Cisco’s Physical Security & Surveillance Portfolio for Safety & Security

John Convy (jconvy@cisco.com)
Physical Security
Cisco Systems
Agenda

- Traditional Video Surveillance Technology
- Video Surveillance Technology Convergence Factors
- IP-Based Video Surveillance Technology
- Cisco PSBU Video Surveillance Products
- Cisco IP Cameras
- Cisco Physical Access Control
“…the physical security environment has been dominated by analog, stand alone control systems with limited interconnectivity, digital communications, or integrated management capability.”
Traditional Safety and Communication Systems

Access—Buildings

Monitoring

Alarms

Paging

Video

Voice

Radio
Example: Safety Incident with Traditional Systems

Chemical Spill at College Science Building Sends Fumes in the Air

1. Professor calls safety office to initiate response protocol.
2. Safety officer calls fire department.
3. Fire department closes building and calls for Hazmat.
4. Dean e-mails students to tell them class is canceled in science building.
5. Hazmat finds fumes are toxic & nearby areas are affected. Calls Dean.
6. Dean calls mayor to tell of community impact.
7. Mayor sends police to evacuate neighborhoods.
8. Nearby elementary school starts calling parents.
9. In-transit students show up to the building for class.
Traditional Systems Response

- Actions are linear
- Communication and decision support systems are independent
- Relies heavily on human intervention
Pain of Traditional CCTV

- Central station access only
  - No remote access
  - No on-scene collaborative access
- Investigation delays
  - Locate tape in archive
  - Ship from remote location
  - Review hours of video
- Low probability of threat detection and high false alarms
More Pain of Traditional CCTV

- Video value limited to security Installation costs of traditional coax or fiber
- Number of monitoring stations is limited as costly cabling must be duplicated
- Matrix switcher cannot be easily expanded without new hardware

Overall scalability, including the cost of expansion, is poor
“Convergence is not about the unification of security into one environment, but about collaboration between environments.”

Trends 2007: Physical and Logical Security Convergence
Forrester Research
Additional Convergence Drivers

IP-based physical security technology **takes advantage of existing network infrastructure**

Leverage network security **features** that authenticate users
Monitor rogue behavior
Implement **policy-based responses**

Industry groups are establishing technical **interoperability standards** between physical security systems and IT
Safety Incident: Converged Systems

Chemical Sensors Note Incident in College Science Building and Trigger Notifications via Multiple Mediums

College Safety Department

Parents of Children in Nearby School

Nearby School

Hazmat

FIRE

Local fire department

Dean

Local Police Department
Converged Systems Response

- Actions occur in parallel
- Communication and decision support systems are connected and trigger policy-related responses
- Less dependent on human intervention
Networked Technologies Enhance Campus Safety

- Location-Based Services
- Video Training
- Digital Signage
- Unified Communications
- Conferencing and Collaboration
- PSAP Integration
- Acoustic and Motion Sensors
- Building Monitoring
- Visitor Management
- Video Surveillance
- Campus Transportation Monitoring
- First Responder Monitoring
- Radio Interoperability
# Comparison of Analog and IP Video

<table>
<thead>
<tr>
<th></th>
<th>Analog</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired and wireless cameras for anytime, anywhere surveillance on campus</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Video recorded digitally for immediate access, enabling real-time incident response, investigation, and resolution on campus</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Control and monitoring can be transferred to any other point on the network</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Feeds can be digitally monitored to detect and flag incidents</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Supports existing analog cameras or newer, IP-based cameras</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Flexibility to add sensors and apply analytics (e.g., facial recognition detection)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Network keeps operating, even if one link or switch goes down</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Every device can be continuously monitored, and an alarm raised if anything fails</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Open, standards-based infrastructure enables deployment of new security applications and maximizes value of total system</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Lowest total cost of ownership</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
Overview of Video Surveillance Technology
Video Surveillance System Components: Matrix Switchers

- Routes multiple audio/video input signals to multiple output signals
- Facilitates the switching of more than one camera or VCR/DVR to more than one monitor or VCR/DVR
- Centralized resource in what is most commonly a Star based topology
- Support for remote monitoring is enabled by extending a link from the matrix and commonly faces a multitude of physical and cost related challenges
- Range in size from one RU to a dozen or more 19” equipment racks
- Expensive, frequently comparable on a price per port basis with large scale Ethernet switches
Video Surveillance System Components: Storage/Recording

- **Video Camera Recorder (VCR)**
  Outdated Technology, Poor reliability, requires manual operations

- **Digital Video Recorder (DVR)**
  Digitally compresses analog feeds onto a hard drive. “Digital” refers to the compression and storage, not transmission. Most likely collocated with the analog feed it records. Typically based on COTS PC hardware with vendor specific software. Frequently used as little more than a “Digital VCR”

- **Network Video Recorder (NVR)**
  Streams have already been digitally encoded and compressed at the camera/encoder. Can be PC software-based or appliance
  Can be located anywhere on a network—the monitoring center, adjacent to cameras, or in a hardened environment. Location is transparent to the operator
  Record and replay simultaneously, and recordings can be simultaneously viewed by multiple operators spread across the network
Video Surveillance System Components: Cameras

- **Fixed Cameras**
  - Type 1—lenses of different focal lengths and/or fixed or variable irises. Flexible configuration and used in most commercial CCTV systems
  - Type 2—fixed lens mounted on a camera circuit board (board camera), packaged in a small case, dome or tube
    - Low cost solution, particularly in a home or retail environment

- **Pan, Tilt, Zoom Cameras**
  - Rotate horizontally 360°, vertically through 90° with powered zoom can be set to auto-scan or move through range of pre-sets and zooms in weatherproof domes when used outside

- **Analog Cameras**
  - Use a continuous signal vs. digital, breaks everything into numbers
  - Scan viewing area a line at a time and convert the varying intensities of red, green and blue (RGB) light into analogous electrical signals

- **IP Cameras**
  - Equipped with an electronic photosensitive sensor
  - Typically supports multiple users, and web browser accessible
  - Located anywhere with a network connection (Wired/Wireless)
  - Few are actually natively digital
Video Surveillance System Components: Monitors/Displays

- Color or B&W—resolution higher than TVs
- Designed to be always on
- Analog CRT are most popular
- Digital (LCD/Plasma)—inferior image and Lifespan
- Size determined by application
- Comparative Resolution to IT centric displays is very different!
Video Surveillance System Components: Transmission Media

- Coaxial cabling (75Ω)
  - Most popular cable used
  - 90%–99% EMI protection

- Fiber Optic
  - Capable of longer distances
  - No interference
  - Immune to EMI—Better for outdoor
  - Resists lightning strikes

- Twisted Pair
  - CAT5/5e/6
  - Easiest to install
  - Requires transmitter and receiver
  - Baluns—From Coax to UTP/UTP to Coax

Cabling is more important with Video than most realize!
Video Surveillance System Components: Analytics

- Security Operators cannot effectively monitor multiple video monitors simultaneously. Studies have shown a 95% drop off in event detection after only 22 minutes of observation.
- Analytics process video to detect events.
- Integrated IP-based analytics:
  - Real time at the Camera or Encoder (IP Gateway)
  - Post-processing from an operator's PC on recorded video
  - Identify events as they occur and provide tools to analyze previous situations.
Video Surveillance System Components: Analytics

Sample Algorithms/Behavior Detection:

- Erratic/suspicious behavior—stopping at more than one car in a parking lot
- Congestion detection—too many people in a space
- Motion detection—object/person moving across a scene
- Abandoned object detection—suitcase abandoned in airport
- Wrong Way flow—object/person moving against a route
- Tripwire—detection and alarm upon breach of a defined line
- Shape-based detection—vehicle detection
- Object missing detection—object removed from a scene
Security System Components: Information Management

- What is Situational Awareness?
  Knowing what is going on so you can figure out what to do
  The ability to answer such questions as:
  - What is happening?
  - Why is it happening?
  - What will happen next?
  - What can I do about it?

- What is Domain Awareness?
  Combine People, Processes, Technology
  Effective understanding of anything associated with your domain that could impact the security, safety, or health of your environment
  Knowledge & Capability

- What does this do for you?
  Proactive versus reactive security posture
  Auditable, provable results
  Deliver—reduce costs
Video CODECs

Compression

Image Based:

JPEG/JPEG2000 (Typically measured in Thousands of Bytes)

MJPEG (Motion JPEG) (Typically measured in Thousands of Bytes)

Wavelet (Typically measured in Thousands of Bytes)

Video Based:

MPEG-2 (Typically 2–20 Mbps)*

MPEG-4 (Part 2) (Typically ~3 Mbps)**

H.264 (MPEG-4 Part 10 + Higher Coding efficiency)
(Typically 40-50% less than MPEG-4 equivalent)***

*Used for numerous applications and quality levels
**Four CIF at 25–30 Frames Per Second
***Four CIF at 25–30 Frames Per Second (CPU and Option Specific)
## Video Resolution

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>PAL</th>
<th>NTSC</th>
</tr>
</thead>
<tbody>
<tr>
<td>QCIF</td>
<td>640 x 480</td>
<td>176 x 120</td>
</tr>
<tr>
<td>VGA</td>
<td>800 x 600</td>
<td>800 x 600</td>
</tr>
<tr>
<td>SVGA</td>
<td>1024 x 768</td>
<td>1024 x 768</td>
</tr>
<tr>
<td>XGA</td>
<td>352 x 240</td>
<td>704 x 240</td>
</tr>
<tr>
<td>CIF</td>
<td>704 x 480</td>
<td>720 x 480</td>
</tr>
</tbody>
</table>
Resolution Comparison
CIF Resolution (352x240) vs. 1080i (1920x1080)
Resolution Comparison
D1 Resolution (720x480) vs. 1080i (1920x1080)
Resolution Comparison
720p Resolution (1280x720) vs. 1080i (1920x1080)
Resolution Comparison
1080i (1920x1080)
Do You See a Real Difference?

30 FPS CIF
30 FPS 4CIF

10 FPS CIF
10 FPS 4CIF
Example

2000 cameras; 24/7 storage for 30 days

All 2000 @ 30 fps; 4CIF

500 @ 30 fps; 4CIF
500 @ 7.5 fps; 4CIF
1000 @ 15 fps; CIF

$4 Million
1.2 Petabytes
(1,200 TB)

$1 Million
482 Terabytes
Cisco PSBU
Video Surveillance
Product Offerings
Cisco’s PSBU Transforms Security to IT

- Network video & security systems
- Use standard IT products
  - 100% Linux & Browser Based
  - COTS Servers, Storage
- Provide easy integration
  - Open API…built from the ground up for interoperability
  - Broad device and technology support
- Robust architecture
  - Extreme scalability
  - Patented streaming and proxy technology
- Total Solution
  - Encoding, Management & Application Servers
Single Site, Analog/Matrix Switch—Centric

- **Cisco Stream Manager**
  - Configuration
  - Monitoring
  - Recording and Archiving

- **Benefits:**
  - Enables new capabilities: faster response and resolution
  - Smooth migration from analog to digital to networked
  - No operator retraining
  - Interoperable with 3rd party analog systems
Remote and Multiple Sites, Network-Centric

- **Cisco Video Surveillance Manager**
  - Network-centric and Browser-based
  - Customizable Configuration, Monitoring, Recording and Archiving

- **Benefits**
  - Access live or recorded video anywhere, anytime
  - Highly scalable for easy expansion
  - Easy integration of applications
  - System and device flexibility and interoperability
Cisco Video Surveillance Manager
Open Architecture Video Surveillance System

[Diagram of a video surveillance system with various components and connections]

- Video cameras
- IP Camera (optional)
- SS (optional)
- Virtual Matrix Switching
- VM Client Station
- VM
- Local Viewer
- Remote Viewer
- Remote VM Client
- Site A LAN
- Site B LAN
- Media Server
- Encoding Server
- Storage System
- Operations Manager
- Virtual Matrix

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential
Open Architecture “Enables” Other App’s

- Digital Video enables other applications
- Need to deliver different video for different applications
  - Viewing; analysis, storage
Support for All Edge Devices

Bosch

Panasonic

Toshiba

Sony

IQinVision

EXACQ Technologies Inc.

Act

RVision

Optecom-NK

Verint

Arecont Vision

Pelco

Axis Communications

Cohu, Inc. / Electronics Division

Teleste

IOI

Lumenera Corporation

Mango DSP

IndaioVision

VBrick

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential
Video Surveillance Manager Overview

Video Management (MS and ES)
- Video Collection
- Video Routing
- Storage & Retrieval
- Event management
- Rules Engine
- C3/4 Integration

Video Storage (SS)
- DAS, SAN, NAS
- Local and Remote
- Loops and Events
- Redundant Archives
- Optional Clustering
- Hardware Agnostic

User Portal (OM)
- Video Viewing
- PTZ and Presets
- System Configuration
- User Management
- Reporting
- Event Display

Virtual Matrix Switch (VM)
- Single Control
- Multiple Displays
- Video Switching
- Video Wall

Operating Systems and Data Bases
- Linux, Windows XP
- MySQL, Oracle, dB/2

Communications
- Internet - Intranet - TCP/IP - HTTP(s) - RTP - RTSP

Common API

S - Media Server
S - Encoding Server
S - Storage System
M - Operations Manager
Video Surveillance Media Server (MS)
The Media Server Enables Distribution, Archiving and Management of Video Feeds

- Open, modular architecture that is Future Proof
- Open Standards—100% Linux
- Support different encoding, analytic, and storage technologies
- Support multiple codecs simultaneously
- Highly scalable—cameras, clients, storage
- Share IT infrastructure and storage systems
- Flexible archiving—simultaneous archives at different frame rates, durations, locations
- Retro-fit friendly
Video Surveillance Virtual Matrix (VM)

- IP Camera
- SS (optional)
- Headquarter LAN
- Remote Viewer
- Local Viewer
- Site B LAN
- Remote VM Client
- MS, OM
- SS (optional)
- Virtual Matrix Switching
- VM Client Station
- VM
- Common API
- Media Server
- Encoding Server
- Storage System
- Operations Manager
- Virtual Matrix

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential
Video Surveillance Virtual Matrix (VM)

- Controls an infinite number of video displays on network
- Easily integrates with other systems
- Flexible delivery of live & archived video
- Distributes to Video Wall
- Controls multiple video displays from a single station
- Event/Action
  Push video to remote screens
Video Surveillance Operations Manager (OM)
Video Surveillance Operations Manager (OM)

- Enterprise solution
- Non-proprietary hardware
- 100% browser based UI—“The Gui”
- Set up and manage multiple servers, cameras, and encoders
- Configure, manage, display, and control video/events throughout an IP network
- Unlimited cameras, storage, users
Features Summary

For Administrators:
- Device Management
- Scheduled and event-based video recording
- User and role management
- Activity and system reports
- Ability to push pre-defined views to any number of monitors
- Imported configuration data from spreadsheets

For Operators:
- Secure login
- Flexible video displays
- PTZ controls and presets
- Digital zoom and instant replay
- Archive review and clippings
- On-demand recording
- Event notifications
Scalable: Small System (Single Box)

Media Server
Virtual Matrix
Operations Manager
Internal Storage

Up to 100 Cameras
Up to 18 Terabytes
Up to 100 Users
Scalable: Nearly Unlimited Cameras and Storage
Vertical Application Examples

- Campus
- Retail
- Aviation
- Mobile
- Highway Transportation
- Corporate Security
Cisco Stream Manager Video Surveillance Product
Single Site, Analog/Matrix Switch—Centric

- Cisco Stream Manager
  - Configuration
  - Monitoring
  - Recording and Archiving

- Benefits:
  - Enables new capabilities: faster response and resolution
  - Smooth migration from analog to digital to networked
  - No operator retraining
  - Interoperable with 3rd party analog systems
Sample Traditional Matrix-Based Solution

PTZ (Pan/Tilt/Zoom) Cameras

Fixed Cameras

Traditional PhySec Keyboards

Analog Matrix Switch

VCRs/DVRs

CRT/Monitors
Matrix Based Solution—Hybrid Integration
Hybrid Integration + VMS Expansion
Cisco Video Surveillance IP Camera
Cisco Video Surveillance
Choice of Platforms & Appliances
Platoforms & Appliances

- ISR
- MAR
- High Performance Multi-Services Servers
Why Cisco Designed an IP Camera

- Variable or low image quality in difficult lighting conditions
- Camera Installation and configuration was tedious
- Multiple cameras needed for single deployments
- Poor Bandwidth Control
- Weak Network security
- Limited System scalability
- Not Integrated with Video Surveillance systems
Technology Breakthrough: Advanced Imaging with Wide Dynamic Range (WDR)

- CMOS based digital imager and dedicated co-processor that replaces traditional CCD technology
- Every pixel has its own dedicated Analog to Digital Converter (ADC) vs. CCD with only 1 ADC for an entire array
- Pixel-independent shutter speed
- Pixel-independent exposure
WDR from Pixel Independent Multi-Sampling

- Every pixel can be sampled multiple times per video field (1 frame = 2 fields)
- Exposure is computed for each pixel by calculating the slope of the light energy hitting it
- All pixels receive the optimal exposure with best Signal to Noise Ratio (SNR)
- Result—wide dynamic range & natural color; eliminating fixed pattern noise
Optimal Image in Multiple Lighting Conditions

Cisco Imager  Typical Imager

Cisco imager can pick up details in extreme lighting conditions—a common issue in warehouse applications.
No Saturation with Strong Lighting

Cisco Imager  Typical Imager

Cisco imager provides color detail even in extreme lighting with a manual iris lens, CCD technology is completely over-saturated
Improved Color Rendering

Cisco imager provides superior color rendering which can distinguish between chip colors, typical imager technology cannot.
Video Motion Artifacts

Typical video camera output:
30 frames/sec.
Or 60 fields/sec.
1 frame = 2 fields
1 field every (1/60) 16 ms
“Interlaced”

Cisco IP Camera
Progressive scan samples up to
5 times per frame
Better picture quality

Typical IP Camera samples 1 time
per field every 16 ms
Interlaces the fields
Resulting in lower picture quality
- Creates color artifacts
- Mosaic and jagged edges
Light Compensation

- Since lighting can change frequently in a given scene, the camera has the ability to compensate for different lighting conditions in the following ways:
  
  **Auto-Iris**

  Auto Iris lens has an amplifier built in which responds to amount of scene light and will **open or close iris automatically to maintain same amount of light coming to imager**

  **Electronic Shutter**

  Shutter speed **controls how long light enters the camera**, the larger the number the shorter the time. A short time lets in light quickly which will stop the motion an object might have as it travels across the imager while being exposed

  **Automatic Gain Control (AGC)**

  Camera supports AGC which automatically **reduces the gain (measured in DB) as the average signal level increases** resulting in the clear image regardless of the light condition
Cisco IP Video Surveillance Camera

- **IP Cameras**
  - High Quality Camera
  - Easy to install, minimize camera setup (tweaking)
  - Easy to deploy with Power over Ethernet (POE)
  - Easy to configure and manage, browser based

- **Excellent Image Quality in Variable Lighting Conditions**
  - Wide dynamic range
  - High total resolution
  - Zero bloom and smear
  - Exposure across ALL lighting conditions
  - Superior color rendering

- **Migration Path for Existing Deployments**
  - Analog cameras can be migrated to IP VS System with encoders
  - Future Proof solution, Investment Protection
Cisco IP Camera Features

- Implementation flexibility
  Simply “point, focus and forget”

- Day/Night Capability
  Automatically movable infrared (IR) cut filter, which enables color video in high and low light conditions and as IR sensitive black/white video at night, automatic or manual

- Dual streaming
  Cisco IP Camera offers dual streaming capability, users can adjust frame rate, and/or resolution to control the quality of the video for different purposes simultaneously, this cannot be done with strictly analog cameras and systems

- Analog Output
  There is an analog output with a standard BNC connector for ease of installation
IP Camera Features (Cont.)

- MPEG-4 compression technology
  - Provides DVD quality D1 video at frame rates of up to 30 fps NTSC, 25 fps PAL
  - Reduces system bandwidth requirements
  - Minimizes network traffic, increases the number of video streams that can be transmitted over a digital network
  - Minimizes Storage Cost & Increases Capacity

- Progressive Scan
  - Samples complete frames of video up to 5 times more often than traditional interlaced imager
  - Minimize color artifacts, especially in high motion scene
  - Eliminate jagged edges within the scene

- Audio
  - Options are available for one or two-way audio
  - Built-in or external microphone, and external speaker output
IP Camera Features (Cont.)

- **Motion Detection**
  Ability to designate specific zones in which motion triggers alarms, and to configure the sensitivity in these zones. No information is sent across the network and stored until an event occurs. Information is captured in great detail and will trigger actions such as alarms or email alerts.

  Motion detection is used to send an alarm to the operator and start streaming the video for recording

- **Alarm I/O**
  Two alarm inputs that can be received and handled anywhere on the network, even by multiple recipients

  Two alarm outputs allows the operator to switch anything on and off and allow operator control from anywhere in the world.

  Configurable pre & post alarm recording—capture the lead-up to events
IP Camera Features (Cont.)

- Browser Based Configuration
  - Web Server built into the Camera
  - Configuration via Browser (Internet Explorer 6.X with Service Pack 2 and above)
  - Save/upload configuration to a server
  - Download configuration to camera(s)

- Event Schedule
  - If an event occurs during the day or range of days, the camera can perform pre-configured actions
  - Action that the IP camera takes when the event occurs
    - E-Mail message to be delivered to the SMTP server
    - FTP video file to upload to the FTP server
    - Alarm outputs
IP Camera Networking Features

- Cisco Discovery Protocol (CDP)
  Cisco IP cameras provide for discovery and management through CDP

- Multicasting
  When multicast is enabled, the IP camera sends video and audio to designated multicast addresses. Multicast enables multiple devices to receive the video signal from the IP camera simultaneously. This feature saves bandwidth, which is a vital component to a scalable solution.

- HTTPS
  Secure HTTP to protect from eavesdroppers and other attacks

- QoS
  The ability to prioritize traffic and allow critical flows to be served before flows with lesser priority
  DSCP Marking
Applications of Cisco Video Surveillance

- Many cameras
- Massive or redundant storage requirement
- Manage hundreds of remote locations
- Interoperability with multiple authorities
- Remote access—escalation of data/decisions
- Wireless mobile video
Casino Challenges

- Compliance for casino floor
- Building Security
- Executive Protection
- Legacy Infrastructure
- Limited budget

“We were able to migrate from analog to digital networked video surveillance without operational disruption. The move was also invisible to our surveillance operators as Cisco's video surveillance solution provides low-latency, broadcast-quality video. Since we could continue to use our existing analog controls and displays, the operators did not have to be re-trained, but now enjoy new capabilities only available with IP-network technology innovations.”

Dan Eitnier
Director of Surveillance
The Venetian
Retail Challenges

- **Primary Focus on Shrinkage**
  - Thieves stole over $5.8 billion from 24 surveyed retailers in 2005
  - Shrinkage accounts for 2–3% of revenues
  - Only 2–3% of this stolen merchandise is recovered today

- **Loss Prevention Efficacy and Productivity**
  - Faster response to real-time events
  - Accessibility to video outside of security operations; on the floor and on a remote basis

- **Ability to use VS system for uses other than LP, such as store operations and merchandising**

- **Ability to interface with video analytics**

- **Improved integration with other systems**

- **Impact on corporate bottom line and stock price**
Retail Application

Storage

15 fps video

Event Storage

30 fps video

Analytic C

Analytic B

1 fps video

Main Entrance

Exit

Checkout

20 fps video

Analytic A

Local Security

Corporate

1 fps video

Vendor

1 fpm video
Education Challenges

- Students and staff safety
- Theft, vandalism and graffiti
- Unauthorized entry
- Security guards ROI
- Budget and resources constraints
Education
Cisco Physical Access Control
Electronic Access Control Architectures Today…

- Complex and expensive to design, deploy and maintain
- Not capable of incremental deployment: Upfront design cycle required
- Separate power circuit required to power door hardware
Cisco Physical Access Control Overview

- **A Comprehensive Solution** for Electronic Access Control
- Leverages IP infrastructure, integrates with other Physical Security applications

### Hardware:
Cisco Access Gateway connects existing door hardware (readers, locks etc.) to the network

Additional doors can be managed by connecting expansion modules to the Access Gateway

### Software
Cisco Physical Access Manager (Cisco PAM) is a Management Appliance for configuration, monitoring and report generation.
A Uniquely Expandable Architecture

Scalable Modular Architecture, open systems integration with IT systems
## Hardware Overview

<table>
<thead>
<tr>
<th>Cisco Physical Access Gateway</th>
<th>Reader Module</th>
<th>Input Module</th>
<th>Output Module</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Cisco Physical Access Gateway" /></td>
<td><img src="image2.png" alt="Reader Module" /></td>
<td><img src="image3.png" alt="Input Module" /></td>
<td><img src="image4.png" alt="Output Module" /></td>
</tr>
</tbody>
</table>

### Cisco Physical Access Gateway
- **Mandatory component.** Connects up to 2 doors, and up to 15 additional modules (connected via a 3 wire CAN bus).
- **Power:** POE or 12V – 24V DC
- 2 Ethernet ports
- 10 pin Weigand Reader port: can be configured as two 5 pin Weigand ports
- 1 RS-485 port
- 3 Outputs (Form C Relays)
- 3 Supervised inputs
- Tamper & PF inputs (can be configured as additional inputs)

### Reader Module
- **Requires Access Gateway**
- Connects up to 2 doors, to the Cisco Access Gateway via CAN bus.
- **Power:** 12V – 24V DC
- 10 pin Weigand port: can be configured as two 5 pin Weigand ports
- 1 RS-485 port
- 3 Outputs (Form C Relays)
- 3 Supervised inputs
- Tamper & PF inputs (can be configured to be used as additional inputs)
- CAN Termination switch

### Input Module
- **Requires Access Gateway**
- Connects up to 10 inputs to the Cisco Access Gateway via a CAN bus.
- Example inputs are: Pushbutton switches, Glass Break sensors, or any contact closure input: circuit
- **Power:** 12V to 24V DC
- 10 Supervised inputs
- Tamper & PF inputs (can be configured to be used as additional inputs)
- CAN Termination switch

### Output Module
- **Requires Access Gateway**
- Connects up to 8 outputs to the Cisco Access Gateway via CAN bus.
- Example outputs are: lights, LEDs, or any contact closure output circuit.
- **Power:** 12V to 24V DC
- 8 Form C (5V, 30A) outputs
- Tamper & PF inputs (can be configured to be used as additional inputs)
- CAN Termination switch
The Cisco Access Gateway is always required, and an control up to 2 doors by itself.

Any combination of additional modules (up to 15) can be connected to the Access Gateway via a 3 Wire Controller Area Network (CAN) Bus.

Additional modules can be a maximum of 40M (130 Feet) from the access gateway.

Modules may be added or removed at run time without affecting operation of the other modules.
## Cisco Access Gateway Embedded Software

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>250K Cardholder cache, 150K Transaction buffer</td>
<td>Door continues to function in case network connectivity is lost</td>
</tr>
<tr>
<td>Web server built in</td>
<td>Simplifies configuration and monitoring</td>
</tr>
<tr>
<td>All communication is 128 Bit AES encrypted</td>
<td>Protects credentials, preserves security</td>
</tr>
<tr>
<td>Device pre-provisioning using network services</td>
<td>Simplifies deployment</td>
</tr>
<tr>
<td>Plug &amp; Play support</td>
<td>Modules can be added or deleted without disrupting service</td>
</tr>
</tbody>
</table>
Cisco Physical Access Manager (Cisco PAM)

- 1 RU Appliance
- Java Thin Client Architecture
- Policy Support: Two-Door, Anti-Passback
- Report Generator (Canned & Custom)
- Badge Design & Enrollment
- Microsoft Active Directory integration
- Fine grained user rights
- Global I/O
- Device Pre-Provisioning
- Capacity & Feature Licenses
- IT Data integration
- Warm Standby High Availability
- Audit Trails
Cisco Video Surveillance Manager (VSM) Integration

- Event Video integration with Cisco VSM
- Dynamically acquires camera inventory stored in Cisco VSM. Automatically tracks inventory
- Allows association of cameras to doors
- For every event by the door, recorded and live video can be viewed
Cisco PAM: Enterprise Application Integration (EAI) Module

- EAI Studio is a standalone tool running on Windows XP
- Select Data sources
- Select fields
- Select schedules

Integrates Cisco PAM data with other databases/IT applications
Summary

- A comprehensive solution for Electronic Access Control, with Software & Hardware components

<table>
<thead>
<tr>
<th>Scalable</th>
<th>Integrated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage one door or thousands</td>
<td>Integrated with Cisco VSM</td>
</tr>
<tr>
<td>Deploy single or multiple Cisco PAM instances</td>
<td>Leverage IP network services</td>
</tr>
<tr>
<td></td>
<td>Easy integration with IT Apps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Flexible</th>
<th>Manageable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mix and match modules to tailor solution</td>
<td>Plug &amp; Play</td>
</tr>
<tr>
<td>Supports centralized and/or distributed deployment</td>
<td>Manage system remotely</td>
</tr>
<tr>
<td></td>
<td>No scheduled maintenance</td>
</tr>
</tbody>
</table>
Thank You!