Are Your People and Systems Protected?
Four Types of Threats

Intruder

Cyber

Weather

Electrical
Intruder Threats

- Two Sources
  - Animals
  - Individuals
    - Malicious Intent
    - Non-Malicious Intent
Emerging Standards

We are living in a world of heightened security concerns where mitigation of risk and separation of responsibility is a fine line.

- Critical infrastructure must be protected
- New government regulations are driving security standards
- Technology that supports security is evolving in significant ways
- Organizations must align or comply with security regulations and standards.
  - DHS
  - EPA
  - DOE
  - CFATS
  - City Policies
  - HSPD-7
Water Facility Security Issues

**Targets:**
- Waste Water Treatment Plants
- Elevated Storage Tanks
- Pump Stations
- SCADA Systems
- Administration & Support Facilities
- Water Dams
- Chemical Storage Tanks

**Implications**
- Physical Equipment Damage
- Property Theft
- Water Contamination (chemical / flammable)
- Water System Disruption
- Harm to workers or public
- Bad Press
Physical Security System Goals:

1. **Deter/Detect/Delay**
2. Communicate
3. Assess & Respond

**Before 2001**
- We had a fence with a lock
- But the gates were open

**After 2001**
- Minor Changes
  - Cameras
  - Gates
  - Readers
  - Guards

**After 2005**
- Adding Smart Systems
  - ISS/SMS
  - PIDS
  - IVMS
  - Mass Notification

Evolution of Security Solutions
3 Layered Security Concept

Outer Layer - Site Perimeter - 1

- Fencing, gates, barriers, protective lighting, intrusion detection, cameras, signs, video analytics
- **Deter**, detect & delay
- Define property line, channel people and vehicles through controlled points

Middle Layer - Building Exterior - 2

- Protective lighting, intrusion detection, locks, signs, security glass, access control, cameras, video analytics
- **Deter**, delay & detect

Inner Layer - Guest & Employee Area - 3

- Locks, access control, cameras, intrusion detection
- Value of asset protected at risk
- People, property, data at risk
- **Deter & detect**
Threat Timeline

FENCE PROTECTION

- Fence alarm triggers
- Zone ID'd
- Camera slews
- Threat assessed
- Response team alerted
- Maybe Intercepted

WIDE AREA SURVEILLANCE

- Alarm from radar
- Camera slews
- Tracking starts
- Threat assessed
- Response team alerted
- Fence alarm trigger
- Intruder Intercepted
Perimeter Detection

Advanced alarm detection to assist first responders

- Designed to detect intrusion at the perimeter
- Early detection is critical to aid first responders
- Should pin-point to a specific area
Video Surveillance

Video management systems offer powerful benefits

- Simultaneous Digital & Analog Camera Integration
- Easy storage, search and control
- Integrated video analytics
- Integrated pan/tilt/zoom
- Fully Integrated with Access Control
- Coax, Fiber or Wireless
- Harsh Environments
CAMERAS

360 degree slew-to-cue functionality for identification and assessment
- Thermal/CCD
- Low-light CCD/spotlight
- Low-light CCD/IR Illumination

Spotlight is fully integrated the P/T/Z camera, provides up to 750 meters of visible light and features a non-lethal deterrent.

RADARS

Ground surveillance radars detects threats over wide areas
- 350 to 2800 meter radius

World’s most advanced and widely deployed ground surveillance radars
- nearly 1500 to date

Designed to work in virtually all weather conditions

High Probability of Detection

Low False Alarm
Integrated Video Management Systems

- Object Recognition
  - Ignores Extraneous Movement

- Rules Based
  - Track Objects
  - Alarms

- Detect

- Interface
  - Aerial Map
  - Integrates with Other Equipment
  - Advanced Forensic Searches

- Analyze

- Cameras & Radar
  - Point & Click Camera Control
  - Thermal
  - Low False Alarm Rates
Video Analytics

**Video intelligence actively monitors your site**

- Can replace/enhance other intrusion detection system
- Automates system response
- Improves guard response
- Reduces false alarms
- Fully integrated into the access control system
- Fully integrated into the video surveillance system
Feature-rich solutions designed to meet stringent security requirements and regulations

- Focal point of system
- Network based
- SCADA Communication
- Alarm management
- Secure & encrypted communications
- Easily control access points such as:
  - Doors
  - Gates
  - Production areas
  - Muster stations
- Fully integrated with video
- One card solution with biometrics
- VOIP Intercom (Local & Remote)
Deterrence

- **Passive**
  - Pad Locks
  - Fences

- **Active**
  - Lights
  - Alarm horns

- **Aggressive**
  - Long Range Acoustic Device
    - High Decibel sound drives away intruders
Weather
Weather Impacts

● Road impacts
  ● Ice
  ● Flooding
  ● Wind Damage

● Process impacts
  ● Power outages
  ● CSO impacts
  ● Service Outages

● Operations
  ● On-site repairs
  ● Emergency Scheduling
Traditional Weather Service Challenges

- Designed for Mass Market
  - “50% chance of rain in the afternoon”
  - Forecast is for an area.
    - Zip code
    - Metropolitan area
- Tough to access real time
  - Watch TV for Tornado tracks
Customized Weather Service Advantages

- Designed for Better Interaction
  - Exact time of storms
  - Street level storm track
  - "Future Weather"
    - 10-120 minutes into the future
  - Access to traffic cameras.
  - Lightening strike mapping
Lightning Management

- **Field Work**
  - General Rule: Halt work at sound of thunder
  - Inaccurate: City vs. Rural
  - Better Tool: Use proximity alarm
    - Sends SMS if lightning is in range
  - Result: Work progress based on real risk
- **Insurance**
  - Some companies require proof of lightning strike
  - Arc Flash Damage is Similar
  - Some policies do not cover Arc Flash Damage
- **Lightning Strike Mapping**
  - Shows when, where, and magnitude of strike
How does weather save energy

- Energy is more than electricity
  - Fuel
  - Labor
- Scenario #1
  - Northern part of your system is vulnerable to storms.
  - Real time, and future weather, shows storm heading south
  - No need to “call out the troops”
- Scenario #2
  - Ballasted Flocculation system in CSO application.
  - Traditional weather service: Chance of PM storms
    - Thus start system at noon
  - Telvent Weather shows storms arriving at 3:45
    - Thus start system at 3:30
Other benefits

- Insurance companies want lightning damage proof
- Realize that Arc Flash damage appears similar
- Storm tracking may allow deployed people to work
THE SKY IS FALLING!!!!

● Media Filled With Doomsday Articles
  ● Partly Justified, Mostly Hype

● Perception Is That We Are Vulnerable
  ● Somewhat True

● Perception Is That We Are Helpless
  ● Not True
A Tale of Two Worlds

**IT World**
- Must have open access
  - Hardware options limited
  - Network options limited
  - Software/Firmware primary means of mitigation

**Control World**
- Can restrict access
  - Hardware options available
  - Network options available
  - Software/Firmware NOT primary means of mitigation

Most Cyber Security Experts Come From The IT World, And Do Not Understand The Control World.
IT vs. Control in WWW facilities

**IT**
- City Webpage
- City Email
- City Databases
  - Includes access to SCADA Database

**CONTROL**
- WWW Control Network
  - PLC’s, Drives, Starters
  - RTU’s
  - Includes access to SCADA Database
What is Cyber Security

- Cyber Security implementation is a **solution** and not a product
  - People, Policies, Architectures, Products

- Cyber Security requires a **multilayer** or Defense in Depth (DiD) approach
  - Security Plan, Network Separation, Perimeter protection, Network Segmentation, Device Hardening, Monitoring & Update

- Vendor’s responsibilities
  - Design products & solutions with security features
  - Ensure they enable customers to comply with security standards
  - Provide recommendations and methodologies to guide implementation

- End User’s responsibilities
  - Define security procedures (organizational security)
  - Mandate responsible people (personal security)
  - Ensure compliance with security standards
How to “Secure” a System

- Protect the perimeter
  - Routers, Firewalls, VPN
- Segment the network
  - DMZ between Trusted Zones
  - Segments within Trusted Zones
- Protect the computers
  - AntiVirus, White-listing, Access control
- Harden the controllers / devices
  - Device security, External protection
- Monitor and React
  - Logs, traffic monitoring, alarms
  - Act on unauthorized events

Policies and Procedures, Staff Training, Secure Architecture
How to “Manage” a Secure System

- Keep the computers protected
  - A/V protection
  - Appl. White-listing
  - Administer access control

- Monitor Device Hardening
  - Device settings
  - External devices

- Monitor traffic, log users, log events, and trap alarms

- Act when unauthorized events occur

- Patch! Patch! Patch!
What is a cyber security vulnerability?

- A cyber security issue with a product or system that could allow the system to be attacked.

- Security researchers are exposing product vulnerabilities
  - Profit, publicity
  - To force improvements by vendors

- Vulnerabilities are very common
  - Microsoft fixes 10-50 each month
  - Over 500 vulnerabilities predicted in Industrial Control Systems in 2012.
Common Attacks / Vulnerabilities

- Logic Bombs
- Denial of Service
- Network buffer overflow
- Input buffer overflow
- Backdoor account
- Password attacks
- Man in the middle
- Replay attacks
- Social engineering / phishing
- Exfiltration of data
- Rootkits
- DNS / Bootp / Service impersonation
- Web based – XSS
- Web based - traversal
What to do with a Vulnerability

- Acknowledge to customers that vulnerabilities occur on all vendors' products.

- Explain vulnerabilities need to be analysed to understand their impact on a system.
  - A PLC command vulnerability on FTP is only an issue for a system if FTP access is allowed from untrusted people that will send that command.

- Show the mitigations that they can take until the vulnerability is removed.
  - Use firewalls when needed.

- Update the customer when a patch is released.
Schneider Electric’s Recommendation

The “Defence in Depth” Approach (DiD)

6 key steps:
1. Security Plan
2. Network Separation
3. Perimeter Protection
4. Network Segmentation
5. Device Hardening
6. Monitoring & Update
Defense-in-Depth Step #1: Security Plan

- Define:
  - Roles and responsibilities.
  - Allowed activities, actions and processes.
  - Consequences of non-compliance.

- Full network assessment:
  - Communication paths.
  - Audit of all devices.
  - Security settings.
  - Network drawings.

- Vulnerability assessment:
  - Potential threats.
  - Consequences.
  - Risk assessment and mitigation.
“Defence in Depth” Step #2: Network Separation

● Separate the Industrial Automation & Control System from the outside world
  ● Create a ‘buffer’ network (DMZ) between the IACS network and the rest of the world, using routers and firewalls
  ● Block inbound traffic to the IACS except through the DMZ firewall
  ● Limit outbound traffic to essential and authorized traffic only

● DMZ host for servers
  ● Vijeo Historian mirror
  ● Web servers
  ● Authentication server
  ● Remote access server
  ● Anti-virus server
  ● Patch management server

Connexium
Eagle 20
ETG Routers
Hirschmann
Routers, Mach, Mice
“Defence in Depth” Step #3: Perimeter Protection

- Protect the Industrial Automation & Control System perimeter using a firewall
  - Validate packets and protocols
  - Manage authorization of certain data packets
  - Restrict IP address or user access via authorization and authentication

- Protect critical parts of the process with additional firewalls within the IACS

- Secure remote accesses
  - Use the VPN technology of routers and firewalls
  - Use the latest authentication and authorization technologies. They’re evolving fast.

Connexium Eagle
Connexium Tofino
ETG Gateways
“Defence in Depth” Step #4: Network Segmentation and Zones

- Create Security Zones
  - Limit and monitor access between zones.
  - Limits the effect of a security issue, alerts when an issue occurs.

- Use managed switches
  - Limit access to network packets.
  - Precisely segment the network using VLANs
  - Limit rates of ‘multicast’ and ‘broadcast’ messages to protect from DoS type attacks
  - Limit physical connections using port security

ConneXium Switches

Connexium Tofino Firewall
“Defence in Depth” Step #5: Device Hardening

- On all devices
  - Replace default passwords with ‘strong’ passwords
  - Shut off unused ports, communication services and hardware interfaces
  - Set up broadcast limiter functions
  - Use multicast message filtering
  - Avoid generating requests faster than system can handle

- On PCs and HMI terminals
  - Forbid or seriously control the use of any external memory

- On Unity Pro and Vijeo Citect
  - Set up all security features: passwords, user profiles, operator action logging

- On ConneXium switches
  - Restrict access on ports to assigned addresses only

- On remote I/Os
  - Restrict access to authorized PACs only

- Vijeo Citect PCs
- Vijeo Historian PCs
- Unity Pro PACs
- Magelis HMI terminals
- ConneXium switches
- Modicon STB I/O islands
- Altivar speed drives
- Any I/O or instrument on fieldbus
"Defence in Depth" Step #6: Monitor and Update

- Monitor, Manage and Protect service
  - 24/7 remote security monitoring
  - Configuration monitoring
  - Reporting for Audit Compliance
  - Network and Host Intrusion Detection systems

- Monitor
  - Authentication traps.
  - Unauthorized login attempts.
  - Unusual activity.
  - Windows Event Viewer.
  - Network load.
  - Device log files.

- Monitor, Manage, Protect Service
  - Citect Log Files
  - Unity Pro log files
  - PLC Event Viewers
  - PLC Diagnostics and access lists
Secure Reference Architectures

- How can I … Reduce Vulnerability to Cyber Attacks.

  - Risk Assessment, Security Planning, Recommended Architectures, Methods of Attack.

- Secure PlantStruxure architectures incorporating key security features
  - Network Separation and server locations
  - Perimeter Protections product and settings
  - Network Segmentation and security zones recommendations with data flows identified.
  - Device Hardening and Monitoring recommendations for PlantStruxure devices.
Electrical
Human Impact of Arc Flash and Arc Blast

- 5-10 US Arc Flash incidents per day – Cap Schell, Inc

Injuries
- Minor to 3rd degree burns
- Blindness
- Hearing loss
- Nerve damage
- Cardiac Arrest
- Death
- “Bullet like” injuries
  - Molten metal velocity > .38 special

Cost
- $1,500,000 average treatment cost
- $8-$10 Million total cost including litigation.
Non-Human Impact of Arc Flash and Arc Blast

- Downtime
- Negative media impact
- Political Fallout
- Equipment damage
- Unanticipated budget impact
- Regulatory fees
  - EPA
  - OSHA
What Do The Regulations Say?

- NFPA 70E has specific requirements
- All water and wastewater utilities must comply
- Requires Training for workers
- Mitigation = Three Steps
  - Tools for safe work
  - Warning labels on equipment

NFPA 70E is law and enforceable. Thus, Facilities must take steps to comply
Who is responsible for implementation

- Facility responsible for proper
  - Training of staff
  - Tools
  - PPE
  - Procedure
- Employee responsible for proper utilization of the above

Who should be trained? Anyone that could operate or maintain electrical equipment
Three Parts of Arc Flash Mitigation

- Eliminate
- Reduce
- Protect

COMPLETE PROTECTION

Partial

Schneider Electric - Division - Name – Date
Eliminate The Risk

- Turn Off The Power
- Lock Out / Tag Out
Three Parts of Arc Flash Mitigation

- Eliminate
- Protect
- Reduce
Arc Flash Reduction

- Temporarily decrease circuit breakers or protective relay settings
  - Protects by making device trip faster
  - Thus less energy propagated

- Use arc reduction equipment
  - Equipment designed to lower and restore settings automatically
  - Arc Termination equipment (Shown)
    - Creates a bolted fault that steals all energy from arc.
    - Opens breaker faster thus minimizing energy released.
Hazard Reductions

- **Remote Racking**
  - Racks breaker from a remote locations
  - Removes worker from Arc Flash area

- **Maintenance Settings Mode**
  - Breakers have maintenance settings
  - Allows for faster opening
    - Thus minimizes energy released
Three Parts of Arc Flash Mitigation

- Eliminate
- Protect
- Reduce

COMPLETE PROTECTION

Partial
Approach distance, and energy involved will determine what PPE is required.

Only qualified persons allowed within these boundaries.

From NFPA 70E 2009 Annex C, Fig. C.12.4
The right outfit for the right occasion!!

<table>
<thead>
<tr>
<th>Category</th>
<th>Cal/cm²</th>
<th>Clothing Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>N/A</td>
<td>Untreated cotton, wool, rayon or silk, or blends of these materials with a fabric weight of at least 4.5 oz/yd²</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>Arc Rated FR shirt &amp; FR pants or coverall</td>
</tr>
<tr>
<td>2</td>
<td>8</td>
<td>Arc Rated FR shirt &amp; FR pants or coverall</td>
</tr>
<tr>
<td>3</td>
<td>25</td>
<td>Arc rated FR shirt &amp; pants or coverall, and arc flash suit selected so that the system arc rating meets the required minimum.</td>
</tr>
<tr>
<td>4</td>
<td>40</td>
<td>Arc rated FR shirt &amp; pants or coverall, and arc flash suit selected so that the system arc rating meets the required minimum.</td>
</tr>
</tbody>
</table>

Note that melt-able fabrics and other similar synthetics are never permitted.

Source: NFPA 70E 2009
Let’s Accessorize!

- Hard Hat
- Safety Glasses
- Ear Protection (not shown)
- Face Sock (Balaclava) for Category 2 (not shown)
- Wrap around safety shield (to protect forehead, neck, ears, etc.)
- Arc Flash Rated Leather Gloves
- Leather Shoes (not shown)

An Arc Flash Suit Hood instead of these items is also in vogue.

Refer to NFPA 70E 2009 Article 130 for clothing system details.