

# Going Critical

How to Design  
Advanced Security Networks  
for the Nation's Infrastructure

# Going Critical: Networks for Physical Security

- Increasing concerns and market growth
  - ▣ Asset protection
  - ▣ Public safety
  - ▣ Regulatory compliance
  - ▣ Video integration with operations processes
- More sophisticated, integrated solutions
- More challenging logistics

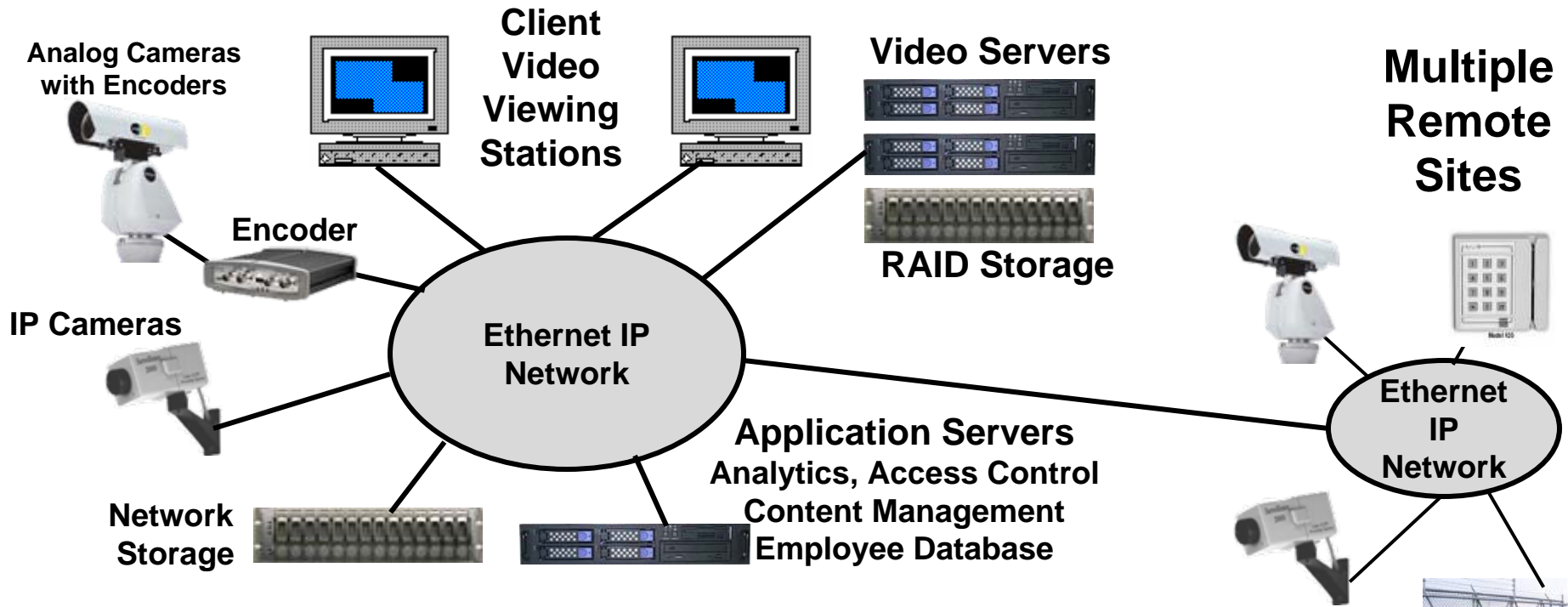
# Physical Security Systems

- Surveillance cameras
- Video monitoring
- Video collection, storage and analytics
- Access and motion sensors
- Access control systems
- Electronic locks and gates





# Integrated Security Networks



- Distributed, networked system with shared infrastructure
- Standards-based hardware/software components
- Integration with off-the-shelf and custom enterprise applications

# Critical Physical Security



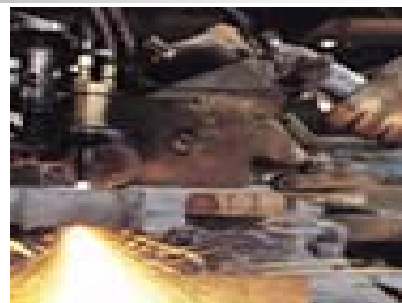
- Traffic systems
- Airports / Seaports
- Parking areas
- Public venues
- Power substations
- Water systems
- Pipelines & refineries
- Other remote facilities



# Special Challenges



- Installation
- Reliability
- Performance
- Security



# Installation Challenges

- Greater ambient temperature ranges
  - Hardened “factory” ranges  $-25^{\circ}\text{C}$  to  $+60^{\circ}\text{C}$
  - “Outdoor” ratings  $-40^{\circ}\text{C}$  to  $+75^{\circ}\text{C}$
- Convection cooling
- Integrated fiber ports
- Variety of form factors
- Alternative mounting options

# Parking Garage Call Station & Camera Examples



# Parking Lot Call Station & Camera Examples

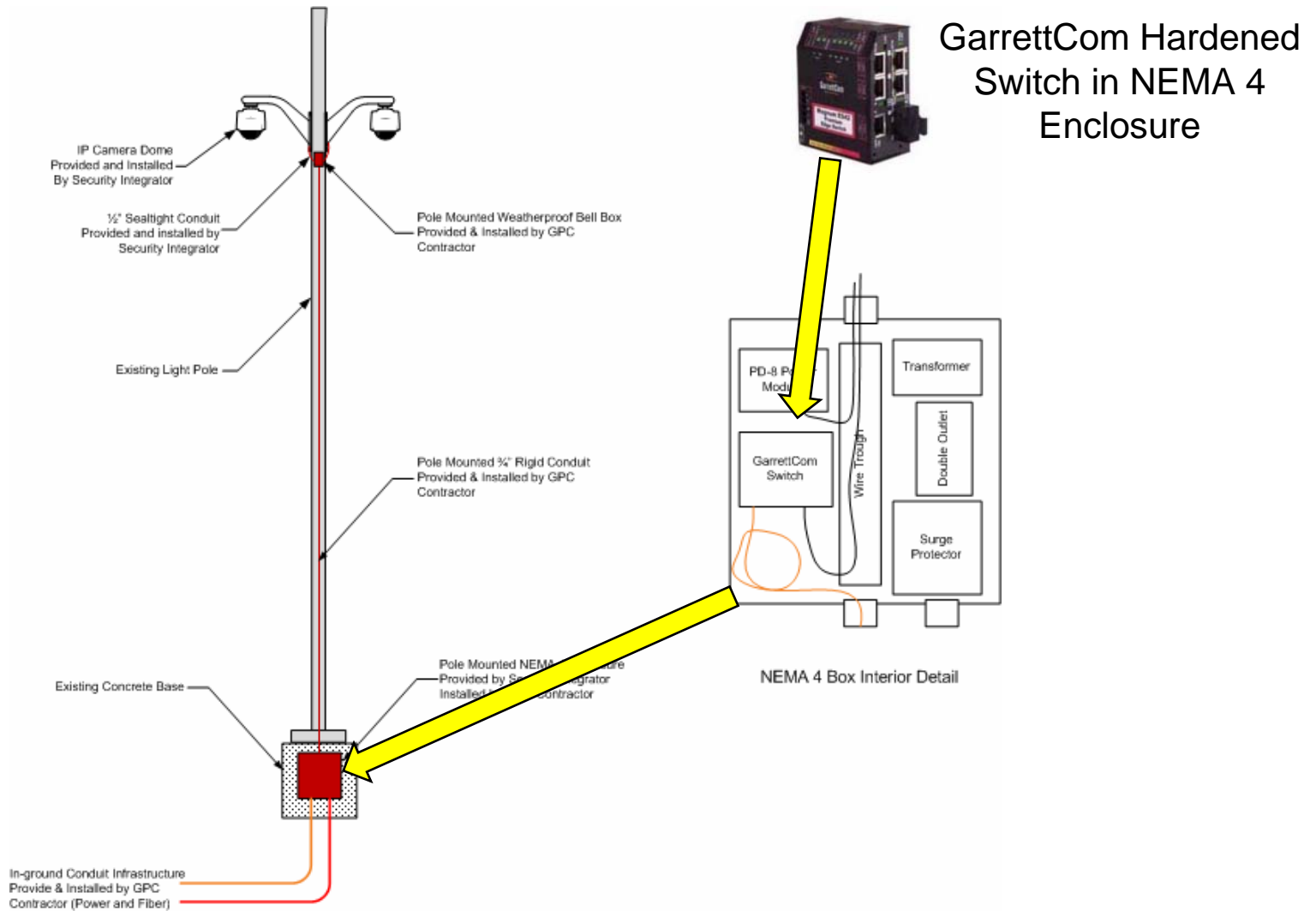


Future IP Call Tower & IP Camera Location

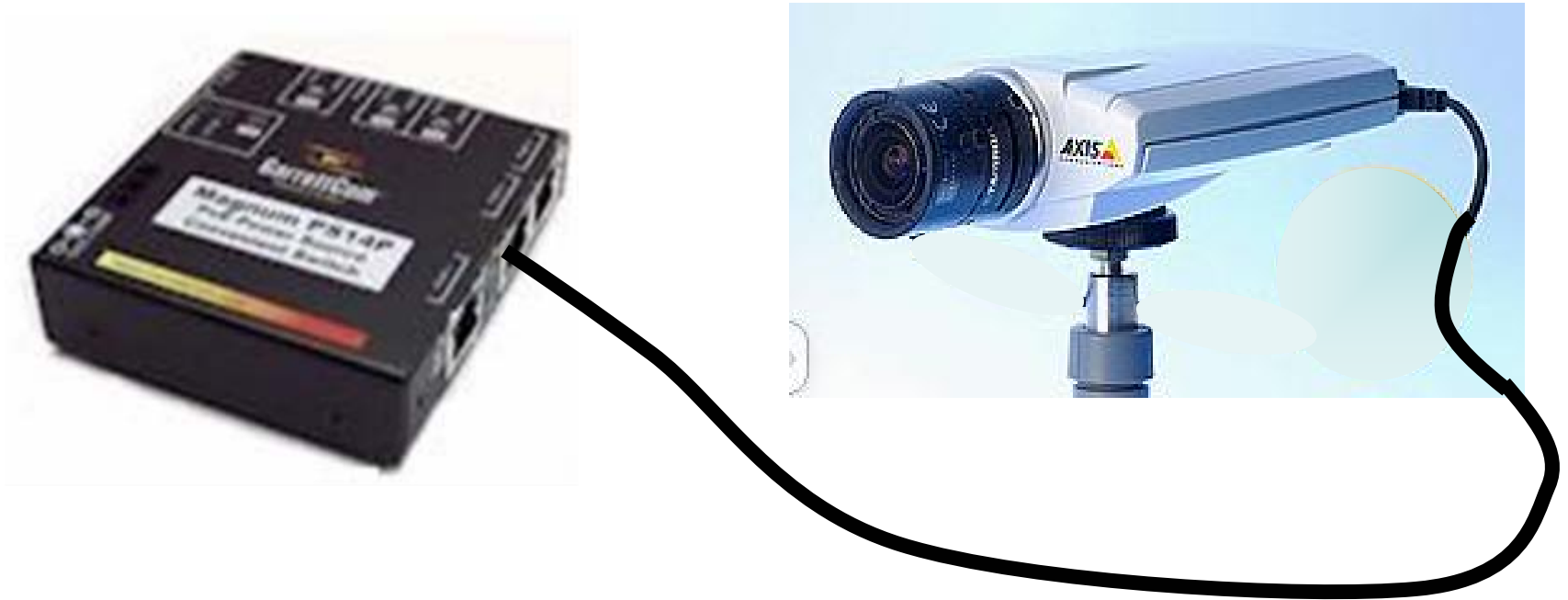
Industrialized / Hardened Ethernet Switch with Fiber Optic Connectivity, To Local IDF.



# Parking Lot IP Camera Example : "What's in the Junction Box?"



# PoE for Installation Flexibility



**Access devices w. Power-over-Ethernet (POE):  
Single cable for power and data (image)**

# Power over Ethernet - PoE

- PoE provides a simplified means to power networking edge devices
  - Cameras, VoIP phones, badge readers, sensors, WAPs, etc.
  - Power Sourcing Device = **PSE**, Powered Device = **PD**
- Current PoE standard is 802.3af
  - PoE provides up to 15.4 watts to powered device
  - Due to transmission losses, only ~13 watts available to device
  - PoE protocol prevents power from being applied to non-PoE devices
- There are two types of PoE PSE's - Endspans / Midspans
  - Endspans are PoE switches designed to power PoE PD's
  - Midspans are power insertion devices used to add PoE without new switch



# Variety of PoE PD's fit the Application

- Different PoE applications need unique solutions
  - Different PSE port density
  - Mix of PoE and non-Poe ports
  - Different backhaul bandwidth capabilities



- A new PoE standard - 802.3at – remains in process
  - Will provide more power to PD's – how much is to be seen

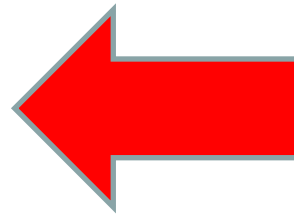
# Special Challenges



➤ Installation



➤ Reliability



➤ Performance



➤ Security



## ➤ Reliable Network Components

- HW made for harsh environments
- SW designed for continuous uptime and network standards compliance
- Device compatibility testing

## ➤ Resilient network design & topology

- Devices, power, interconnects will fail
- ***A resilient network design can mask these failures***

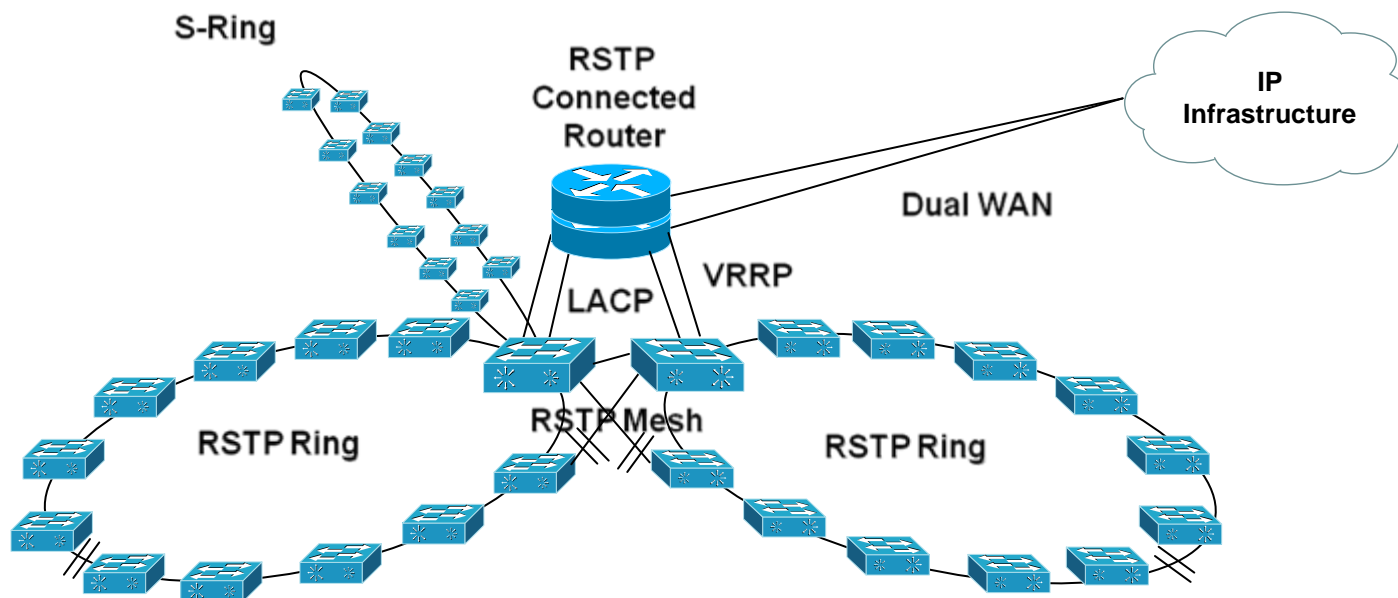
# Resilient Network Design

- There are numerous protection protocols to enable resilient networks and maximize network uptime ...

Redundancy Feature	Line Cuts	Switch Failure	Power Failure (local)	Router Failure	Bandwidth Protection	Recovery Speed
<b>Ethernet / Layer 2 Redundancy</b>						
Rapid Spanning Tree Protocol (RSTP)	X	X	X			15 mS + N*2ms
S-Ring	X	X	X			500ms + N*20ms
Dual Homing (Remote switch redundant path)	X	X	X			300ms
LAN Aggregation Control Protocol	X				X	0 Seconds
<b>IP / Layer 3 Redundancy</b>						
RIP / OSPF / BGP Alternate Routes	X		X	X		Variable
Redundant WAN (in conjunction with routing)	X			X	X	Variable
Virtual Routing Redundancy Protocol (VRRP)	X		X	X		Variable

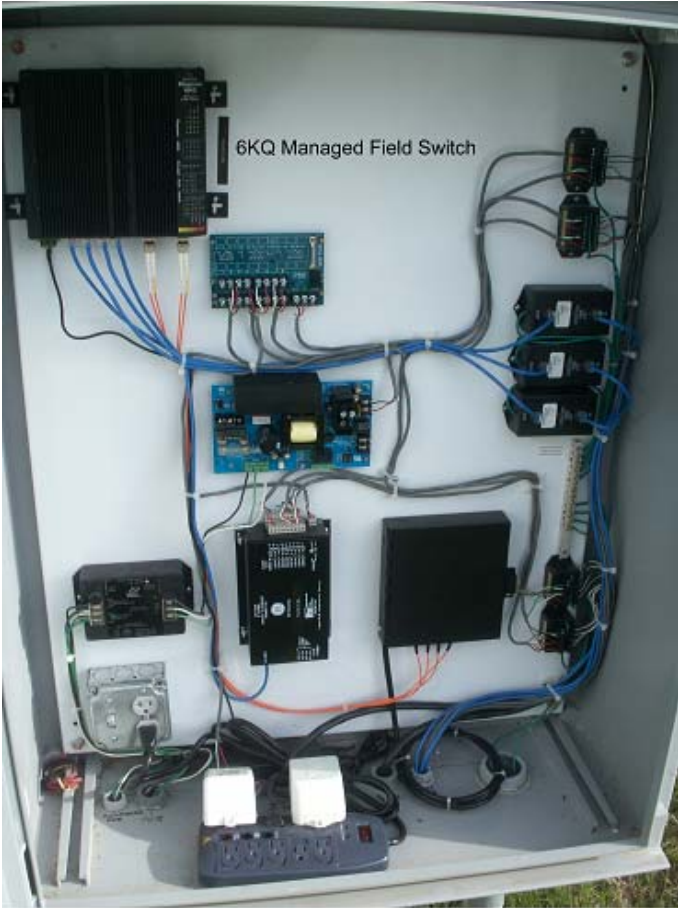
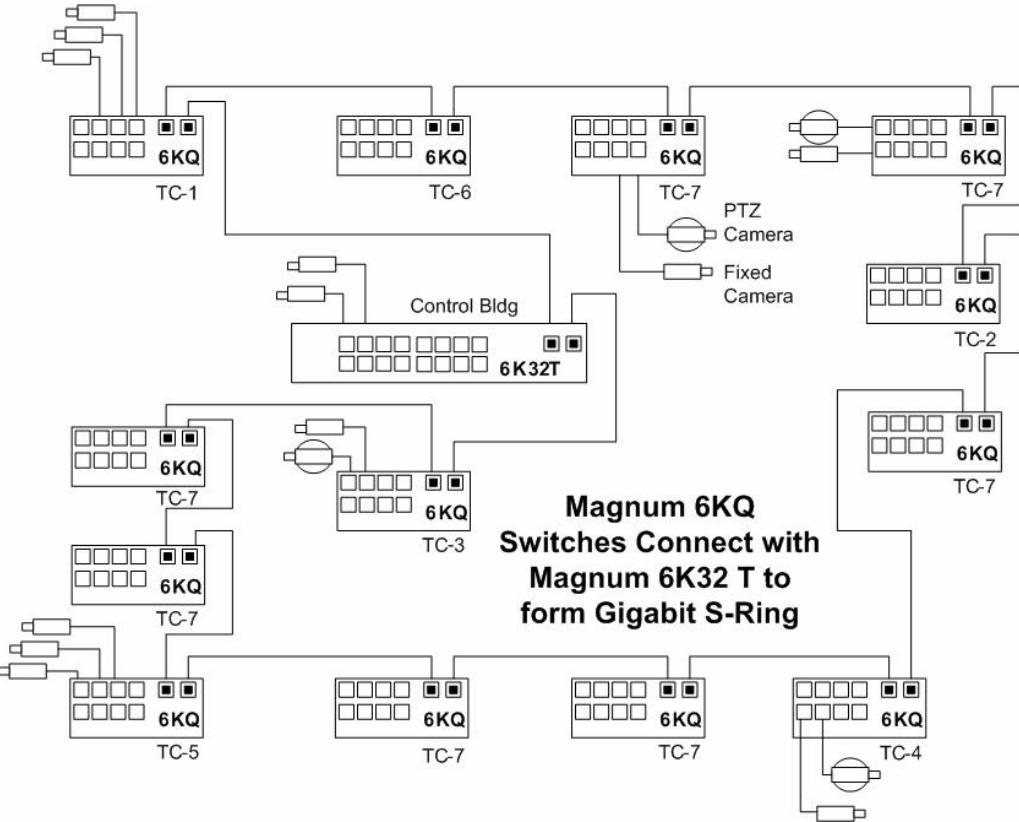
- For Layer 2 Redundancy:
  - RSTP (802.1-2004) recovers large rings or mesh networks very quickly
  - For smaller or low-cost solutions proprietary recovery protocols can be used
  - LACP allows LAN aggregation for increased bandwidth
- Redundant routes and VRRP protect networks at Layer 3

# Resilient Network Example



- Ethernet RSTP network design can be tailored to fit the application
  - ▢ Networks can be designed to suit the application need
  - ▢ RSTP networks up to 100 nodes recover at speeds up to 2ms/node
- Router Resiliency protocols can be used at the IP layer

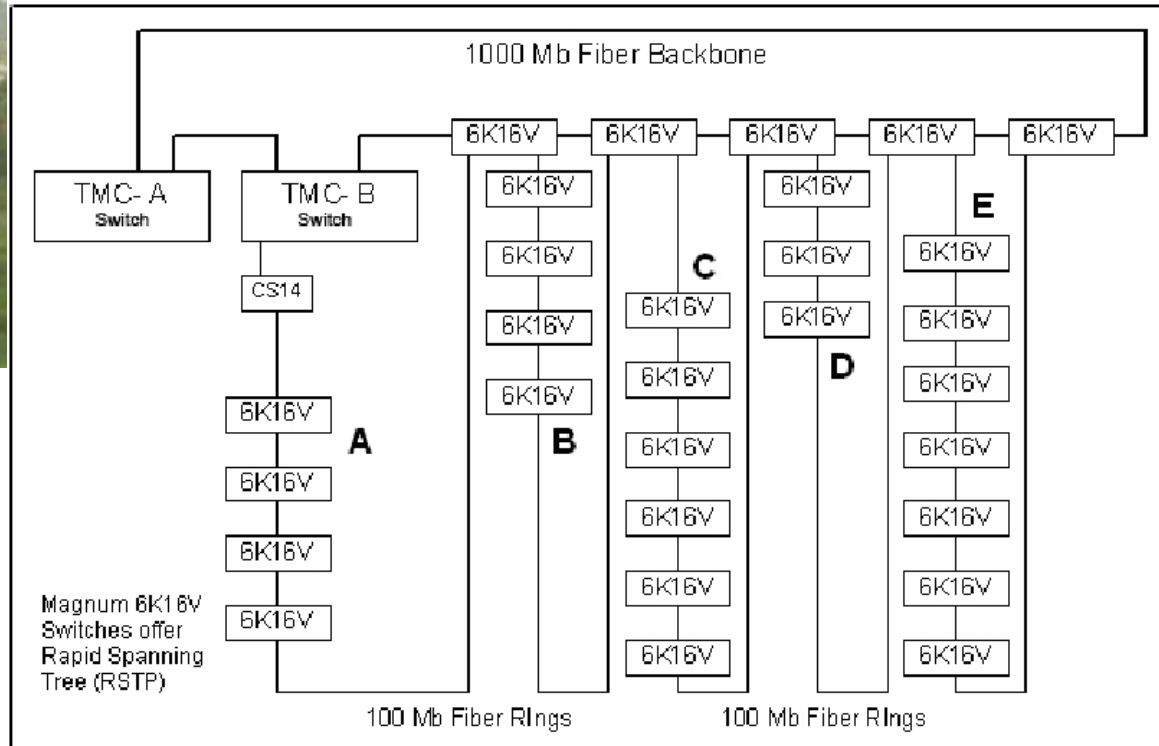
# St Cloud Water Treatment



# Tampa Expressway



Redundant rings for traffic control,  
DMS, sensors and video surveillance



# Special Challenges



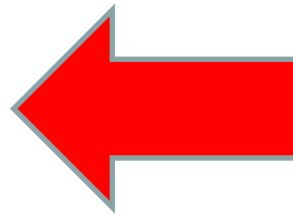
➤ Installation



➤ Reliability



➤ Performance



➤ Security



## ➤ Too many bits

- Multiple dense video streams competing for finite network capacity

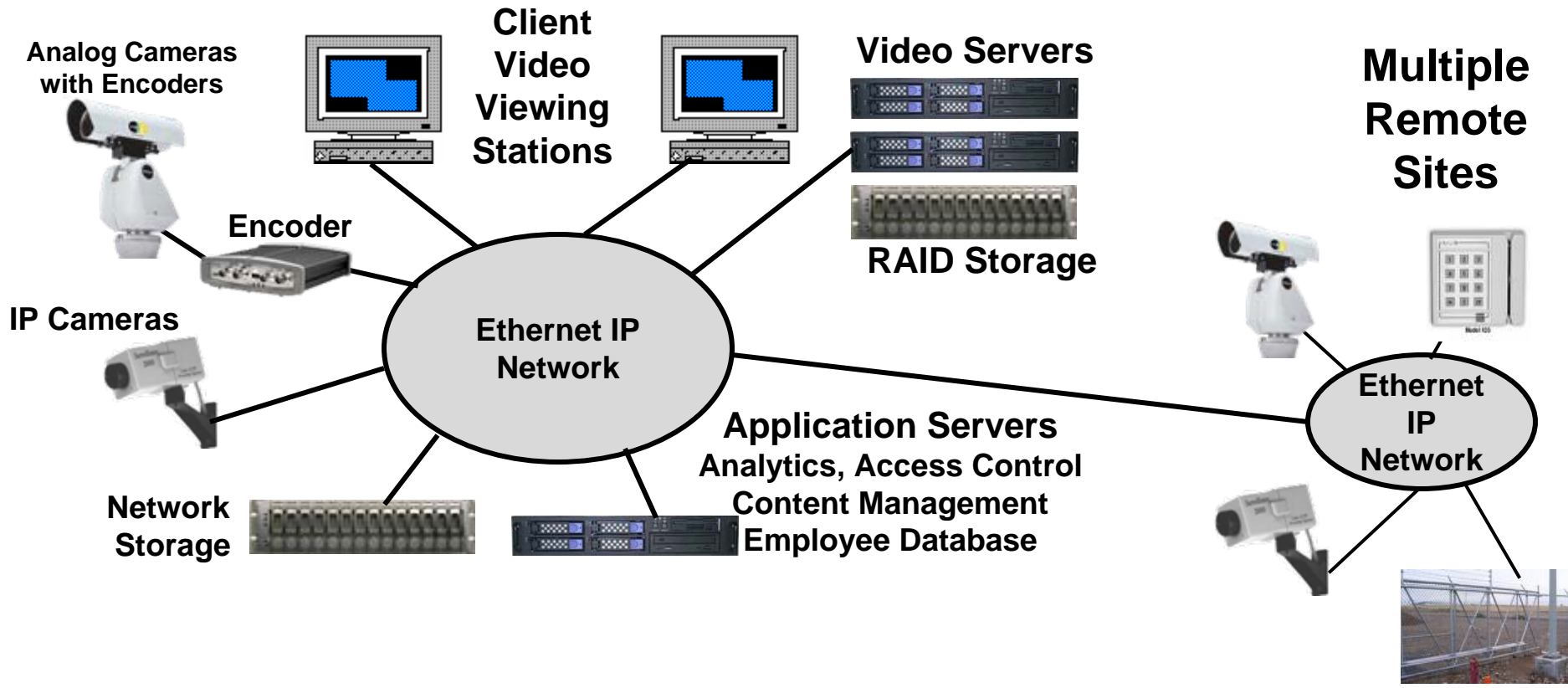
## ➤ Bits going everywhere

- Many video streams are multicasting – potentially flooding networks

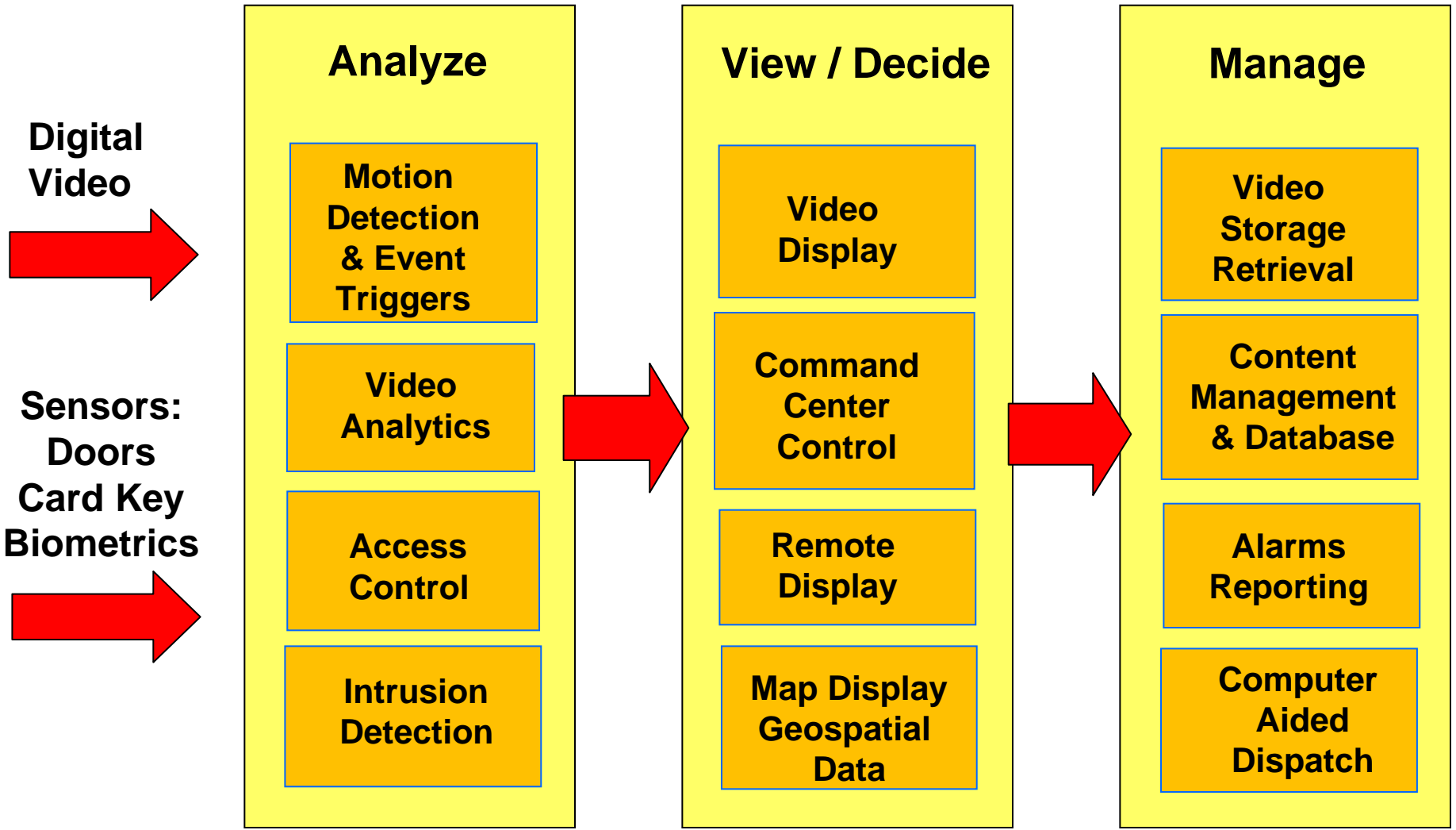
## ➤ Differing priorities among applications

- Multiple different security functions on the same network compete with each other

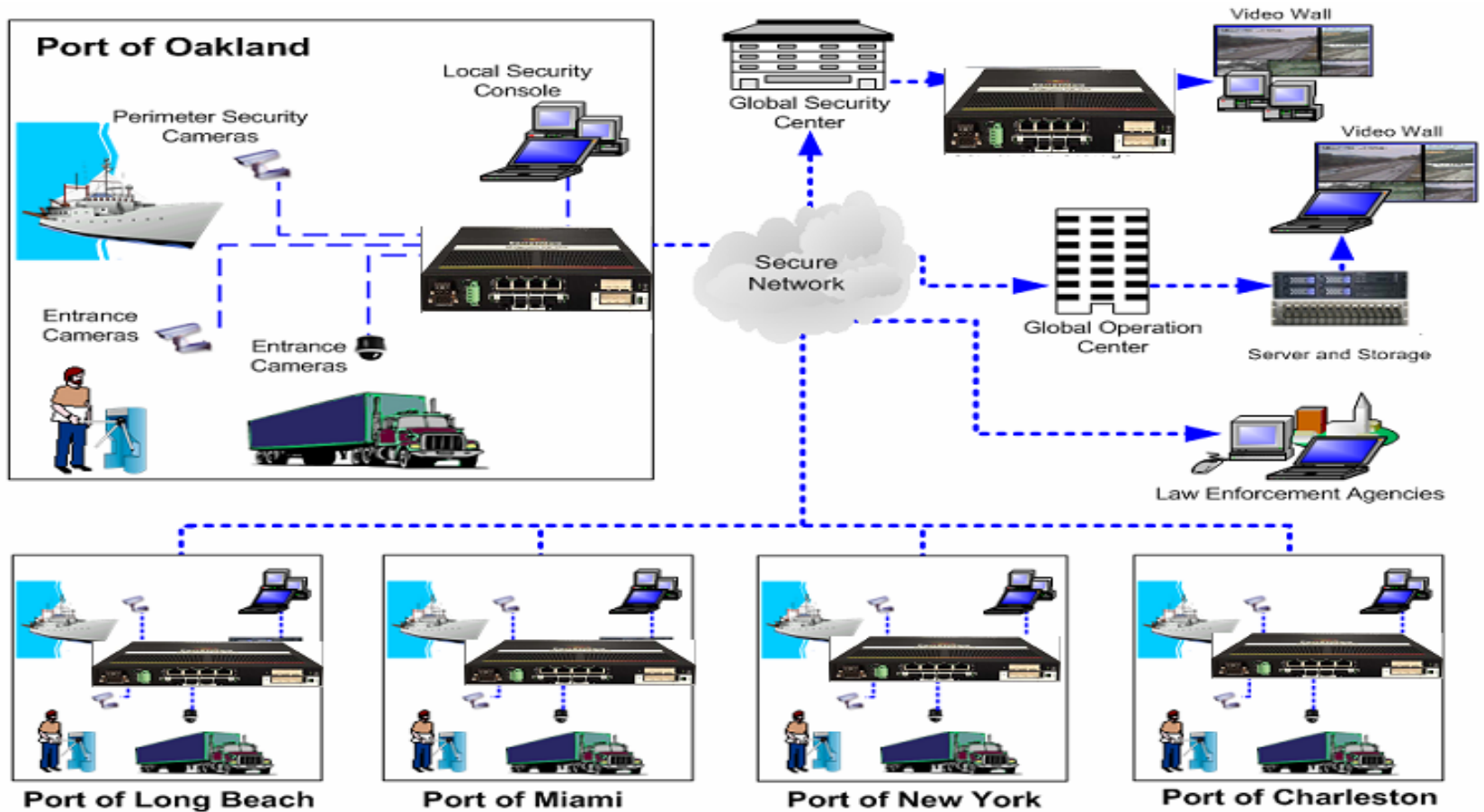
# Integrated Security Networks



# Integrated Security Application



# National SeaPort Security Network



# Quality of Service (QoS) Technologies

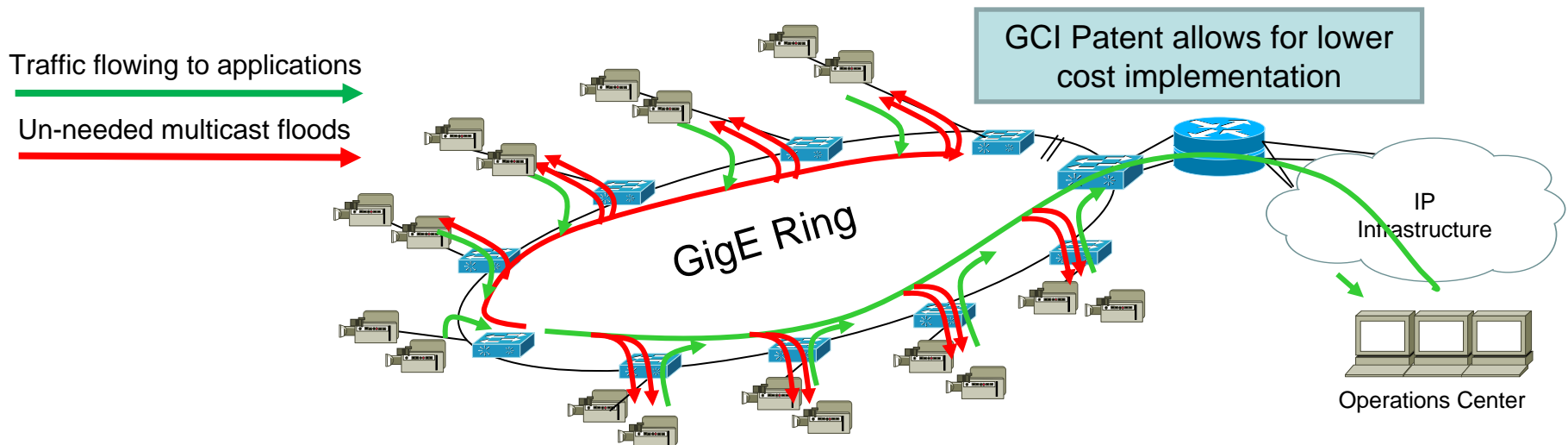
- Different traffic types can be prioritized differently
  - DiffServ, or DSCP can be used at the IP layer
  - 802.1p can tag Ethernet frames for layer 2 priority
- Both functions allow traffic to be identified, marked and prioritized to achieve desired performance

Priority Level	Traffic Type	Example
0	Best Effort	Web Access
1	Background	File Access
2	Standard	File Transfer
3	Business Applications	Business Critical Processing
4	Controlled Load	Streaming Multimedia
5	Interactive Voice and Video	IP Video
6	Layer 3 Network Control Traffic	Routing Protocols
7	Layer 2 Network Control Traffic	RSTP Protocols

- In a surveillance application QoS can be used to ensure network control traffic is not over-run by the bandwidth heavy video streams

# IGMP – Internet Group Management Protocol

- Without IGMP video multicast traffic will flood the entire network
- How IGMP works:
  - A video application comes on-line & advertises a multicast stream
  - A local router logs IGMP message & queries for subscribers
  - Applications subscribe to these multicast streams
  - IGMP enabled switches learn where subscribers are & filter traffic



# Other Video Considerations ...

- Video is very bandwidth heavy
- Multiple cameras per node add up – even on Gbit rings!
- Multiple Gbit links should be considered for applications with:
  - ▢ High resolution cameras
  - ▢ High number of cameras
  - ▢ Possibility of significant future growth per node

		Number of Cameras				
Resolution	Stream size (mbps)	50	100	150	200	250
Poor	0.512	25.6	51.2	76.8	102.4	128
Low	1	50	100	150	200	250
Medium	3	150	300	450	600	750
High	6	300	600	900	1200	1500

# Special Challenges



➤ Installation



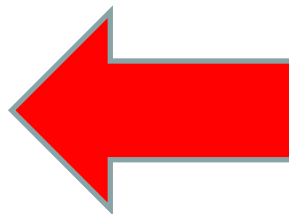
➤ Reliability



➤ Performance



➤ Security



## ➤ LAN Security

- ▣ Port security
- ▣ VLANs
- ▣ Who/what gets access to which ports?

## ➤ Perimeter Security

- ▣ Firewall
- ▣ WAN VPN
- ▣ Keep the bad stuff out!

## ➤ Remote Access Security

- ▣ Authenticate/authorize
- ▣ Allowing permitted remote operations

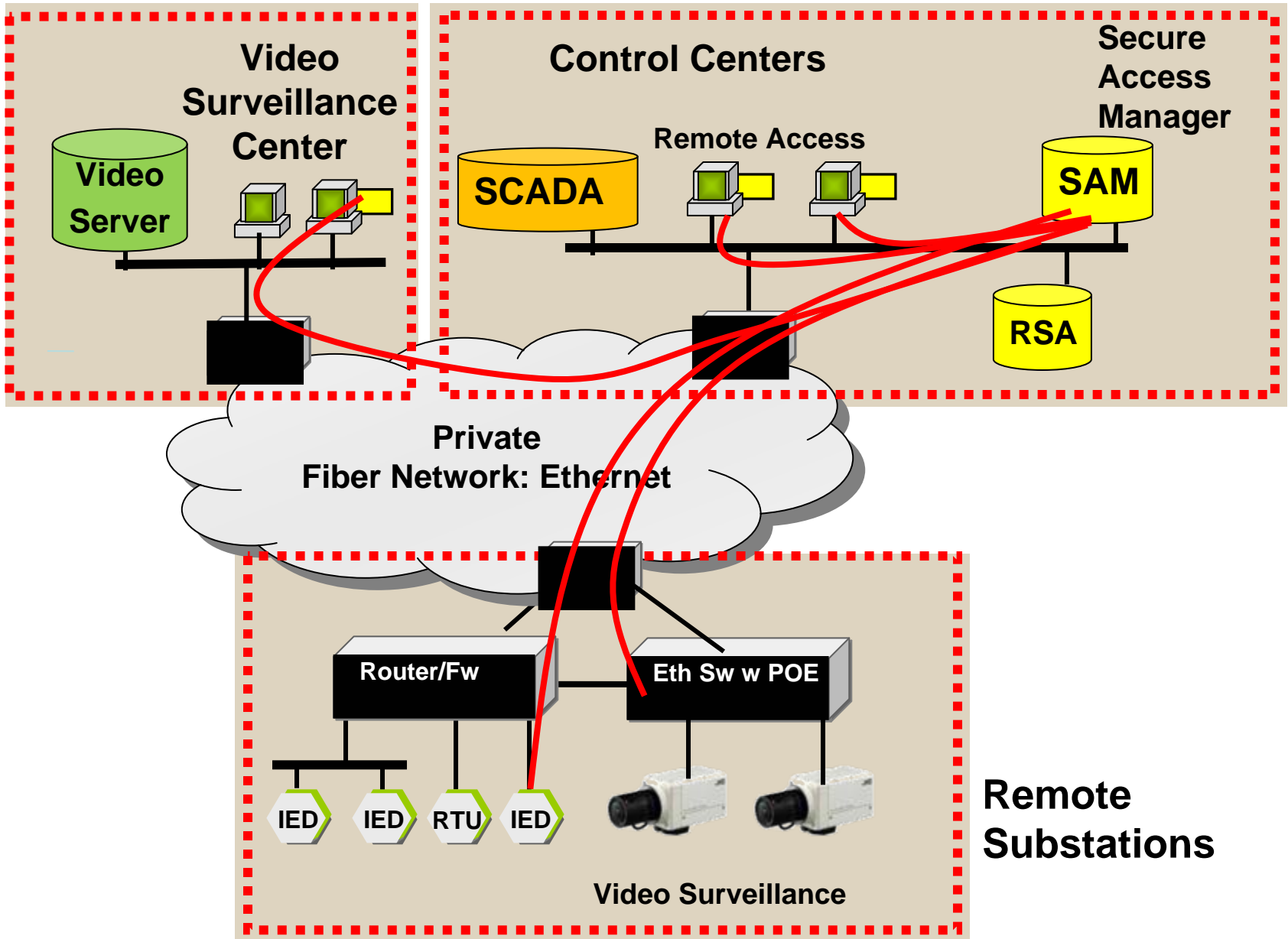
## ➤ Management Security

- ▣ Secure mgmt. protocols
- ▣ User authentication
- ▣ Logging

Federally mandated cyber security standards for power utilities:  
NERC Critical Infrastructure Protection CIP-002--- CIP-009

<b>CIP-002</b>	Critical Cyber Asset Identification
<b>CIP-003</b>	Security Management Controls
<b>CIP-004</b>	Personnel and Training
<b>CIP-005</b>	Electronic Security Perimeters
<b>CIP-006</b>	Physical Security of Critical Cyber Assets
<b>CIP-007</b>	Systems Security Management
<b>CIP-008</b>	Incident Reporting and Response Planning
<b>CIP-009</b>	Recovery Plans for Critical Cyber Assets

# Mid-Atlantic Power Company



# Special Challenges



- Installation
- Reliability
- Performance
- Security



# Going Critical: Networks for Physical Security

- Critical asset protection and public safety require advanced physical security solutions
- Integrated IP / Ethernet networking can address these special challenges
  - ▣ Product and cabling flexibility for constrained installations
  - ▣ High system availability via product hardening, networking resilience, performance management and network security

# Going Critical

How to Design  
Advanced Security Networks  
for the Nation's Infrastructure