UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 11

Always A Pioneer, Always Ahead

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UTeM

Physical and Environmental Security

Dr Zaheera Zainal Abidin
zaheera@utem.edu.my

MyUTeM

By the end of the lesson the student will be able to:

a) understand the meaning of the physical and environmental security concept

b) explain the perimeter areas, data centers, and standard for protection

c) explain the standard of operation in protecting the assets in the organization

OVERVIEW

- Introduction
- Environmental Sensors: A technology background
- Automated response to environment threats
- The netbotz solution
- Components of a defense in depth strategy
- Challenge of integration
- Data center meltdown

INTRODUCTION

INTRODUCTION - TERMINOLOGY

- The physical and environmental security means measures taken to protect people, facility, equipment, system, offices and the infrastructure of the organization from unauthorized physical access, damage and misuse activities. **Reference**: ISO 270001 : 2013 A.11
- The Physical (Environmental) Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physical, protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

Reference: *CISSP CIB*, January 2012 (4.17.14 Rev. 13)

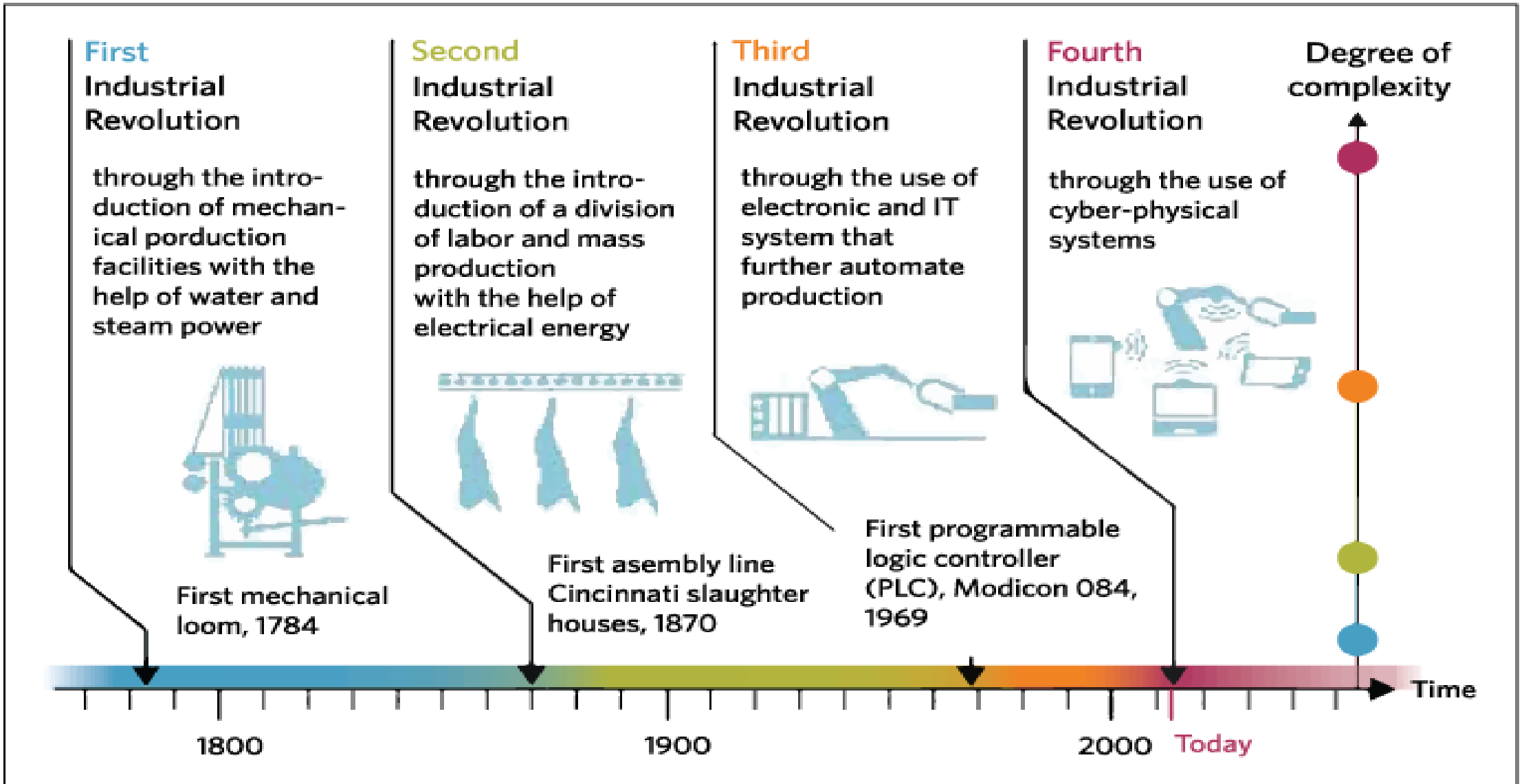
INTRODUCTION – 1

- Physical environment security integrates environmental sensors products with Enterprise Security Management (ESM).
- The environmental sensors are intended to alert and respond to physical threats to IT system, in order to prevent disasters (e.g., temperature increases) from causing a massive outage.
- With early detection and strategic policies, efficiencies in maintaining operational activities can be achieved.

INTRODUCTION – 2

- Due to industrial revolution 4.0, the use of physical and environmental sensors has become wider since the IT devices and gadgets included in the operational processes such as in manufacturing, healthcare systems, transportation and business intelligent system (BIS).

IN THE INDUSTRY 4.0 ERA



INTRODUCTION – 3

- Five fundamental areas are:
  - Information Protection Requirements
  - Information Protection Environment
  - Security Technology and Tools
  - Assurance, Trust and Confidence
  - Information Protection and Management Services

Information Protection Requirements-1

- Perimeter and Building Areas
- Building Entry Points
- Inside the Building – Building Floors
- Data Centers or Server Room Security
- Object Protection
- Computer Equipment Protection

Information Protection Requirements-2

- Risks to CIA (Confidentiality, Integrity and Availability) :
  - Interruptions in computer services – Example of Availability
  - Physical Damage – Example of Availability
  - Unauthorized Disclosure of Information – Example of Confidentiality
  - Loss of Control over Information – Example of Integrity
  - Physical Theft – Example of Confidentiality, Integrity and Availability

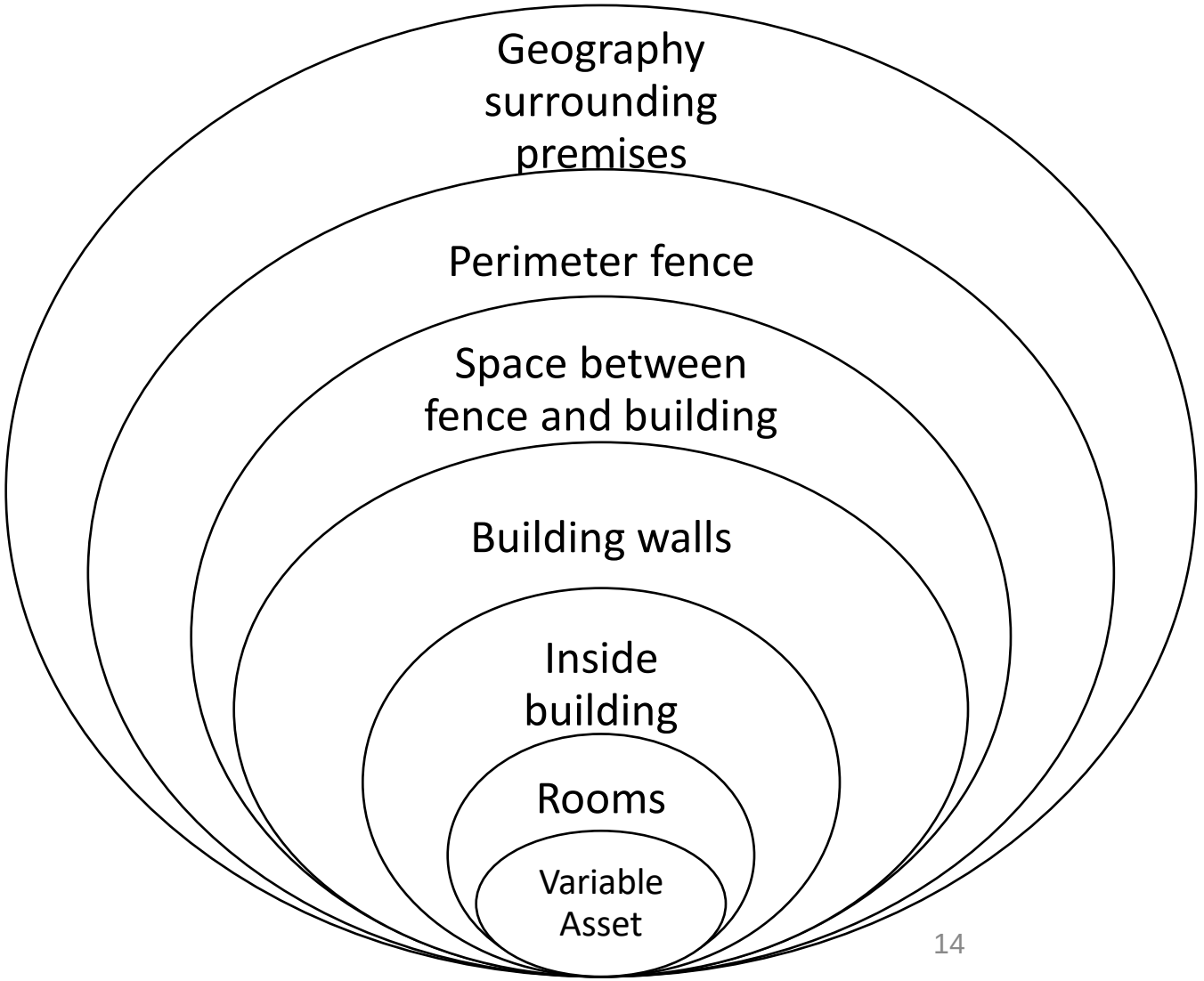
Information Protection Environment-1

- List the threat, type of threat, in protecting the environment. What is threat?
- Threat is any event with potential to cause loss of Asset, personal injury or loss of live.
- There are 2 types of Threat :
  - Natural / Environmental
    - Pandemic Flu (i.e.: COVID 19, H1N1)
    - Earthquakes, Flood, Fires, Snow and Smoke
  - Human Made / Political Events
    - Terrorist attacks, vandalism, explosion, theft, sabotage
    - Acts of commission or omission

Information Protection Environment-2

- Designing Site Location
  - Include WHERE the building and HOW it should be built:
  - Choosing a secure site:
    - Visibility – any landmark or mark on the building
    - Local consideration – is it in flood area, is it near to waste dump area?
    - Natural disaster – is it landslide? Flood?
    - Transportation – near to highway? Near to public transportation?
    - Joint Tenancy – Is there any HVAC near the building?
    - Adjacent Building
    - External Services

Information Protection Environment-3

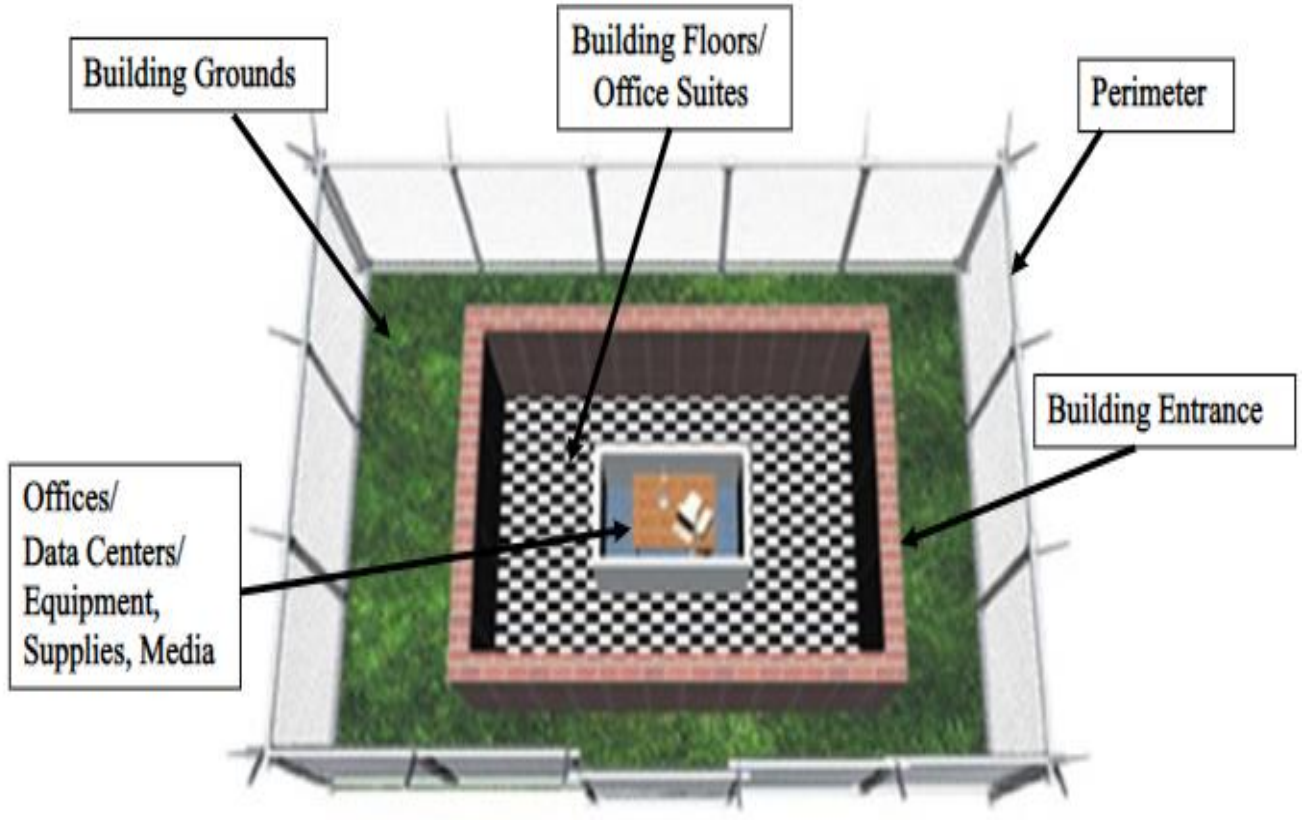


Layered Defense Model

Information Protection Environment-4

Layered Defense Model

- Approaching security through “layers” of controls
- Multi-layered
- Starts with the perimeter, then building grounds, then building entry points



Information Protection Environment-5

- Design a Secure Site
  - Walls
    - Wall must meets the acceptable fire rating
  - Ceiling
    - The ceiling needs to follow the standard of fire rating
  - Floors
    - Slab or raised?
    - If slab – if concrete then weight typically 150 pounds per square foot
    - If raised – need to meet fire rating and electrical conductivity
    - Must employ non-conducting surface material in data center

Information Protection Environment-6

- Doors
  - The door need to follow standard and requirement by forced entry
    - Solid or hollow
  - Electrical doors or emergency exit
  - If emergency exits must be clearly marked or monitored
- Windows
  - Must follow standard plate glass (brittle or breaks easily)
  - Tempered glass (stronger, or easily breaks into small pieces)
  - Bullet resistant windows
  - Glass breakage sensors
  - Bomb blast film

Information Protection Environment-7

- Procedural Controls
  - Guards Post / Dogs
  - Checking and escorting visitors on site
  - Managing deliveries to the site
- Facility security management
  - Administrative security controls that is not related to initial planning process
    - Audit trails
      - the entrance and exit attempts determined Who, when and where in log file
    - Emergency procedures
      - Documentation is a must
      - Update periodically

Information Protection Environment-8

- Audit Trails
  - Date and time of access attempt
  - Whether the attempt was successful or not
  - Where the access was granted
  - Who attempted the access
  - Who modified the access privileges at the supervisor level
  - Send alarms or alerts is required
- Emergency Procedures
  - Should include the following:
    - Evacuation procedures
    - Emergency system shutdown procedures
    - Periodic equipment and systems test

Information Protection Environment-9

- Administrative Personnel Controls
  - Pre-Employment Screening
    - Backgrounds investigation
    - Employment and educational history checks
  - On-Going Employee Checks
    - Security clearance
    - Ongoing ratings on employee by supervisors
  - Post-Employment Procedures
    - Exit interview
    - Return of computers
    - Removal of network access
    - Removal of email access

Information Protection Environment-10

- Environmental and Life Safety Controls
  - 3 areas of environmental control
    - Electrical power
      - Green, clean and steady power
      - Excellent power quality
      - Power threat and Protective Measures
        - Noise – interference: EMI, RFI. Protection: proper line conditioning, proper grounding, space heater
        - Anomalies – brownout, blackout, spike, surge
        - Electrostatic discharge – low humidity (40% - 60%)
    - Fire detection and surge suppression – use to protect electrostatic field, UPS to spare some time before safely shutdown
    - Heating, Ventilation and Air Conditioning (HVAC)-70-74 Ferenheit
      - Who is responsible, clear the step to be determined

Security Technology and Tools-1

- Areas, assets and tools for protection are :
  - Badges, Restricted Areas, Lights, Dogs, CCTV, Locks, Access Control, Barriers, Fences, IDS and Security Forces.
- Functions for Technology and Tool Selection based on :
  - Deter, Delay, Detect, Access and Respond
- The Layered Defense needs to be based on :
  - Biometric Access and Exit Sensors
  - UPS and Backup
  - Redundant HVAC Equipment
  - Electronic Motion Sensors
  - Continuous Video Surveillance

Security Technology and Tools-2

- The first line of Defense is the Perimeter Security Control.
- The protective barriers either natural or structural
  - Natural Barriers
    - Landscaping (Trees, Mountain, River, Canyon, Sea)
  - Structural Barriers
    - Fence, Gate, Wall
    - For fence - Required Height for fencing:
      - 3 ft – 4ft or 6 ft – 8 ft or 8 ft with 3 strands of barbed wire
      - 3 types of fencing:
        - Chain link
        - Barbed Wire
        - Barbed Tape / Concertina Wire

Security Technology and Tools-3

- Structural Barriers
  - 3 types of fencing:
    - Chain link
      - 6 ft / 8 ft / 2 inch opening or less
      - Within 2 inches of ground or below surface
    - Barbed Wire
    - Barbed Tape / Concertina Wire

Security Technology and Tools-4

- Intrusion Detection System and Surveillance
  - Perimeter Intrusion Detection Systems
    - Sensors that detect access into the area
      - Photoelectric
      - Ultrasonic
      - Microwave
      - Passive Infrared (PIR)
      - Pressure Sensitive (Dry Contact Switch)
- Surveillance Devices
  - Closed-Circuit Television (CCTV) – camera (fix/zoom/pan/tilt), transmission media (coaxial/fiber/wireless) and monitoring
    - CCTV Levels: Detection, Recognition and Identification
    - Monitoring Live Events is Preventive and Recording Events is Detective

Security Technology and Tools-5

- Lighting
  - Provides a deterrent to intruders
  - Makes detection similar if object matched
  - Should be used with other controls such as fence, CCTV and patrol
  - Types of Lighting:
    - Continuous (Glare Projection / Flood Lighting)
    - Trip
    - Standby
    - Movable
    - Emergency

Security Technology and Tools-6

- Access Control
  - Card Access
    - Smart Card
    - Magnetic Stripe Card
    - RFID tag and RFID reader
  - Biometrics
    - Fingerprint
    - Retina or Iris Scans
    - Signature Dynamics

Security Technology and Tools-7

- Locks
  - Types of locks
    - Key locks
    - Combination locks
  - Key Locks
    - Key-in-knob
    - Dead bolt lock
    - Mortise lock
    - Padlock
  - Combination Locks
    - Combination number must be changed under specific circumstances

Security Technology and Tools-8

- Locks
  - Keyless (Cipher) Locks
    - Push-button locks
  - Smart Locks
    - Permit only authorized people into certain door at particular time
  - Key Control Measures
    - Keep record of all keys
    - Investigate the loss of all keys
    - Use as few master key as possible
    - Key is a single factor authentication that it can be lost, stolen or copied (use 2-factor authentication)
    - Restrict issue of key on a long term of duration

Security Technology and Tools-9

- Data Center
  - Walls
    - The wall needs to be extended from the true floor to actual ceiling
  - Access Controls
    - Depending on sensitivity of the equipment and electronic access controls that need to be installed
- Portable Device Security
  - Laptop and PDA – protect the data in the device
    - Lock cable for docking stations
    - Tracing software
    - PIN Protection
    - Encryption Software

Security Technology and Tools-10

- Alarm Systems
  - Local Alarm Systems – at least 400 ft
  - Central Stations Units – < 10 minutes travel time and monitored 24x7
  - Proprietary Systems – owned and operated by customer, features same as central station units
  - Auxiliary Station Systems – systems that ring at local fire or police station

Assurance, Trust and Confidence-1

- Drills / Testing / Exercise
  - Keeps everyone aware on the responsibilities
  - Alert on evacuation
- Physical Vulnerability / Penetration Tests
  - Identify Weak Entry Points
  - Findings – must documented
- Checklist, Maintenance & Service
  - Checklist
    - Identify elements of physical security that need to be checked
  - Maintenance & Service
    - What needs to be done, need to monitor the maintenance (if contractor)

Information Protection and Management Services-1

- Managed Services
  - Contractor follows the requirements stated in the agreement
  - The contracting organization can audit the security services provided
  - There is a channel of communication between the contracting authority and contractor
- Media Storage Requirements
  - Common Storage Areas for Media
    - On site / off site
  - Elements and Resources to Protect Media
    - Physical Access Control at Storage Area
    - Environmental Controls
    - Audits

Information Protection and Management Services-2

- Data Destruction and Reuse
  - Overwriting destroys most data
  - Formatting Data
  - Paper records = Burn
  - Paper Shredding

ENVIRONMENTAL SENSORS: A TECHNOLOGY BACKGROUND

Environmental Sensors - Overview

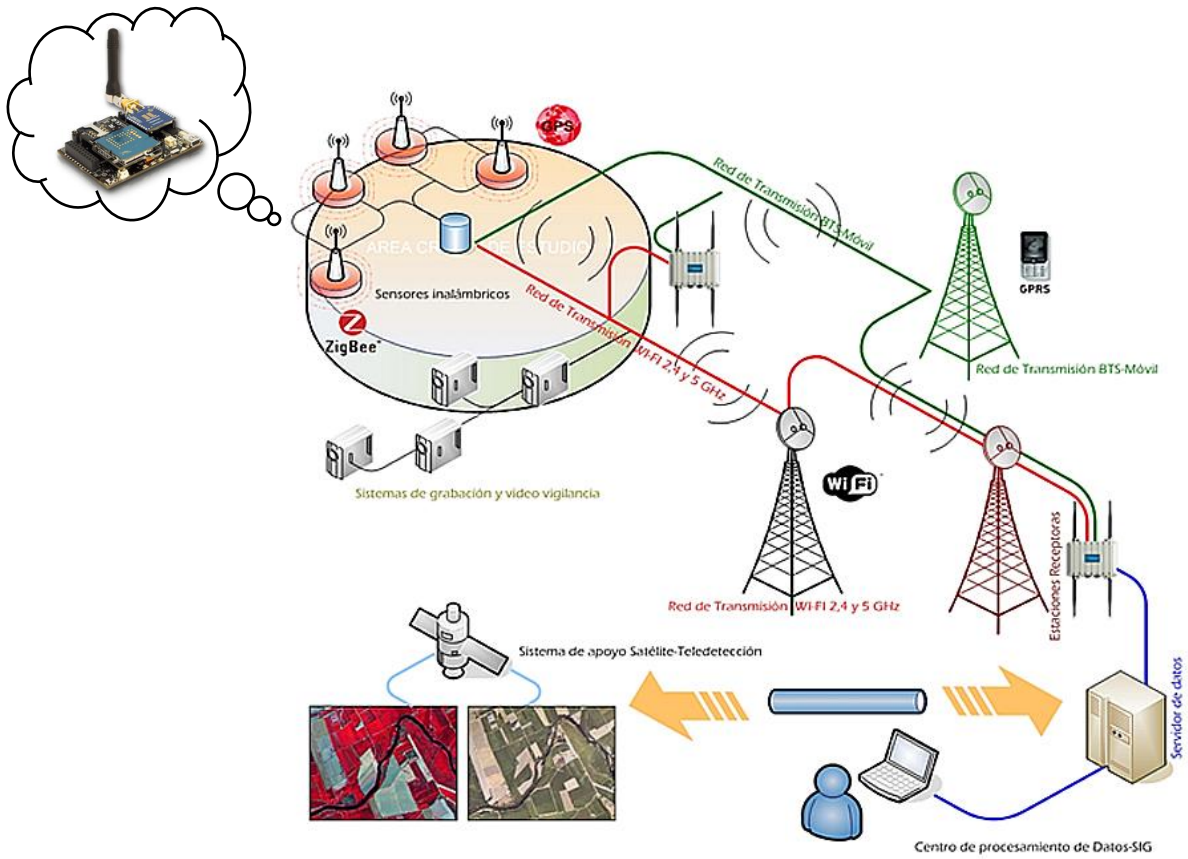
- The environmental sensors typically do the monitoring process and it is not a new idea.
- For example:
  - The room temperature at the accurate Celsius (in Hotels)
  - Smoke Detector (in Building)
  - Lighting (in Energy)

Environmental Sensors – Sensor Type

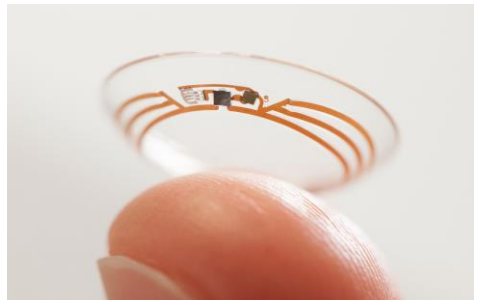
- Voltage Sensors – Batteries or UPS
- Humidity Sensors – Battery leakage, rusting and premature aging of equipment
- Temperature Sensors – Air conditioning outages especially in data center
- Fluid Sensors – Water and electronics
- Airflow Sensors – Enough air is flowing to prevent hot spots
- Motion Sensors – Alerted to presence of a person
- Audio Sensors – Noise detector

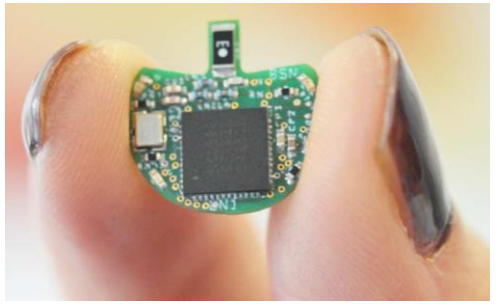
Environmental Sensors: Example

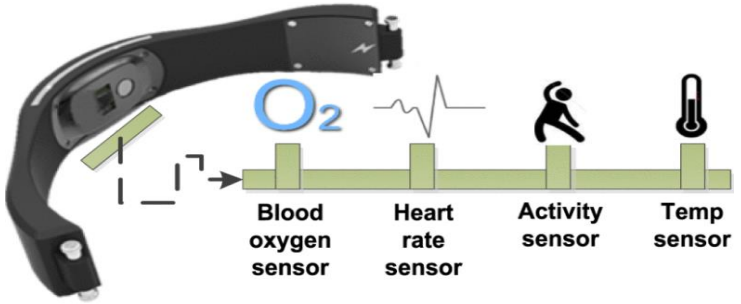
- Detecting Forest Fire using Wireless Sensor Networks

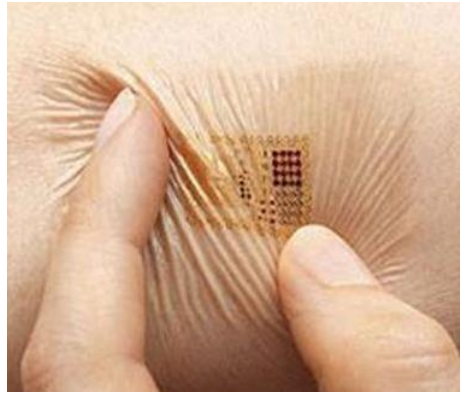


- Body Sensor Networks









Environmental Sensors: Remote Response

- Remote response is a system to alert the operators (human) in the center unit to prevent the disaster from occurring (i.e., close the valve remotely or remote device configurations) even though the control from a distance or involve geographical area.
- To perform remote response, need to follow IPMI Standard.

IPMI Standard

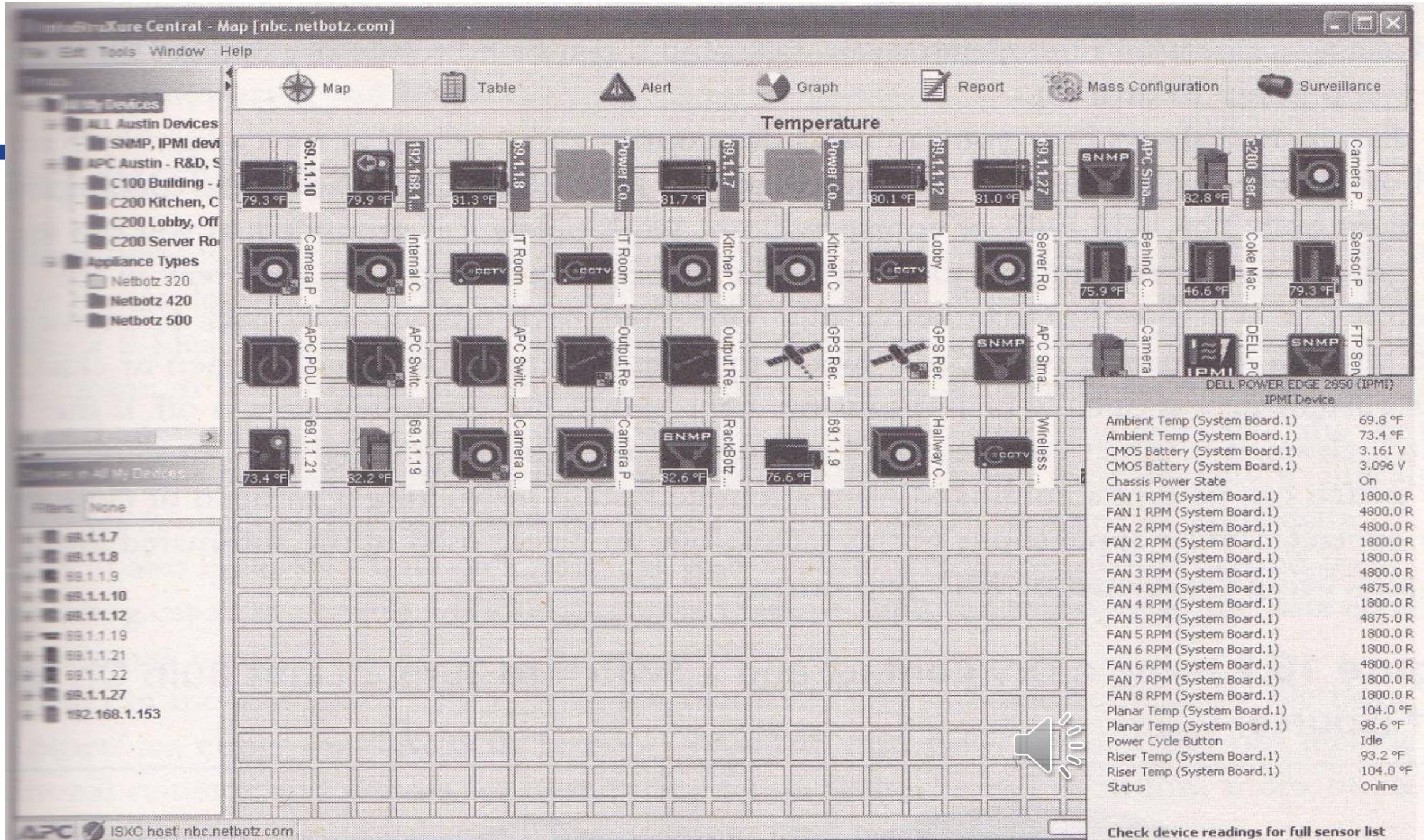
- IPMI is an abbreviation standard for Intelligent Platform Management Interface (IPMI).
- IPMI performs a monitoring and managing computer systems
- A set of interfaces used to communicate with computer hardware and firmware
- Out-of-band interfaces, even if a system is powered down, communication is still possible
- Dell, HP, Intel and IBM have adopted the IPMI standard

IPMI Standard – The key information

- Packet Format
- Enable system packet over Ethernet
- Other Communication Mechanisms
- Serial or Modem
- Sensor codes
- Standard for programmers to understand the meanings of communication
- How to retrieve information
- Standard include way to communication with an IPMI-enabled system and request data from component.

Download tools: http://sourceforge.net/projects/ipmitool

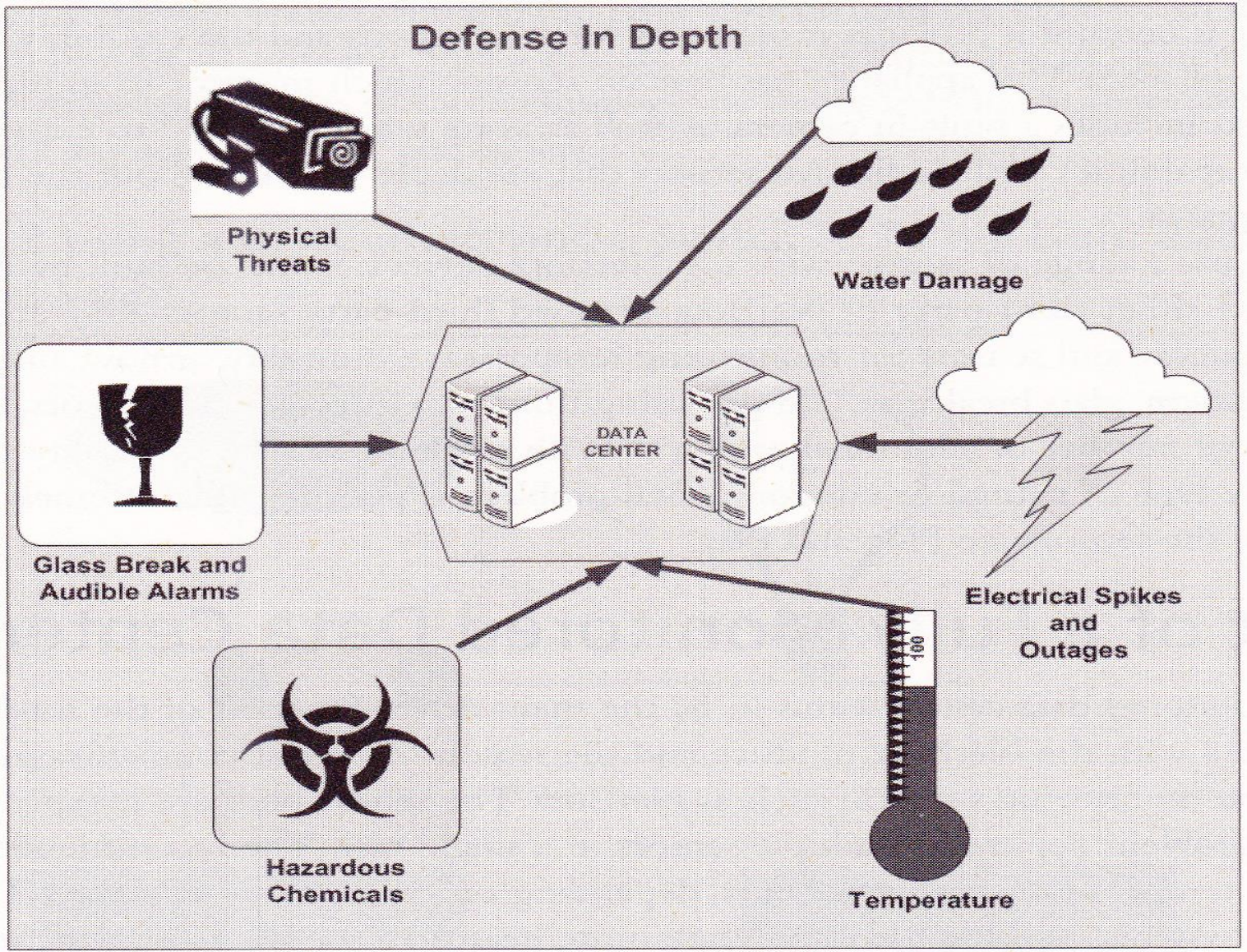
Download www.intel.com/design/servers/ipmi


Xure Central - Map [nbc.netbotz.com]
File Edit Tools Window Help
Map
Table
Alert
Graph
Report
Mass Configuration
Surveillance
Temperature
My Devices
ALL Austin Devices
SNMP, IPMI devi
APC Austin - R&D, S
C100 Building -
C200 Kitchen, C
C200 Lobby, Off
C200 Server Ro
Appliance Types
Netbotz 320
Netbotz 420
Netbotz 500
Filters: None
69.1.1.7
69.1.1.8
69.1.1.9
69.1.1.10
69.1.1.12
69.1.1.19
69.1.1.21
69.1.1.22
69.1.1.27
192.168.1.153
DELL POWER EDGE 2650 (IPMI)
IPMI Device
Ambient Temp (System Board.1) 69.8 °F
Ambient Temp (System Board.1) 73.4 °F
CMOS Battery (System Board.1) 3.161 V
CMOS Battery (System Board.1) 3.096 V
Chassis Power State On
FAN 1 RPM (System Board.1) 1800.0 R
FAN 1 RPM (System Board.1) 4800.0 R
FAN 2 RPM (System Board.1) 4800.0 R
FAN 2 RPM (System Board.1) 1800.0 R
FAN 3 RPM (System Board.1) 1800.0 R
FAN 3 RPM (System Board.1) 4800.0 R
FAN 4 RPM (System Board.1) 4875.0 R
FAN 4 RPM (System Board.1) 1800.0 R
FAN 5 RPM (System Board.1) 4875.0 R
FAN 5 RPM (System Board.1) 1800.0 R
FAN 6 RPM (System Board.1) 1800.0 R
FAN 6 RPM (System Board.1) 4800.0 R
FAN 7 RPM (System Board.1) 1800.0 R
FAN 8 RPM (System Board.1) 1800.0 R
Planar Temp (System Board.1) 104.0 °F
Planar Temp (System Board.1) 98.6 °F
Power Cycle Button Idle
Riser Temp (System Board.1) 93.2 °F
Riser Temp (System Board.1) 104.0 °F
Status Online
Check device readings for full sensor list
ISXC host nbc.netbotz.com

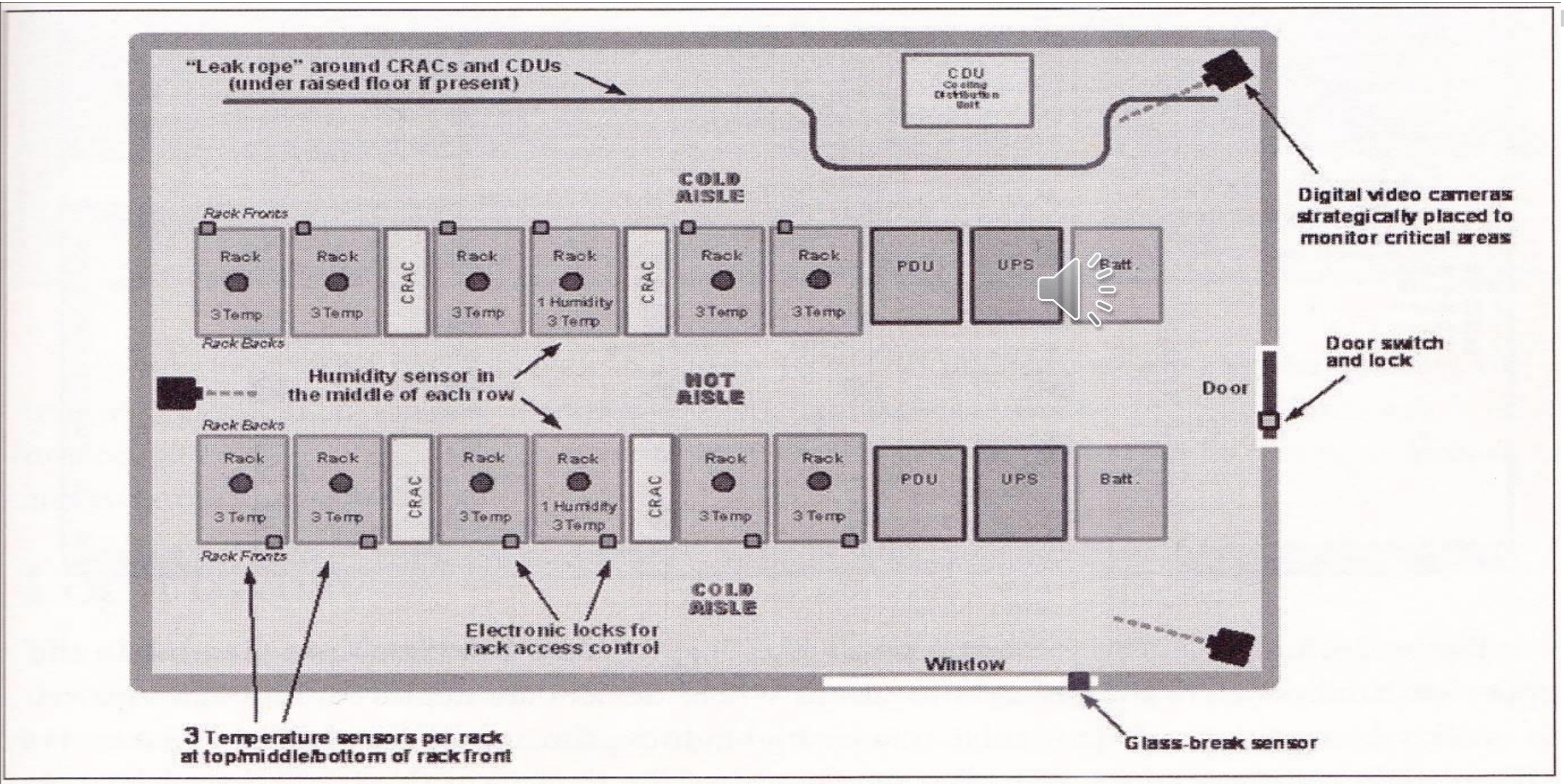
Automated Response to Environmental Threats – The Netbotz Solution

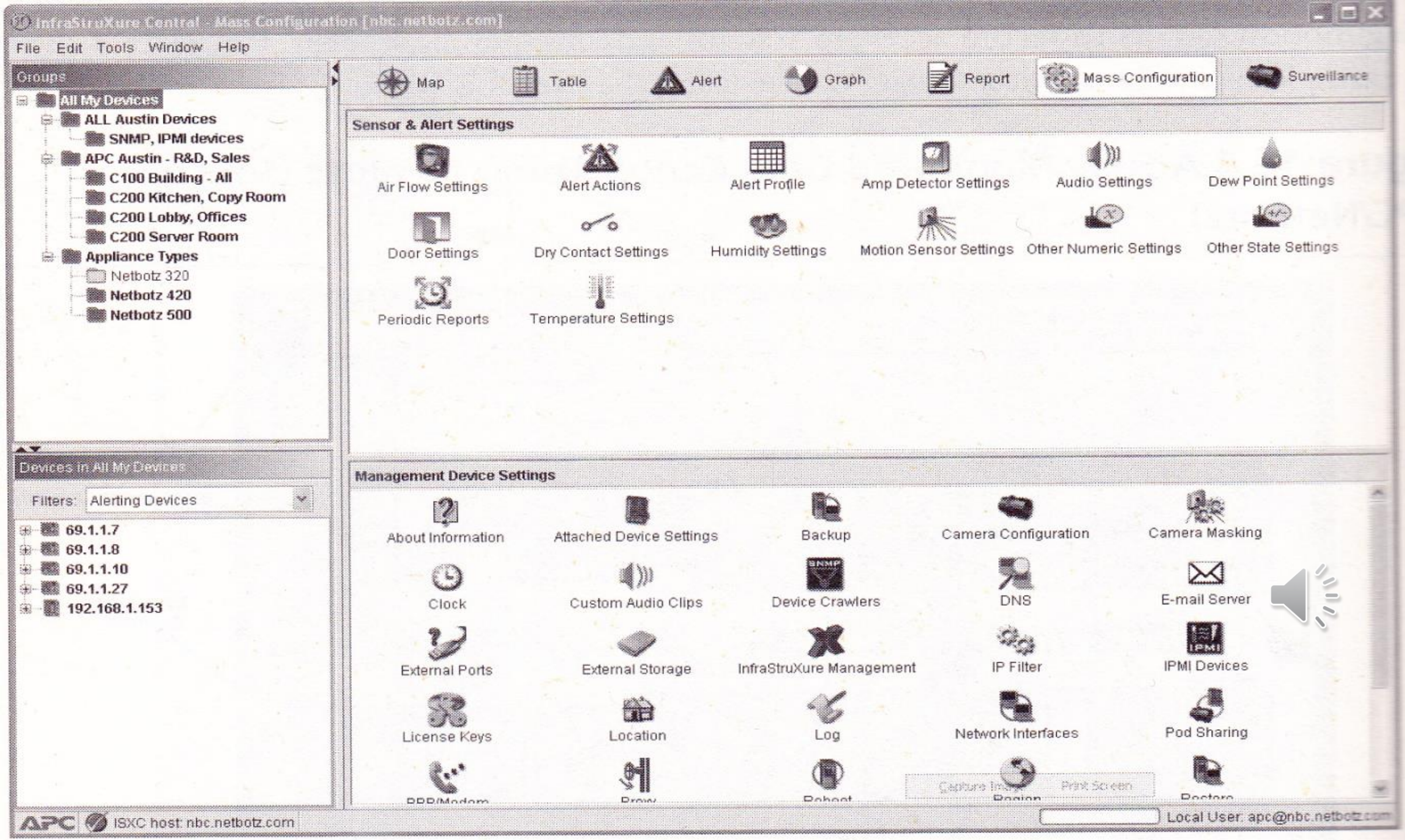
- Netbotz offers a complete solution include video monitoring capabilities, controlling and monitoring power in data center
- Provides more expandable and more ports of sensor pods
- Can add-ons the variety of sensors with Plug and Play
- Can monitor a large number of additional products
- Provide built-in 24/7 monitoring

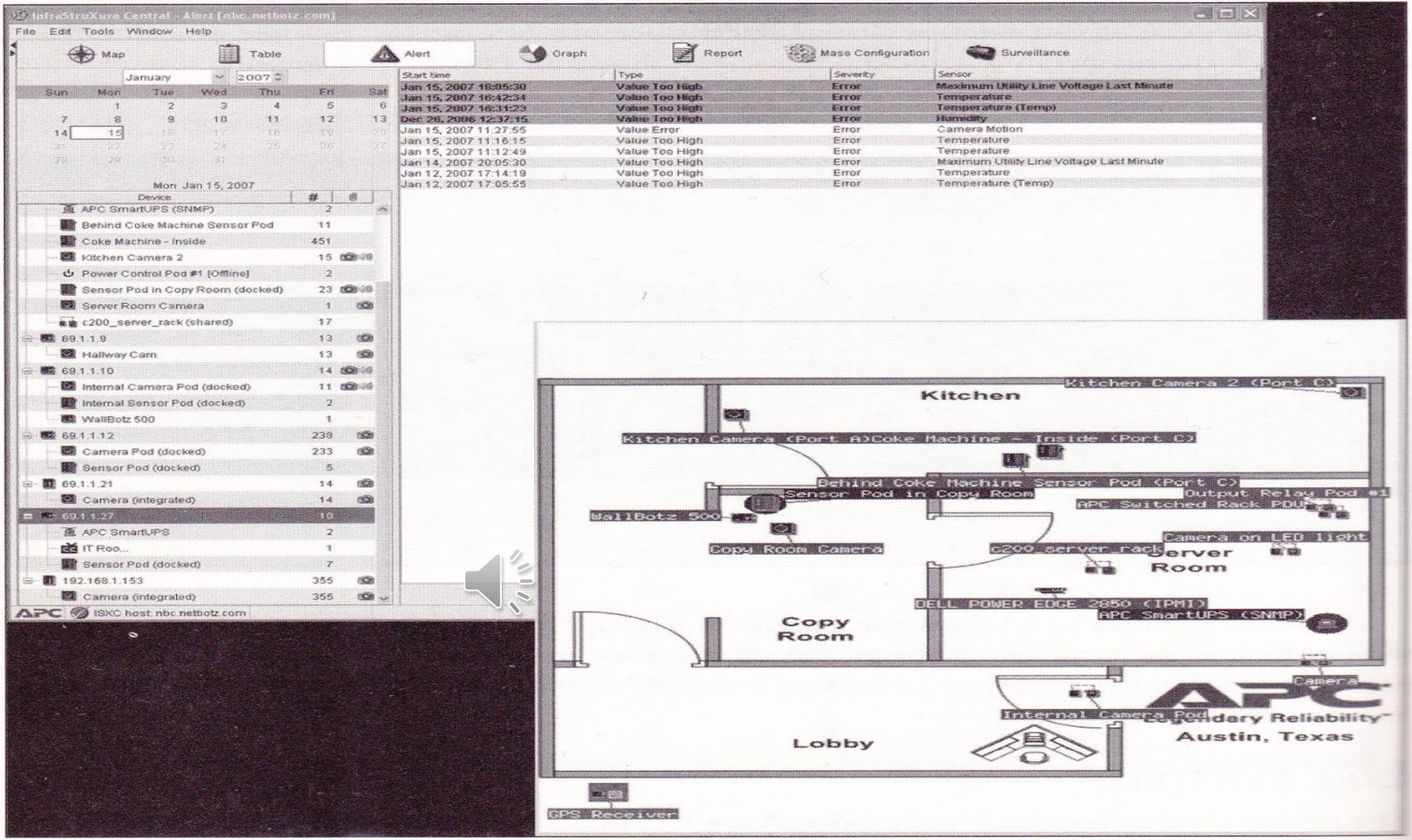
Components of a Defense in Depth Strategy



Data Center with NetBotz




InfraStruXure Central - Mass Configuration [nbc.netbotz.com]
File Edit Tools Window Help
Groups
All My Devices
ALL Austin Devices
SNMP, IPMI devices
APC Austin - R&D, Sales
C100 Building - All
C200 Kitchen, Copy Room
C200 Lobby, Offices
C200 Server Room
Appliance Types
Netbotz 320
Netbotz 420
Netbotz 500
Devices in All My Devices
Filters: Alerting Devices
69.1.1.7
69.1.1.8
69.1.1.10
69.1.1.27
192.168.1.153
Map
Table
Alert
Graph
Report
Mass Configuration
Surveillance
Sensor & Alert Settings
Air Flow Settings
Alert Actions
Alert Profile
Amp Detector Settings
Audio Settings
Dew Point Settings
Door Settings
Dry Contact Settings
Humidity Settings
Motion Sensor Settings
Other Numeric Settings
Other State Settings
Periodic Reports
Temperature Settings
Management Device Settings
About Information
Attached Device Settings
Backup
Camera Configuration
Camera Masking
Clock
Custom Audio Clips
Device Crawlers
DNS
E-mail Server
External Ports
External Storage
InfraStruXure Management
IP Filter
IPMI Devices
License Keys
Location
Log
Network Interfaces
Pod Sharing
PPP/Modem
Prow
Reboot
Restore
Capture Image
Print Screen
Region
APC
ISXC host: nbc.netbotz.com
Local User: apc@nbc.netbotz.com


File Edit Tools Window Help
Map
Table
Alert
Graph
Report
Mass Configuration
Surveillance
January
2007
Sun Mon Tue Wed Thu Fri Sat
Mon Jan 15, 2007
Start time
Type
Severity
Sensor
Jan 15, 2007 16:05:30 Value Too High Error Maximum Utility Line Voltage Last Minute
Jan 15, 2007 16:42:34 Value Too High Error Temperature
Jan 15, 2007 16:31:23 Value Too High Error Temperature (Temp)
Dec 26, 2006 12:37:15 Value Too High Error Humidity
Jan 15, 2007 11:27:55 Value Error Error Camera Motion
Jan 15, 2007 11:16:15 Value Too High Error Temperature
Jan 15, 2007 11:12:49 Value Too High Error Temperature
Jan 14, 2007 20:05:30 Value Too High Error Maximum Utility Line Voltage Last Minute
Jan 12, 2007 17:14:19 Value Too High Error Temperature
Jan 12, 2007 17:05:55 Value Too High Error Temperature (Temp)
Device
APC SmartUPS (SNMP)
Behind Coke Machine Sensor Pod
Coke Machine - Inside
Kitchen Camera 2
Power Control Pod #1 [Offline]
Sensor Pod in Copy Room (docked)
Server Room Camera
c200_server_rack (shared)
69.1.1.9
Hallway Cam
69.1.1.10
Internal Camera Pod (docked)
Internal Sensor Pod (docked)
WallBotz 500
69.1.1.12
Camera Pod (docked)
Sensor Pod (docked)
69.1.1.21
Camera (integrated)
69.1.1.27
APC SmartUPS
IT Roo...
Sensor Pod (docked)
192.168.1.153
Camera (integrated)
ISXC host: nbc.netbotz.com
Kitchen
Kitchen Camera 2 (Port C)
Kitchen Camera (Port A)Coke Machine - Inside (Port C)
Behind Coke Machine Sensor Pod (Port C)
Sensor Pod in Copy Room
Output Relay Pod #1
APC Switched Rack PDU
WallBotz 500
Copy Room Camera
c200_server_rack
Camera on LED light
Server Room
DELL POWER EDGE 2850 (IPMI)
APC SmartUPS (SNMP)
Copy Room
Camera
Internal Camera Pod
Lobby
APC
Austin, Texas
GPS Receiver

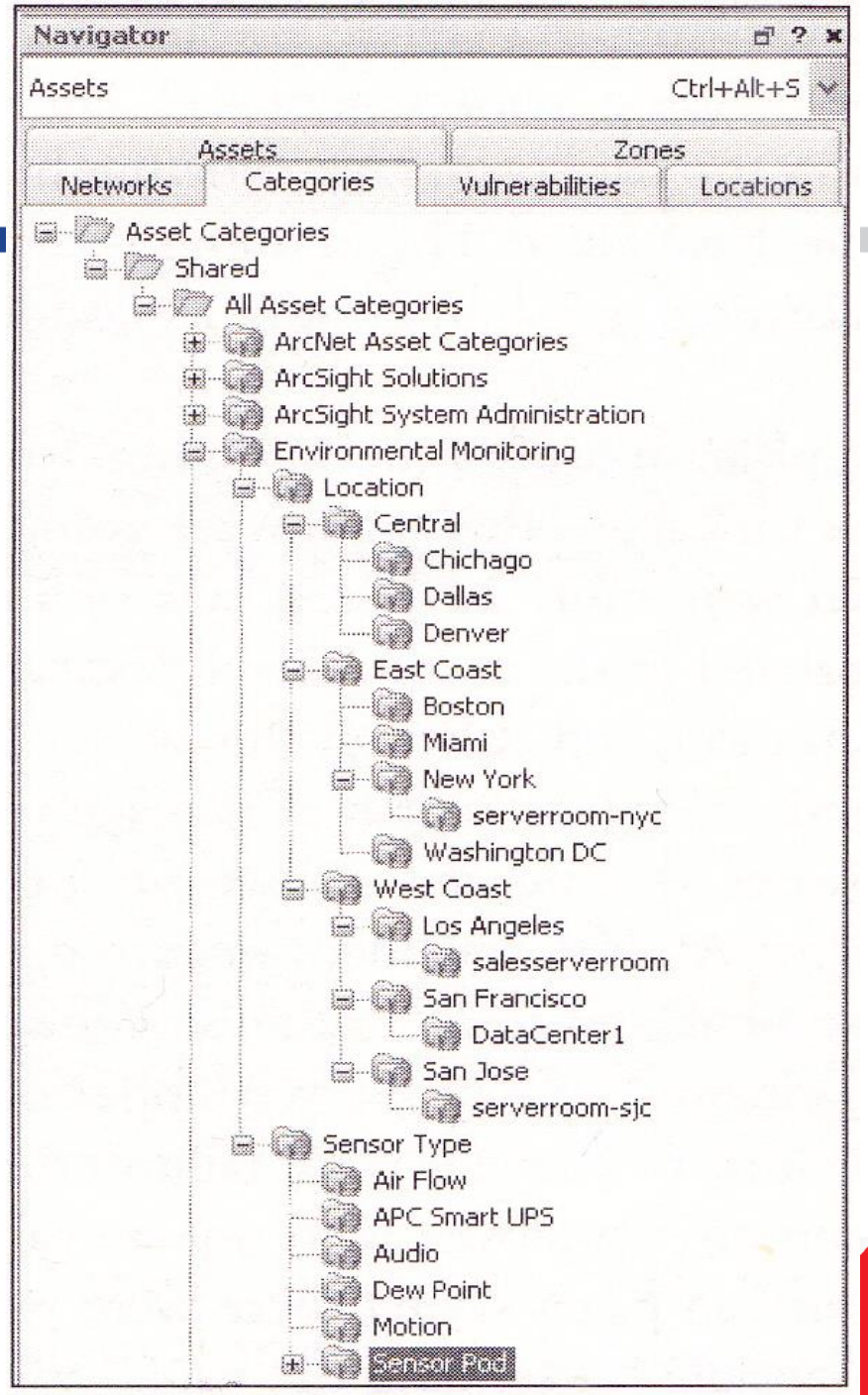
AUTOMATED RESPONSE TO ENVIRONMENT THREATS

Threats to Physical Security

- Natural/Environmental (e.g. earthquake, floods, storms, fires and hurricanes)
- Utility Systems (e.g., communication outages, power outages)
- Human-Made/Political Events (e.g., explosions, vandalism, theft, terrorist attacks, riots)

Challenges of Integration

- Integrating a product such as NetBotz with ESM is a challenging task.
- Firstly, identify the alarm and monitor multiple data centers that provide the alert.
- Secondly, classification based on location, function, asset and critically, which the sensor is part of the device and asset in the ESM system.



Challenges of Integration

- Once the operator identifies that an alert is detected and additional information is provided about the location, type of the sensor and critical location, it will be easily for the operator to decide the next task to be done.
- Moreover, the operator could make a statistical analysis based on per-location if the problem occurred. Also, the operator could provides analysis results to the management for keeping the data center and server room safe from harmful activities.

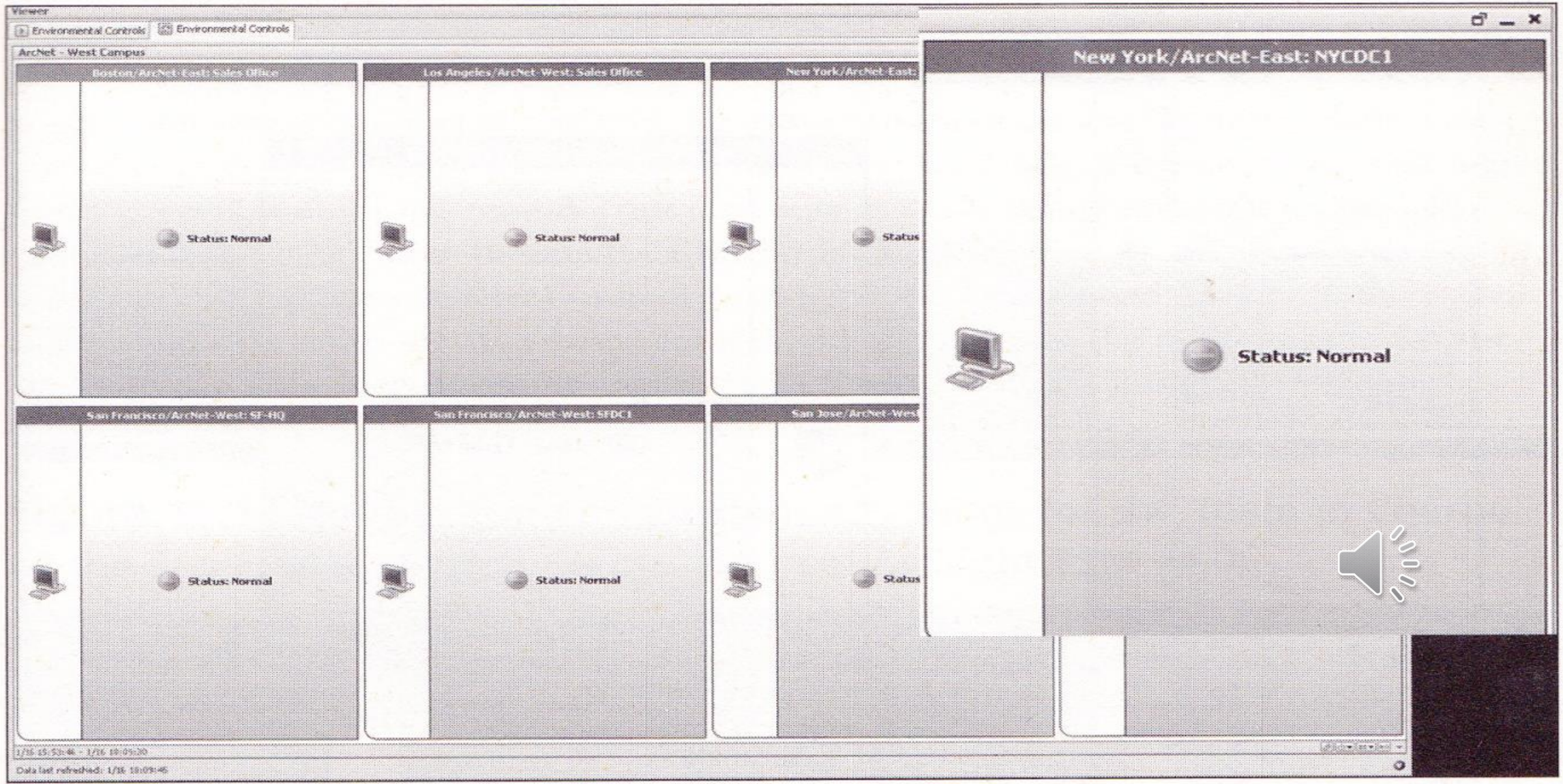
Challenges of Integration

- NetBotz sends a simple event to the ESM system. Each NetBotz sensor is automatically connected into the ESM system and function as an asset.
- Once the NetBotz recognize the asset, the whole asset functionality with ESM system is enabled.
- However, if the data center (NOC/SOC) is centralized in another state, how the operator knows the person in charge who would respond?

Challenges of Integration

- ESM sends alert to different groups of sensors and assets and also among users and assigned owners to various sensors or assets.
- If the alert setup is enabled and the alert has been received by the operator in the SOC or NOC, then the alarm has been cleared. If no alert received, it means the operator need to investigates the problem and manually troubleshoot the asset owner and sensor.

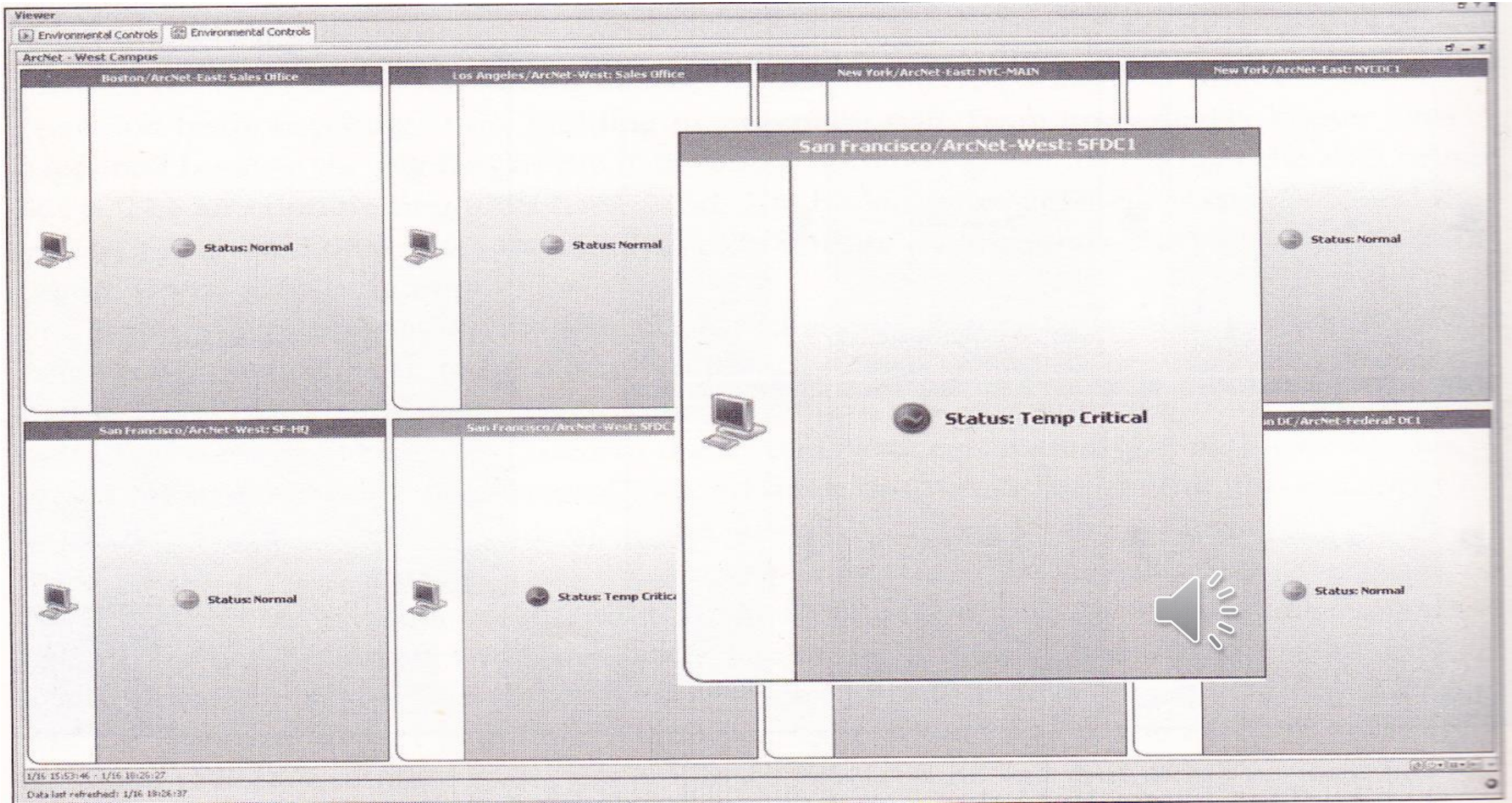
Challenges of Integration



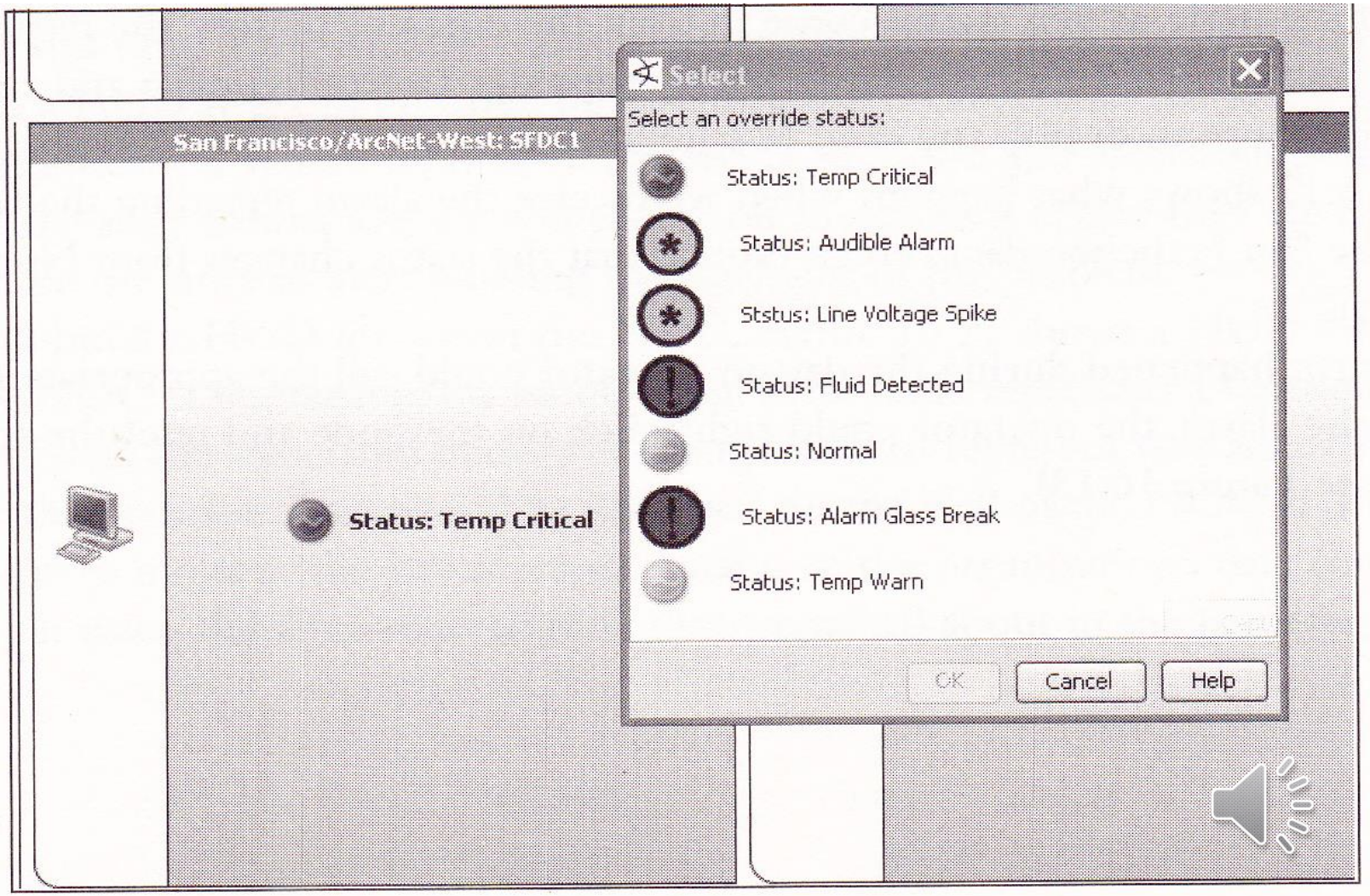
Challenges of Integration

- The individual node for each location is being monitored in the NOC. The dashboard shows that all asset is in a good condition since the status is “NORMAL”. The location is indicated on the title bar of each node and the status is indicated in the center of the node. When alarms come from different sensors, the display will change to reflect the current alarm status, which useful for different groups of user or assets at any stateful data.
- If alarm occurred during the day, the operator could just call the entity of user else the operator could reset the status back to “NORMAL”, by right-click to node and click reset.

Challenges of Integration



Challenges of Integration

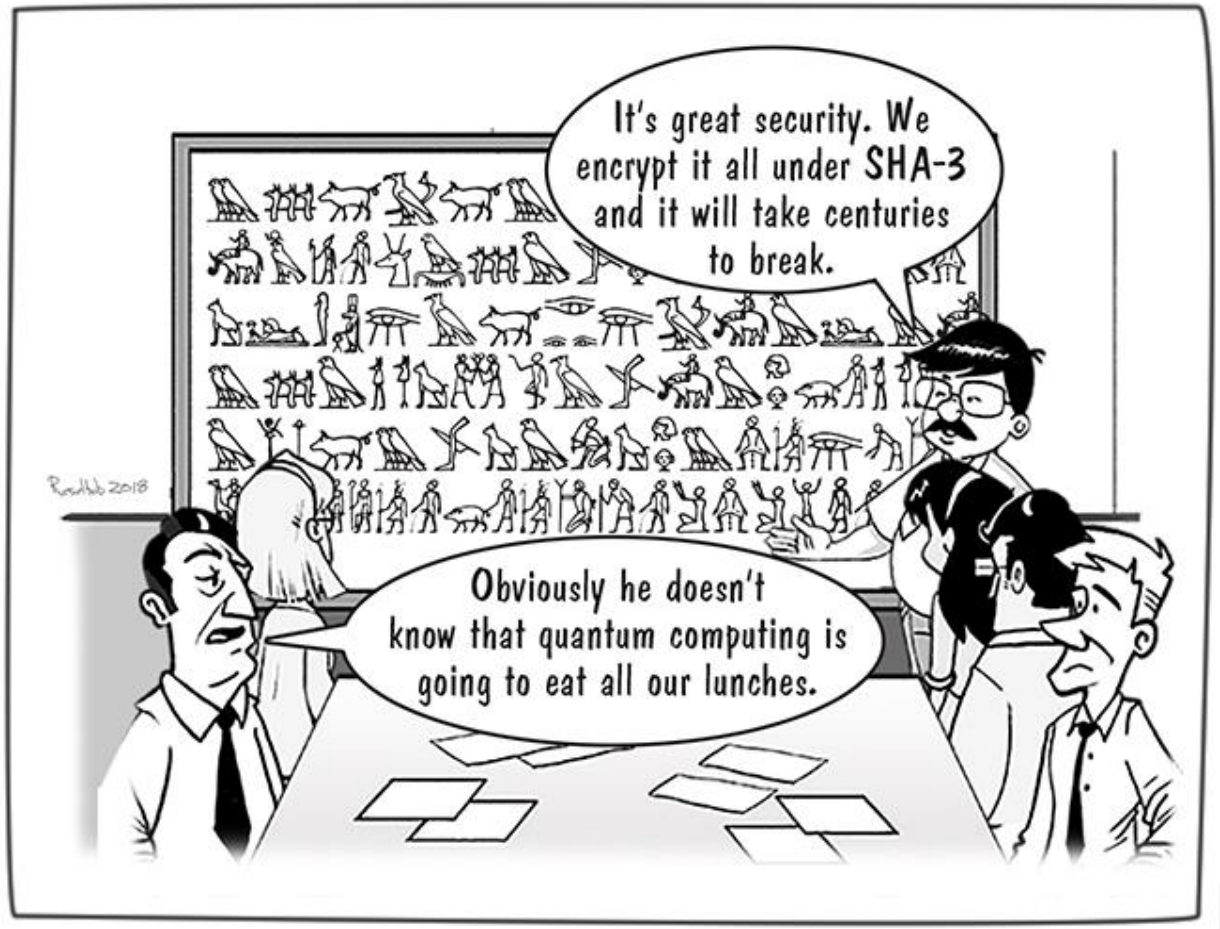


Challenges of Integration

- However, the air conditioners have failed and the organization does not have 24/7 on-site monitoring. ESM is configured to send notification depending on the location of the alarms and the criticality. If the alarm is just a warning, the system will not send a notification during off-hours.
- If the alarm is critical, it send an email notification. The time to set for a critical severity alarm is around 10 minutes to respond.

Data Center Meltdown

- Meltdown is a type of exploits (attack) that produce an out-of-order execution on modern processors to read arbitrary kernel-memory location.
- The impact of Meltdown: cost and compensation



CONCLUSION

Conclusion

- Monitoring for security incidents whether internal or external is extremely important.
- Availability is an important aspect of protection. If information system is unavailable, then the business will collapse.
- The emergence of products benefits the IT infrastructure and provide efficiency in NOC/SOC using ESM solution.
- A practical solution to build tool within console that query for all IP address using IPMI integration for better management.

EXERCISE

1. Identify the risk to facility, data, equipment and support system of the physical security.
2. Describe the threats, vulnerabilities and countermeasures related to physical protection of the organization's confidential information assets.

Thank You

MyUTeM

www.utem.edu.my