don’t need to remain completely separate.

Physical Security
- Video Cameras
- Perimeter Detection
- Lights, Horns

Logical Security
- Access Cards
- Biometrics
- INTERCEPTOR
- Firewalls
- Encryption
- ACLs

Some tools can be used to support both Logical and Physical security systems.
Focus for Today is on Physical Security

Physical and Logical Security systems don’t need to remain completely separate.

Some tools can be used to support both Logical and Physical security systems.

Physical Security
- Video Cameras
- Perimeter Detection
- Lights, Horns

Logical Security
- Access Cards
- Biometrics
- INTERCEPTOR
- Firewalls
- Encryption
- ACLs

CSC Communications Supply Corporation
A Subsidiary of WESCO Distribution, Inc.

WESCO Confidential – Do not copy or distribute without express permission from WESCO Distribution, Inc.
Physical Security helps you detect and identify threats and restrict access to sensitive computer system equipment rooms.
What are your goals for the system?

- **Detect**
  - Be alerted to unauthorized entries or attempts
  - Be alerted to mechanical/electrical failures
  - Be alerted to remote site entry requests

- **Identify**
  - Remotely view facility, people, equipment
  - View recorded information and events
  - Restrict and allow entry to facility
  - Create physical facility access logs
  - Prosecute offenders

- **Restrict**
  - Keep the bad guys out
Detection

• Reasons to employ detection technologies
  – Early warning alerts
    • Someone, something is approaching restricted area
      – Generally doesn’t differentiate, threat or no threat
    • Train cameras, attention to detected object
      – Alert humans to assess situation
      – Correlate other inputs to determine threat level
      – e.g. someone cuts/climbs fence

  – Detect / Alert for Potential Operational Abnormalities
    • Used in the absence or constant human surveillance
    • Computer software used to recognize “behaviors”
      – Images and patterns that potentially represent concerns
      – e.g. Area that is hotter than normal = potential fire
      – e.g. Worker in area that no one should be in
Detection Technologies

- Fence detection – approach, cut, climb
- Motion detection
- Video Analytics software
- Infrared cameras and sensors (PIR)
- Photobeam, Fiber Sensing, Microwave detectors
- Object tracking cameras
- One or more of these technologies can be applied to meet the facility’s specific needs
• **Perimeter Security**
  - World’s leading manufacture of Fiber-optic Sensors

**Fiber SenSys**

**High Performance - High Reliability - High Security**
Advantages of Fiber

- **Difficult to defeat.**

- **Sensor cable cannot be detected when buried below the ground or embedded in a wall.**

- **The system requires little or no maintenance.**

- **Long service life (greater than 20 years).**

- **Resistant to most environmental effects (wind, high temperature, etc.).**
How it works

Fiber optic sensing cable is *glass*.

– Inner conductor, called the *core*, conducts light

Light waves are conducted by the glass core

**High Performance - High Reliability - High Security**
How it works

If the fiber optic cable is disturbed, the pattern of conducted light changes.

- Sensitivity to motion, vibration, or pressure
- The propagation of light through the fiber is altered
Very small changes in the multimode speckle pattern are detected and analyzed by the system’s digital signal processors.
The sensor cable is deployed as an intrusion detection barrier along a site perimeter.

The sensor cable can also be buried covertly in a serpentine pattern in gravel or under controlled areas in the ground that have been factory approved.

Common barriers: chain link fences, ornamental fences, anti-climb fences, walls, rooftops, and ceilings.

High Performance - High Reliability - High Security
Deployment

Daisy-Chain Deployment (low security)

Loop-Back Deployment (medium security)

High Security Deployment
Each intrusion detection system is composed of two main components:

• **An Alarm Processing Unit (APU)**
• **Fiber optic sensor cable***

• **Sensor cable is inserted into flexible, protective conduit for use in fence line applications**
• **Hyperion is used to program APU with tuning software**
System Components

High Performance - High Reliability - High Security
Programming

AutoTune™

• Calibrate your perimeter protection system as effectively as the most experienced technician.
• AutoTune™ is uniquely designed to derive tuning parameters that are as effective at minimizing nuisance alarms and maximizing the probability of detection as the most experienced service technicians.
• It’s that simple: once you’ve installed the AutoTune™ software and calibrated your system, AutoTune™ uses the data to “learn” what climb and cut alarms look like at your particular installation and at the channel or zone being tuned.
Software
APPLICATIONS

Aviation Perimeter Applications
APPLICATIONS

Versatile Perimeter Barrier Deployment Options
APPLICATIONS

Energy/Utility
APPLICATIONS

PetroChemical & Large Perimeter

[Images of industrial petrochemical facilities]
DOE EXPERIENCE

- Sandia National Laboratories – Tested, certified for approval and implemented
- Los Alamos National Laboratory
- Y-12 National Security Complex at Oak Ridge, TN
- Savannah River Site
- Idaho National Laboratory
- Pacific Northwest National Laboratory
- Bonneville Power Administration
- Lawrence Livermore National Laboratory

* Fiber SenSys has the only fiber-optic intrusion detection system that is Priority Level 1 Nuclear Approved
UTILITY DEPLOYMENTS

- Portland General Electric
- Southern Electric
- Allegheny Power
- American Electric Power
- Bonneville Power Administration
- Boston Edison
- East Bay Municipal Utility District
- Progress Energy
- Entergy
- Gulf Power
- PacifiCorp (including Portland General Electric and Utah Power)
- Sacramento Municipal Utility District
- Southern Companies (Georgia Power)
- SCANA
Differentials

**High Security**
- Only fiber optic solution that is PL-1 Nuclear Approved by USAF
- Only sensor Certified PDS by USAF
- Active Seals Sandia National Labs Approved

**High Performance**
- Superior operations in robust conditions
  - EMI/RFI Immune
  - Temp Hardened
  - Corrosive environ.
- Advanced DSP-based algorithm provides most precise tuning
- Industry leading NAR/FAR

**High Reliability**
- Designed for 20 year lifespan
- Centralized power and comm eliminates field infrastructure
- Designed for rapid and reliable field installation
- Lowest “Total Cost of Ownership” (TCO) in the industry
Protect/Detection for Logical/Cyber Assets

SIPRNET (Secret Internet Protocol Router Network)
SCIF (Sensitive Compartmented Information Facility)
SCADA (Supervisory Control and Data Acquisition)

Transmission of National Security Information must be protected by one of the following methods:

1. Encryption
2. Protected Distribution System (PDS)
   A. Hardened PDS
   B. Alarm Carrier System
Interceptor: Not a Traditional Alarm Carrier System

Shortcomings of traditional alarm carrier:

• Traditional Alarmed Carriers morphed from perimeter security systems - not developed with data security in mind

• Traditional Alarmed Carrier monitors the *pathway* carrying the cables

• Requires a special sensing fiber

• No specificity to events: frequent false alarms - must be set very sensitive to detect intrusions into duct system

• Difficult to retrofit into existing cable systems when upgrading from unclassified to classified traffic
Interceptor™ Optical Network

Developed in part with DoD funding to monitor and protect the integrity and availability of C4ISR networks

- Monitors actual cables being protected to detect physical tampering or attempts to access them
- Learns network physical environment to eliminate false alarms
- Plug-and-Protect™ - setup in less than an hour
- 100% physical layer protection
  - Does not touch or process data
  - Usually installed on dark or unused fibers but works on active fibers too
  - No impact on network bandwidth
- Supports any network protocol - including 10GBase - and any fiber type (SM or MM)
- Interfaces with building security system through dry contact interface
  - Can also be monitored using SNMP traps, Ethernet
How Interceptor Works

• Interceptor turns unused, unlit, spare fibers into an internal “sensor” along an entire cable run
• This sensitizes the entire cable structure to intrusion
• Interceptor is installed on one end of cable

Monitoring as few as two fibers protects up to a 144-fiber “loose tube” cable
Works in a Variety of Applications

Closet-to-Closet Backbone

Dedicated Workstation
(Single User)

Zone Architectures
(SCIF / Workcenter)

Building Trunk Uplink

Works in a Variety of Applications
Comparison of Encryption, Hardened PDS and Interceptor with respect to cost, scalability and bandwidth...

Scenario: Provide SIPRNET Uplinks to Four End User Buildings
Encryption

Deployment Outcome
Cost: $45,000
Install Time: 1 Day
Lead Time: 6-9 Months
Bandwidth: <100MB

Capacity: 100Mbps

Uplink: 25 Mbps
User: <1 Mbps

Uplink: 25 Mbps
User: 12 Mbps

Uplink: 25 Mbps
User: 3 Mbps

Uplink: 25 Mbps
User: 4 Mbps

Uplink: 25 Mbps
User: 6 Mbps
Hardened PDS

Deployment Outcome
Cost: $800,000 x 4
Install Time: 6-8 Weeks
Lead Time: ~4 Weeks
Bandwidth: Unlimited

Concrete-Encased Duct Bank
A single Interceptor provides secure connectivity to all four buildings.

**Deployment Outcome**
- Cost: $24,500
- Install Time: 1 Hour
- Lead Time: < 6-8 Weeks
- Bandwidth: Unlimited
Summary Benefits:

**OSP Building-to-Building**
- **32%** cost savings vs. encryption
- **80%** cost savings vs. concrete
- Can be ordered and installed in <50% of the time it would take for either of the other solutions
- Can be added to a single link on Day 1 and then seamlessly added to the other three links with no further work or reconfiguration

**Indoor SCIF**
- **40%** cost savings for new deployments
- **20%** cost savings for legacy installations
- Improves building aesthetics - carrier can be hidden above the ceiling
- In some cases, carrier can be eliminated
- Eliminates the need for Periodic Visual Inspections (PVIs)
- Can be installed with minimal disruption to the facility
- Allows the upgrade of existing cables
Interceptor Approvals

• **NRO + ISR** - Special Access Program & Contractor Facilities
  – *Locations undisclosed*

• **DIA** - JWICS (vis CTTA/EMSEC Office)
  – *Deployed at CENTCOM, S. Korea, VA*

• **USAF** - Alarmed Carrier Approved Products List
  – *AFI 33-201 - Communications Security: PDS Systems*
  – *Deployed at MacDill AFB, Scott AFB and Pentagon*

• **Navy** - (via SPAWAR CTTA and NETWARCOM)
  – *Basewide deployment at NUWC*

• **Army** - Reviewed through the G6 IA process and approved for use (alarm carrier)
  – CRDA by INSCOM 2003

• **DHS** - HS Information Network
  – *Interceptor is standard for DHS NCR*

• **DOJ** - FBI SCION Network + Terrorist Screening Center
  – Deployed in Northern VA at multiple sites
**INTERCEPTOR is…**

...**Flexible**: Users can move INTERCEPTORs around or add additional INTERCEPTORs as needed and at will

...**Scalable**: INTERCEPTOR protection can easily be added to additional or new network links and does not create any bandwidth limitations

...**Reliable**: INTERCEPTOR provides consistent protection and performance with no false alarms.

...**Affordable**: INTERCEPTOR typically saves between 30-80% of the cost of deployment over encryption and hardened carrier PDS. On certain deployments, armored cables can be used in place of EMT for further savings.

...**Proven**: INTERCEPTOR has been reviewed, tested, approved, and deployed by several other DoD services and C4ISR agencies with impeccable performance and protection
Identification

• Goal: Specifically identify Who or What
• Its all relative…
  – Is it Sam or Samantha climbing the fence?
  – Was it Joe who forgot his access card at home that snuck in… or was it a bad guy who stole Joe’s card?
  – Who entered just before the system went down?
  – To be sure it is Joe before the system unlocks the door, what does Joe need to prove who he is?
    • Access Card
    • Thumbprint
    • PIN
    • All of the above

• Match the system with the threat level of the facility
• Everything can be done for a price $$
Identification Technologies

• Access Control Systems
• Readers: Card, PIN, Biometric, Iris, etc.
• Activity Logs
• Pan, Tilt, Zoom (PTZ) cameras
• High Resolution (HD) cameras
• Video Walls
Restriction Technologies

- Electronic Locks (Mag, Strike, etc.)
  - Provides security and remote locking control

- Access Control Panels and Software
  - Programming determines access by:
    - Individual (need to accurately identify)
    - Privileges – restricted to certain areas in facility
    - Time of Day
    - Group control eases configuration burden
Physical Security Products at the Substation

Physical Security for Substations

Legend:
- Power Grid
- Communications Network

NVR's Monitors

Regional Transmission Operator

Fence - protecting all assets

IP Cameras
IR Cameras
Thermal Imaging
PODS
Alarm Cable
Control Cable
Access Control

Fence - protecting all assets

Consumers:
- Industrial
- Commercial
- Residential

Power Generation

Transmission Substation

First layer of hardened electronics

Distribution Substation(s)

Distribution Control Center

IP Cameras
IR Cameras
Thermal Imaging
PODS
Alarm Cable
Control Cable
Access Control
# Security Technologies

<table>
<thead>
<tr>
<th>Technologies and Resources</th>
<th>Threat Level Potential</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CRITICAL</td>
</tr>
<tr>
<td><strong>Detect</strong></td>
<td></td>
</tr>
<tr>
<td>On-site Guard Service</td>
<td>X</td>
</tr>
<tr>
<td>Infrared Cameras</td>
<td>X</td>
</tr>
<tr>
<td>Video Analytics Software</td>
<td>X</td>
</tr>
<tr>
<td>Object Tracking Cameras</td>
<td>X</td>
</tr>
<tr>
<td>Motion Detection System (within premises)</td>
<td>X</td>
</tr>
<tr>
<td>Door/Gate Contacts</td>
<td>X</td>
</tr>
<tr>
<td>Perimeter Detection System</td>
<td>X</td>
</tr>
<tr>
<td><strong>Identify</strong></td>
<td></td>
</tr>
<tr>
<td>Biometric Access Readers</td>
<td>X</td>
</tr>
<tr>
<td>24 hour Video Surveillance (local or remote)</td>
<td>X</td>
</tr>
<tr>
<td>High Resolution (HD) Cameras</td>
<td>X</td>
</tr>
<tr>
<td>Pan, Tilt, Zoom (PTZ) Cameras</td>
<td>X</td>
</tr>
<tr>
<td>Video Display Wall</td>
<td>X</td>
</tr>
<tr>
<td>High Speed Video Recording/Playback System</td>
<td>X</td>
</tr>
<tr>
<td>Activity Logs</td>
<td>X</td>
</tr>
<tr>
<td>Access Control System</td>
<td>X</td>
</tr>
<tr>
<td><strong>Restrict</strong></td>
<td></td>
</tr>
<tr>
<td>Walls</td>
<td>X</td>
</tr>
<tr>
<td>Barriers</td>
<td>X</td>
</tr>
<tr>
<td>Perimeter Fence</td>
<td>X</td>
</tr>
<tr>
<td>Access Control System</td>
<td>X</td>
</tr>
<tr>
<td>Electronic Locks</td>
<td>X</td>
</tr>
</tbody>
</table>
Increased Deployment of IP

- Low Voltage Systems
  - Data
  - Phones
  - Sound
  - Surveillance
  - Access Control
  - HDTV over IP

- Upgraded Bandwith

- New Standards
  - POE (IEEE 802.3af “Power over Ethernet”)

- IT Professionals
  - Delivery of Information
The Move From DVRs to Open Systems

Open Systems – Infrastructure – Scalability – Integration – Cost efficiency
Why IP?

Level of image clarity
- Interlaced
- Progressive

Resolution
- Analog
- Megapixel
Thermal Technologies

Thermal Cameras can be added for detection of threats or abnormalities.
Advantages

- IP Surveillance also offers significant advantages over standard Analog CCTV
  - Unlimited scalability
  - More cost efficient network infrastructure
  - Network convergence
  - Systems integration
  - Remote accessibility
  - Intelligence at camera level
  - Increases reliability
  - Lower system cost
Working Together

• Nothing does it all…
• To accomplish all of your goals
  – Multiple systems are needed
  – Integration between systems is required
• IP based systems = easier integration
  – Standard interface for communications
  – No geographic proximity requirement
Why you need a Security Partnership

• The right integrator
  – Certified Solutions
  – Can they bond the job?
  – Are they qualified?
  – Do they have the experience?

• The right product
  – What are you expectations and will they be met?
  – Does it fit your needs?
  – Can it grow with you?
  – What about your legacy equipment?

• Delivery
  – Will it be there when you need it?
  – Staging in our warehouse for delivery
  – Kitting
  – Pre-build
    • Reduce labor hours on the job
    • Plug and play installation
    • Speed of installation
CSC’S Bundled Security Solutions

We are the Facilitators
Recap

• Determine needs – based on threat potential
  – Detect
  – Identify
  – Restrict

• Leverage resources (WESCO)

• Select technologies and to meet your needs

• Utilize IP technologies to integrate systems
Thank You