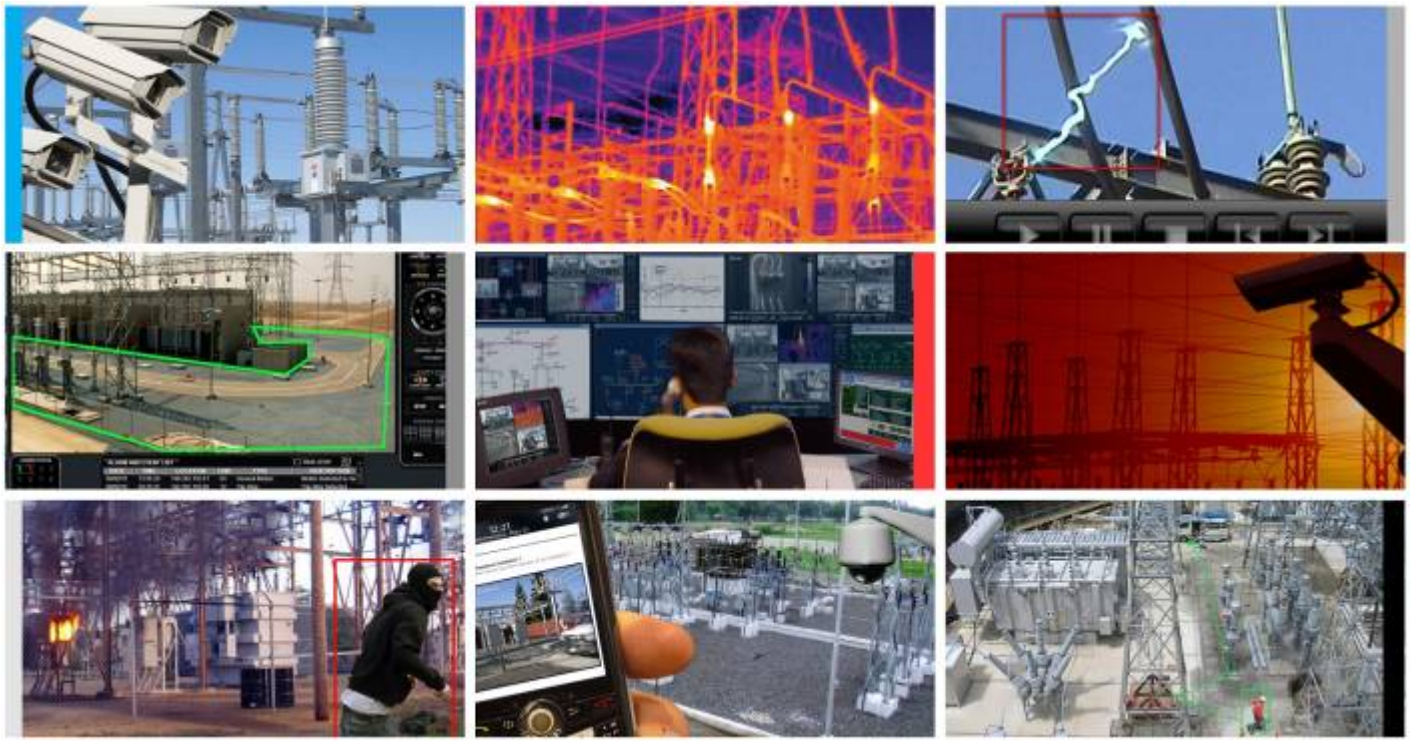
systems with intelligence

Video Monitoring Solutions . . .



. . . for Electric Utilities

" Intelligent Video Monitoring Solutions for the Protection of Critical Infrastructure."

Private and Confidential

Video Monitoring for Electric Utilities

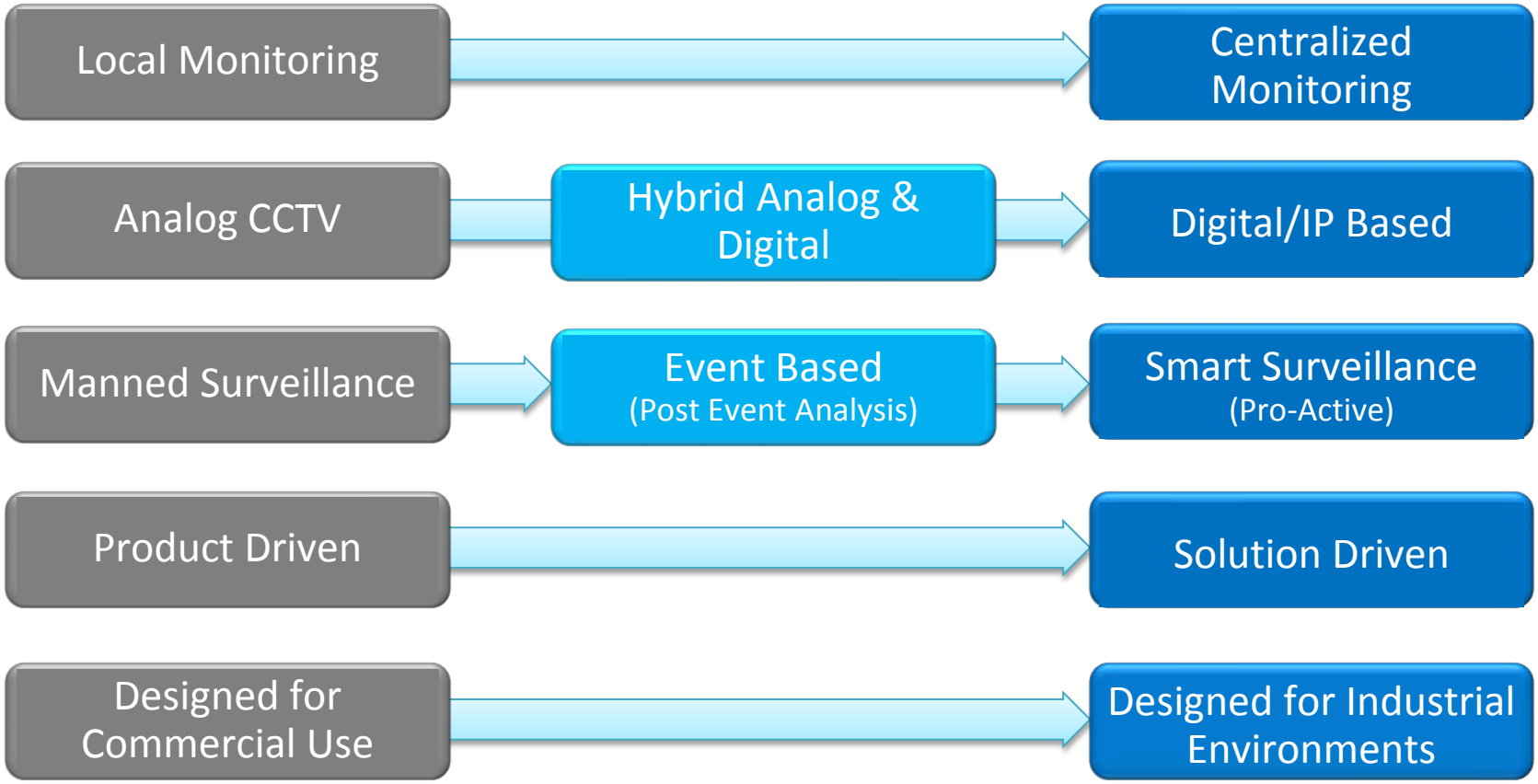
- **Physical Security**
  - Protect critical transmission and distribution infrastructure
  - Reduce theft and damage to physical assets
  - Monitor multiple remote sites over a widely dispersed geography
- **Asset Monitoring**
  - Increase asset utilization and improve efficiencies
  - Enhance “Smart Grid” capabilities by enabling new applications
- **Safety**
  - Improve safety for workers and the public
- **Regulatory Compliance**
  - Help to meet new regulations such as NERC CIP

Electric Utility Trends

- **Theft of Copper and other High Value Metal Electrical Components**
  - US 2009: $20M loss of copper material, $60M impact to costs related to replacing stolen material, and over 457,000 mts of outages.

- **The Smart Grid Initiative**
  - New solutions to increase grid reliability and improve asset utilization are now possible
- **Regulatory Requirements to Protect Critical Infrastructure**
  - NERC CIP Requirements
- **The Application of Technology Based Solutions Designed for Specifically for Electric Utilities**
  - Solutions designed for Harsh Environments, Remote Locations and Mission Critical Applications

Video Monitoring Technology Trends



Video Surveillance - Solution Components

Cameras

- the “eyes” of the system
- use newer IP cameras or traditional analog cameras

Digital Video Server

- aggregates video cameras, provides digital video recording, local short term storage, platform to run video analytics

Video Management System

- the “hub” of the overall solution
- provides video monitoring, viewing, recording, event and archive management

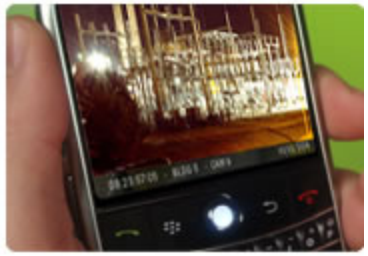
Video Surveillance - Solution Components

Video Analytics

- software algorithms that automatically identify various types of intrusions

Storage Systems

- archiving recorded video for post event analysis and regulatory audit requirements



Remote Access and Event Monitoring

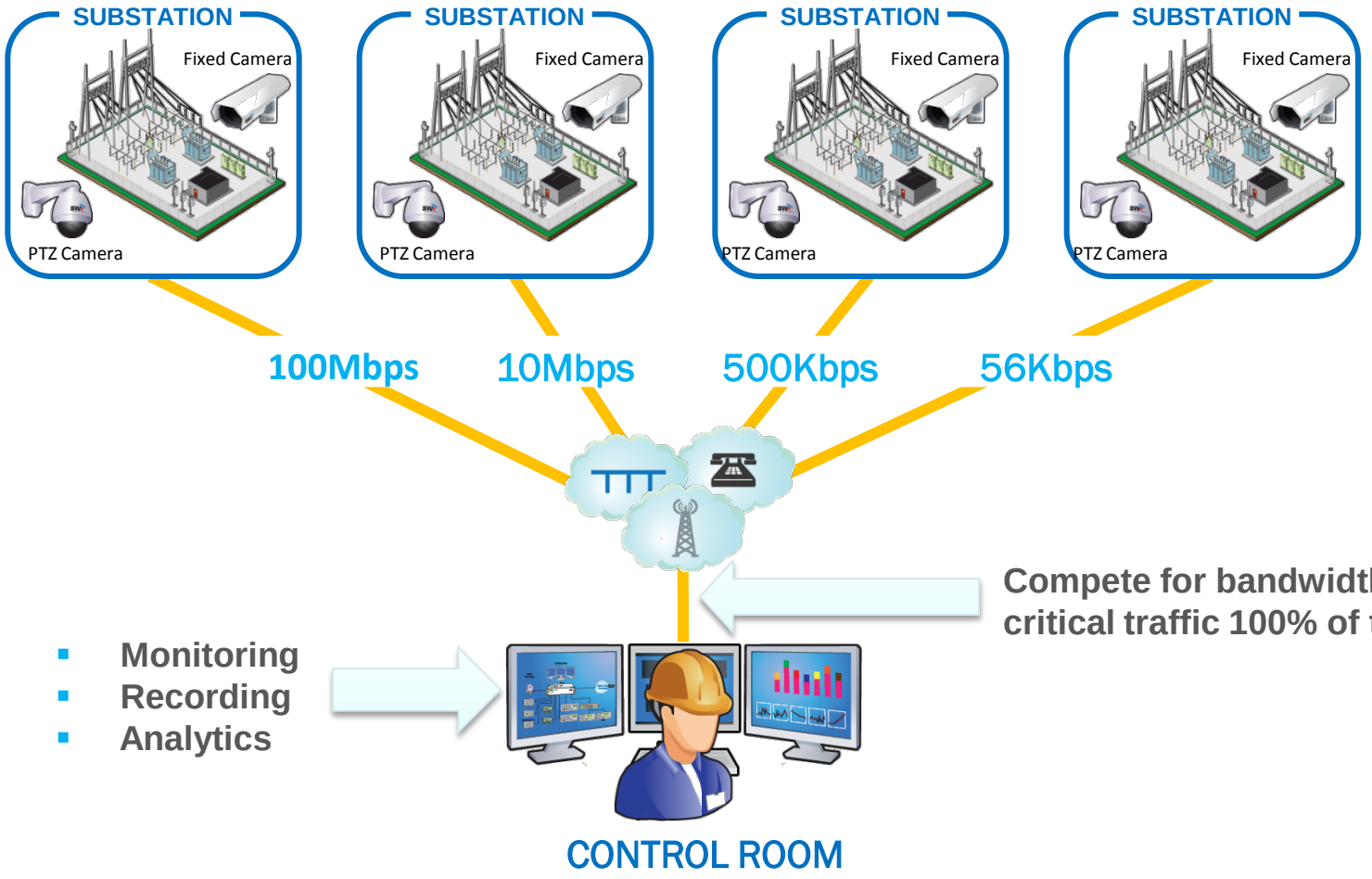
- viewing and receiving video, systems events, and alarms at remote locations or to a handheld device

Guidelines for Video System Design

Key Items for Consideration

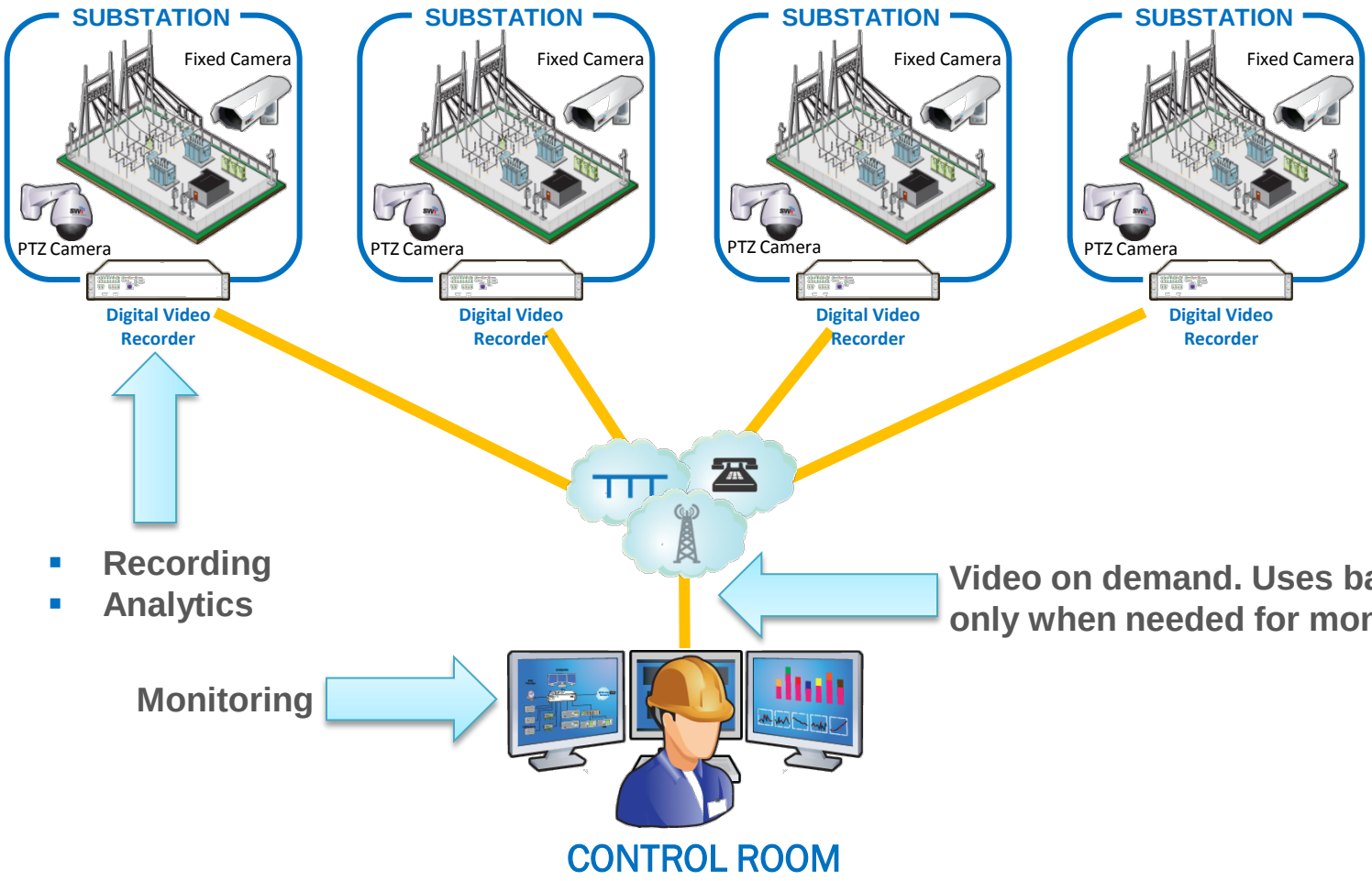
- Architecture: Centralized vs Distributed
- Bandwidth and Storage Considerations
- Camera Selection and Locations
- Hardware and Software Specifications

Architecture - Centralized



" Intelligent Video Monitoring Solutions for the Protection of Critical Infrastructure."

Architecture - Distributed



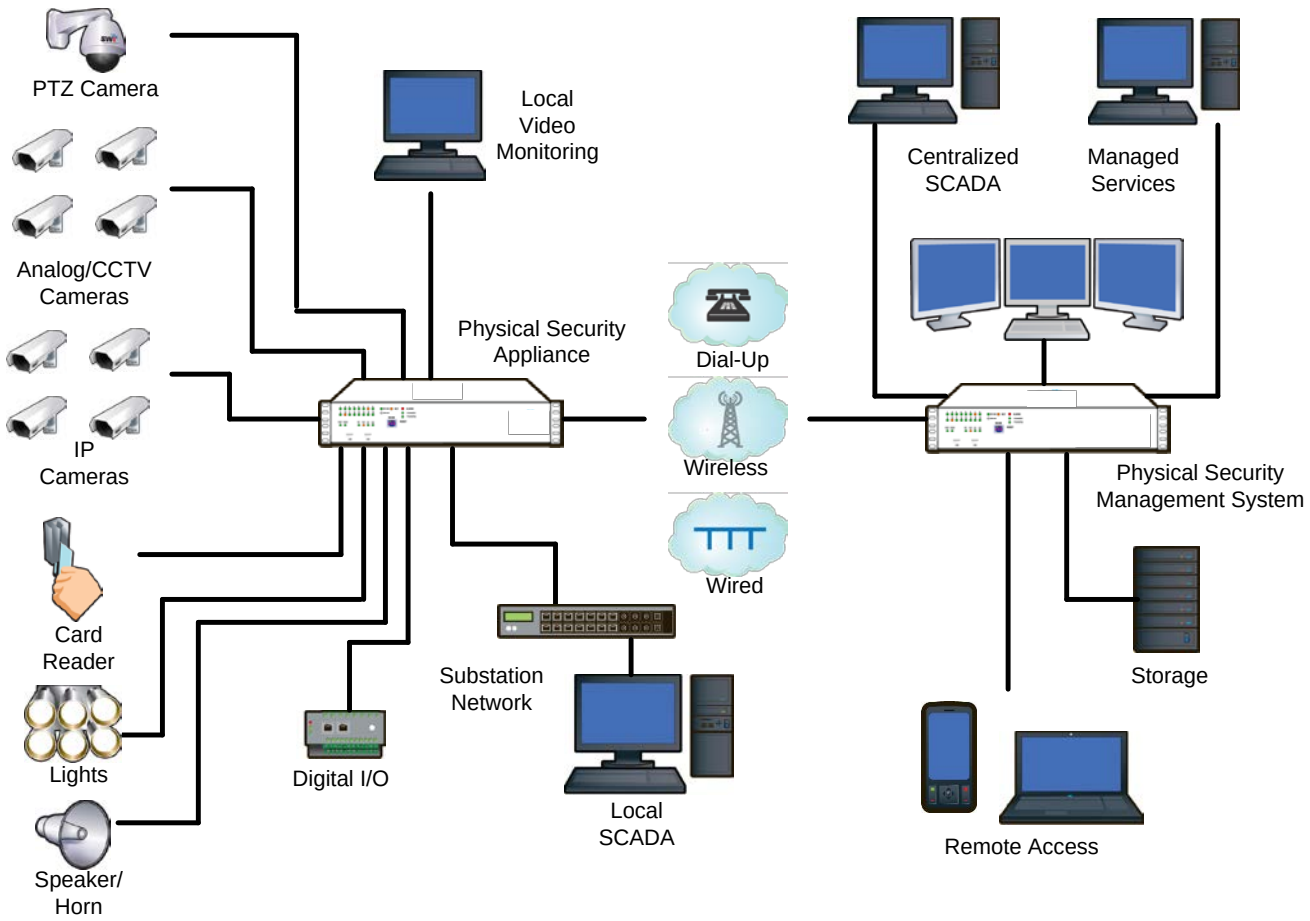
" Intelligent Video Monitoring Solutions for the Protection of Critical Infrastructure."

Private and Confidential

Architecture Comparison

Centralized	Distributed
Only cameras at the substation	Cameras and at least one video server in each substation
Needs a lot of bandwidth	Optimized bandwidth
Any problem in the network will stop the recording process	Constant recording, even when there are problems in the network
Limited users	Multiple users

Video Monitoring Solution Architecture



Key Components:

- Video Surveillance
- Access Control
- SCADA Integration
- Communications
- Video Management /Storage
- Remote Access
- Managed Services

" Intelligent Video Monitoring Solutions for the Protection of Critical Infrastructure."

Private and Confidential

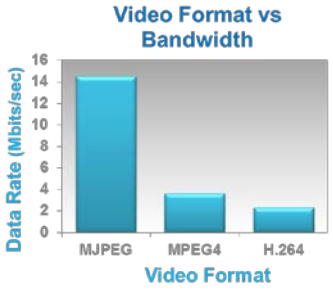
Guidelines for Video System Design

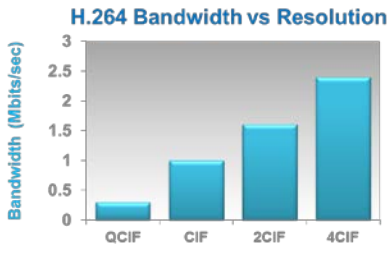
Key Items for Consideration

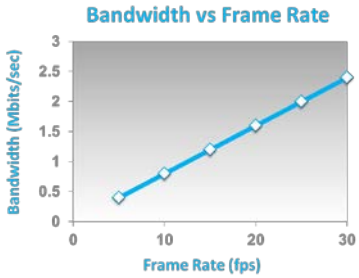
- Architecture: Centralized vs Distributed
- **Bandwidth and Storage Considerations**
- Camera Selection and Locations
- Hardware and Software Specifications

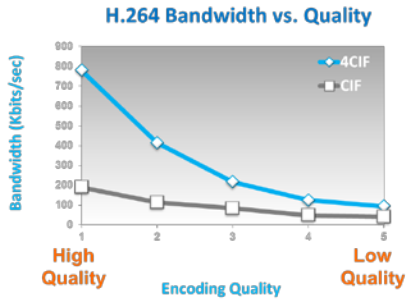
Bandwidth/Storage Optimization Techniques

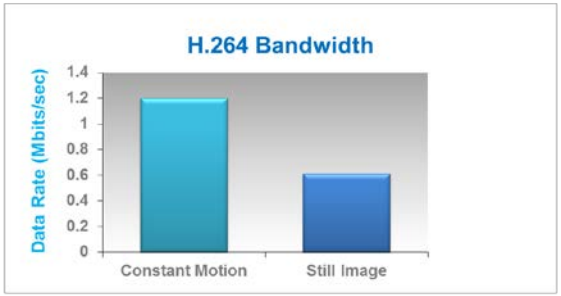
- Video Format
- Resolution
- Frame Rate
- Encoding Quality
- Installation Parameters
  - Camera Selection, Lighting, Amount of Motion Expected …
- Using Video Analytics for Automatic Detection
  - Send video only on pre-defined triggers
- Send video on a pre-defined trigger (eg. motion)
- Use multiple video channels with different settings for different users
- Local recording to reduce streaming











Guidelines for Video System Design

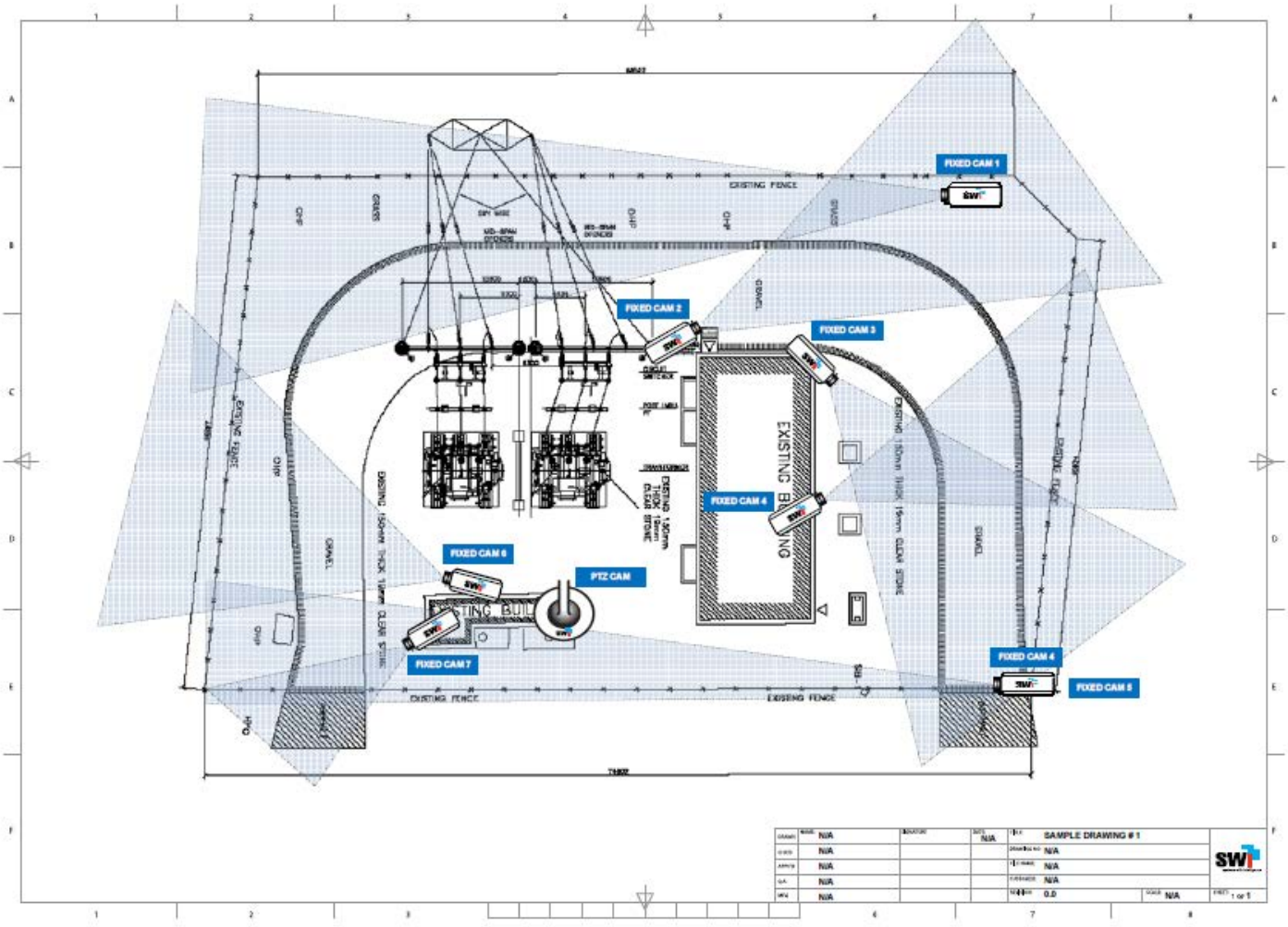
Key Items for Consideration

- Architecture: Centralized vs Distributed
- Bandwidth and Storage Considerations
- **Camera Selection and Locations**
- Hardware and Software Specifications

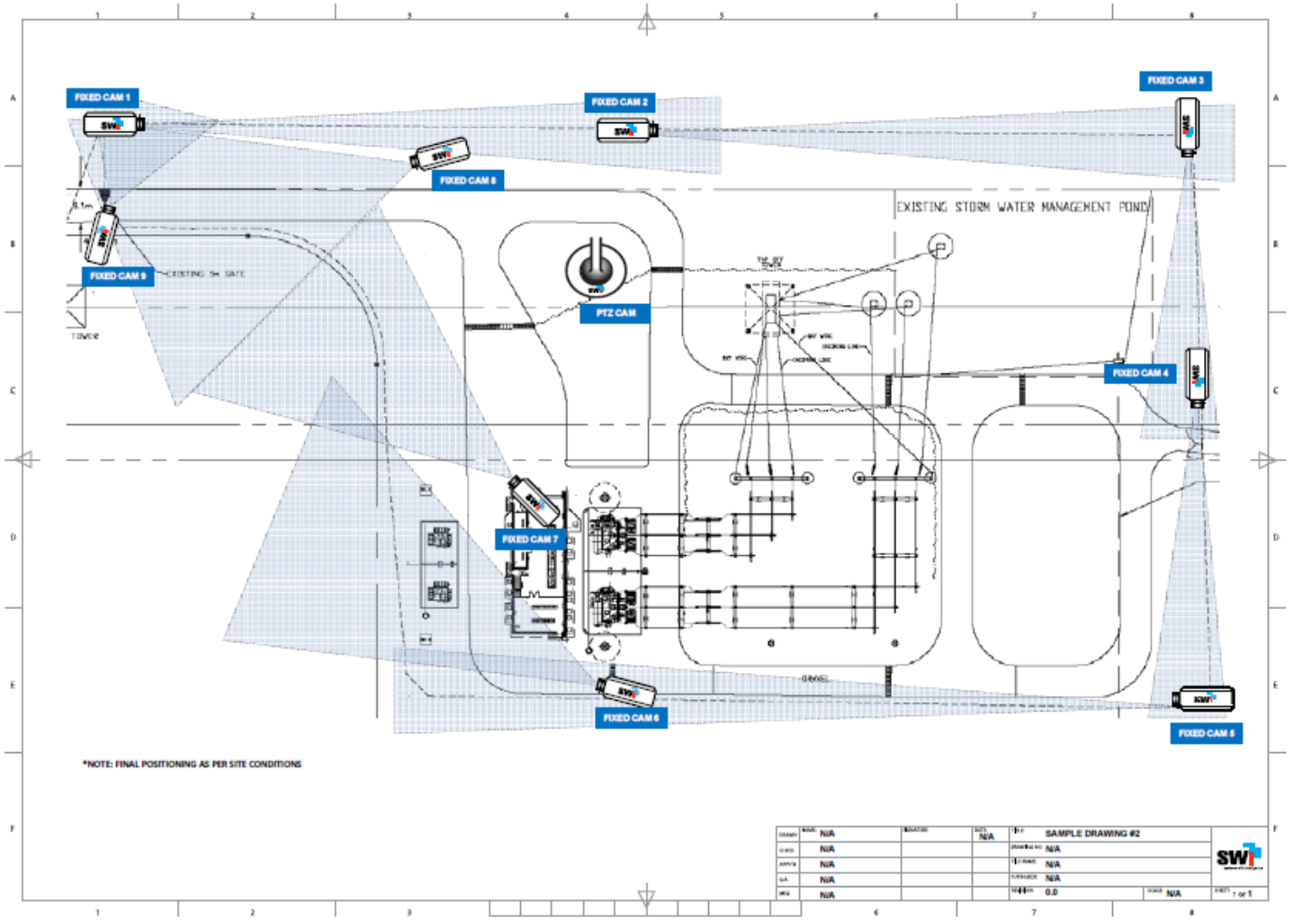
Camera Considerations

- **Analog vs IP**
  - Trend is towards IP
- **Fixed vs PTZ**
  - PTZ increases flexibility but is more costly
- **Camera Lenses** (Configuration)
  - Defining the field of view; Controlling the flow of light toward the image sensor; Focusing
- **Enclosure and Environmental Factors**
  - Resistant to Electromagnetic fields; Wide operating temperature range; lens occlusions; IP rating (IP66)

Camera Locations – Site Survey



Camera Locations – Site Survey



Guidelines for Video System Design

Key Items for Consideration

- Architecture: Centralized vs Distributed
- Bandwidth and Storage Considerations
- Camera Selection and Locations
- Hardware and Software Specifications

Video Monitoring System Hardware

- **Designed for harsh substation environments**
  - Meets Substation Specifications: eg. IEC61850-3, IEEE1613
  - Wide operating temperature (- 40ºC to +85ºC), no fans
- **Industrial rated power supply with dual power supply option**
- **Ability to handle IP and Analog Cameras**
  - "IP-enable" legacy CCTV cameras, use existing installed cameras
- **Multiple communication network options**
  - LAN and WAN interfaces (copper, fiber, wireless, etc)
- **Integration Features**
  - Serial Ports, Digital I/O
  - Access control and other physical security

Video Management Software

- Real-time viewing of multiple remote sites
  - Multiple clients can connect to any Digital Video Server
- Digital video recording
  - local and centralized storage
- Integrated video analytics for automatic detection of events
- Alarm and event notification through email
- SCADA Integration options (eg. DNP, Modbus)
- System can be optimized to available network bandwidth

Intelligent Video Surveillance – Video Analytics

- **Motion detection:**
  - automatically detection motion in a field of view
- **Perimeter violation (or "virtual tripwire"):**
  - monitor a fence line for any intrusion (eg. someone jumping a fence)
- **Camera tampering:**
  - determine if a camera has been compromised
- **Loitering:**
  - determine if people are loitering near a restricted area

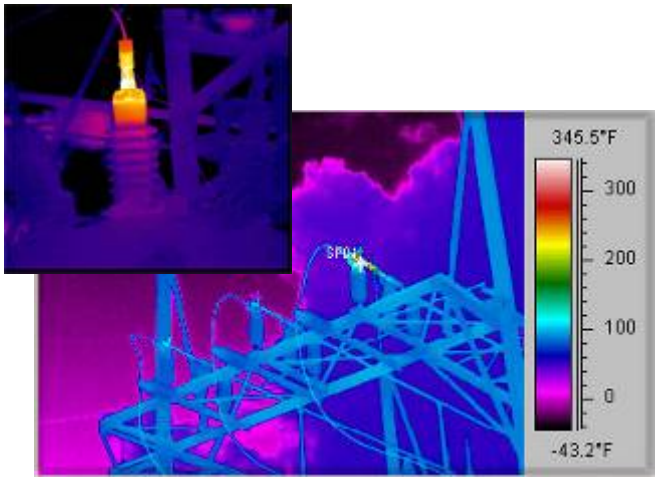
Software Algorithms for Automatic and Accurate Detection of Events!

Video Analytics – Automatic Detection of Events

- Motion Detection
- Virtual Tripwire
- Loitering
- Camera Tampering

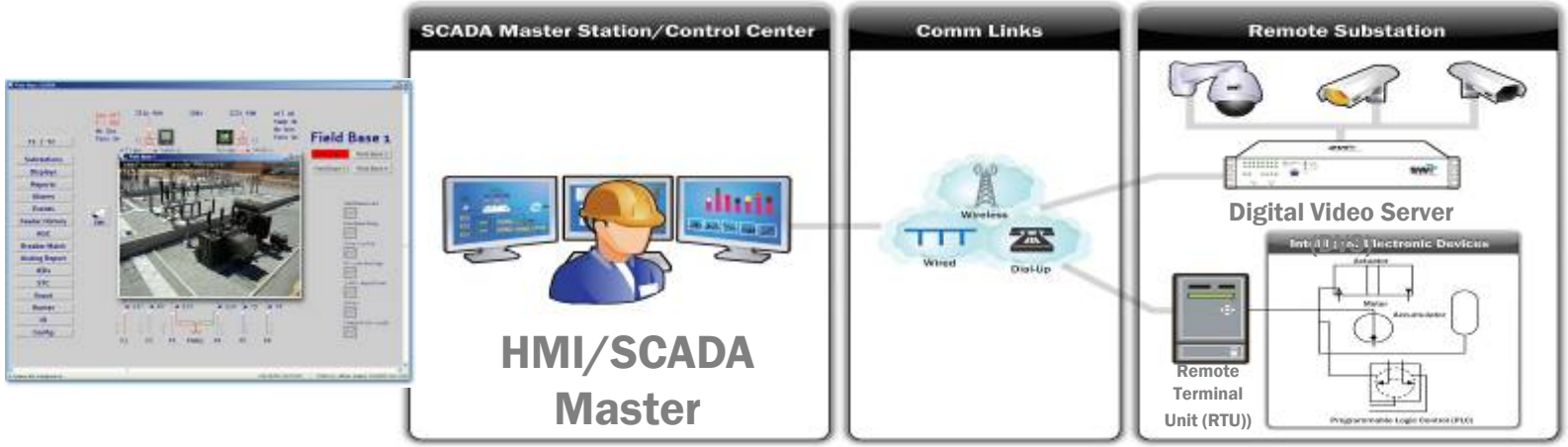
Example of Video Analytics in Action

Asset Monitoring Using Thermal Cameras



- Continuous and automatic remote monitoring of critical substation components
- Preventive Maintenance: Provide early warning of impending equipment failures – reduce downtime and chance for failures
- Obtain temperature readouts of overheating
- Automated alarm and email notification when problems are detected
- Thermal camera cost have come down dramatically, making thermal camera applications cost effective

Integrating Video with SCADA



- Allows Video Management System video data and statuses to be accessible from a SCADA system
- Digital Video Server is seen as an IED or RTU to the Master Station
- Integrate into existing HMI's (via API or system calls)
- Obtain alarm and event information via standard utility protocols (DNP3, Modbus)

NERC CIP Compliance and Video Systems

CIP 006	Physical Security controls should be documented and implemented that provide perimeter monitoring and logging along with robust access controls. All cyber assets used for Physical Security are considered Critical and should be treated as such.

Requirement	Short Description	Applicability of Video Systems
R1	Physical Security Plan	"Processes, tools, and procedures to monitor physical access to the perimeter(s)", "measures to control entry at those access points"
R2	Physical Access Controls	"implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week."
R3	Monitoring Physical Access	"monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week"
R4	Logging Physical Access	"logging physical entry at all access points to the Physical Security Perimeter(s) ", "Video Recording: Electronic capture of video images of sufficient quality to determine identity."
R5	Access Log Retention	"shall retain physical access logs for at least ninety calendar days.", "Logs related to reportable incidents shall be kept in accordance with the requirements"
R6	Maintenance and Testing	

Video Systems are an Important Tool in NERC Compliance!

Conclusions

- **Video Monitoring Can Be Used Effectively for a Variety of Purposes:**
  - **Security:** Protect critical transmission and distribution infrastructure; Reduce theft and damage to physical assets
  - **Asset Monitoring:** Increase asset utilization and improve efficiencies
  - **Safety:** Create safety zones for workers and the public
  - **Regulatory Compliance:** Help to meet new regulations such as NERC CIP
- **Solutions Designed for Electric Utilities are Available Today**
  - Traditional video surveillance solutions were designed for "commercial" applications
  - Newer solutions that deal with the unique conditions present in substations make "useful" video monitoring more feasible

Intelligent Video Monitoring Solutions
for the Protection of Critical Infrastructure

1215 Meyerside Drive, Unit #7, Mississauga, Ontario, L5T-1H3 Canada Phone: +1-289-562-0126 Fax: +1-289-562-0152
Email: info@SystemsWithIntelligence.com

www.SystemsWithIntelligence.com

Challenges for Electric Utilities

- Reliability and uptime of the Electric Grid – mission critical application!
- Theft, vandalism, sabotage, terrorism or other damage to the critical infrastructure
- How to comply with regulatory requirements for physical security (eg. NERC)
- Widely dispersed infrastructure typically in remote locations
- Unmanned facilities
- Not enough resources for any type of dedicated monitoring
- Finding technology solutions that can withstand harsh substation environments (eg. EMI, temp.) and which can interoperate with existing systems (eg SCADA)