Creative Defense Techniques for Process Control Systems

Presenter:

Jonathan Pollet

VP Professional Services
Verano

plantdata technologies
a Division of Verano

Co-Presenter:

Clint Bodungen

President
Critical Infrastructure Institute, USA

Critical Infrastructure CIi Institute

QuickTime™ and a
decompressor
are needed to see this picture.

© 2005 PlantData Technologies

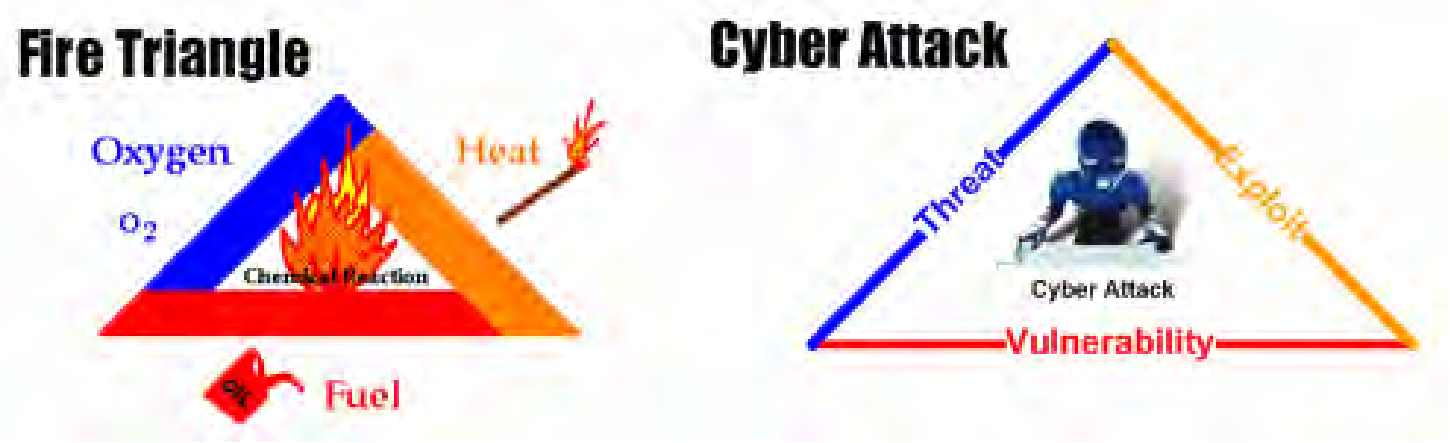
Overview of Presentation

- Security Review (Defining the Problem)
  - Threats, Vulnerabilities, and Exploits
  - Recent Incidents Impacting Performance and Security
  - Typical Vulnerabilities from Over 5 Years of SCADA Audits
- Architecture Review (What are We Trying to Secure)
  - Typical SCADA / DCS environment
  - Introduction to Concept of Defense in Depth “Component Layers”
- Creative Solutions
  - Perimeter vs. Subsystem Perimeter Protection
  - Virtual Patching
  - Authentication to legacy systems and Remote Access
  - Internal Network Monitoring
  - Building Internal IPSEC tunnels at the NIC layer using IPSEC “Teaming”
  - Using Native OS Scripts to Passively Monitor Workstations / Servers
- Summary
- Q & A

© 2005 PlantData Technologies

Ingredients for a Successful Cyber Security Attack

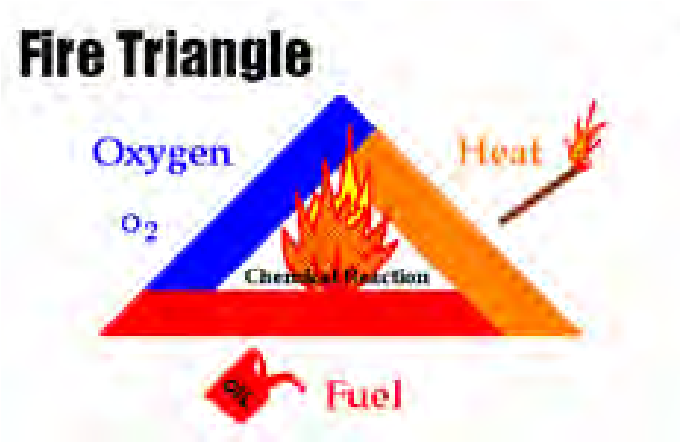
- A Cyber Attack is the result of the presence of a **Threat**, taking advantage of a **Vulnerability**, through a successful **Exploit**
  - Threats typically stem from people or organizations
  - Vulnerabilities are deficiencies in the security of a system
  - Exploits are created by Threats to take advantage of Vulnerabilities
- Think of this like the Fire Triangle

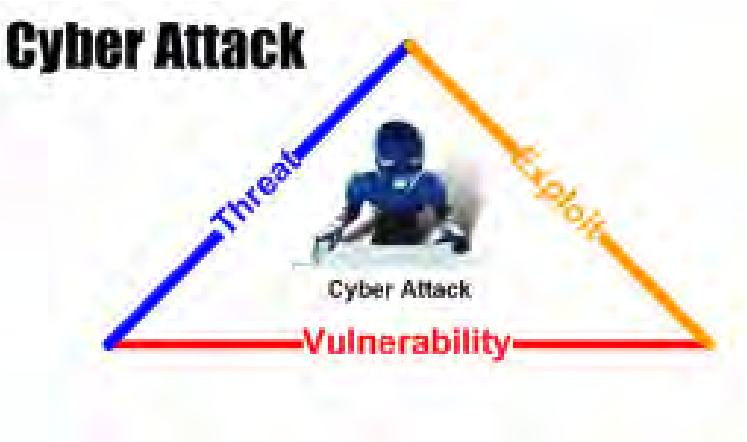


- Take any one leg out, and the Fire will be mitigated
- This same principle applies with Cyber Security

© 2005 PlantData Technologies

Understanding Each Element of a Cyber Attack





1. Threats can never fully be mitigated, so the strategy is to model or understand what the threats are and how they work
   - "Understanding the Threats"
2. Vulnerabilities Mitigated are either Eliminated, Reduced, or Managed, based on the Risk
   - "Mitigating the Vulnerabilities"
3. The chance of an Exploit being successful can also be reduced through Deterrents and Detectors
   - "Deterring and Detecting the Exploits"

© 2005 PlantData Technologies

Game Playing Affects Control System Performance

Problem

An industrial cyber security consultant in the U.S. was hired to investigate control system performance issues. Operators had found a way around console lockdown, allowing them to install games and streaming media. These programs were used during the night shift.

Consequences

Control system performance was reduced. Operators' distraction increased risk to the plant. Money and effort were spent investigating the problem, hiring an external consultant, and cleaning up the problem.

Key Control System Recommendations Consequences

Technology: File and process monitoring

Policy: Correct console lockdown procedure

Source: Verano contact

© 2005 PlantData Technologies

Hacked Historian Becomes Spam Server

Problem

A power generation company in the U.S. had a historian connected to the Internet to receive time syncing data (NTP). The server was compromised and used as a spam relay and a file server.

Consequences

Operators had slow display refresh rates and there was a huge bandwidth usage increase. Additionally, spam servers eventually become blacklisted in the Internet community. Valid emails from that company could be rejected by other companies subscribing to blacklisting services.

Key Control System Recommendations

Technology: Firewall, IDS/IPS, and file, process and bandwidth monitoring

Policy: Have dedicated NTP servers and put historians in a DMZ

Source: Verano contact

© 2005 PlantData Technologies

…and you wonder why NERC is calling for more background checks?

QuickTime™ and a
decompressor
are needed to see this picture.

Common Network Issues Found

- Security efforts focused solely on Corporate Internet interface point (Castle Model)
- Routers vs. Firewalls
- Out-of-date Router and Firewall Firmware
- Sharing network infrastructure with business/IT systems
- Use of clear-text protocols for device configuration
- Insufficient network separation between corporate and real-time control systems
- Access to critical systems by IP range only, allowing easy spoofing
- Access to critical systems for 3rd parties and remote users often wide open once authentication is made (too much privileges)
- Network Performance and Security Monitoring not typically found on the Industrial Networks.

© 2005 PlantData Technologies

Workstations/Server Configuration

- Password cracking made easy with LMHash enabled (left ON by default installation)
- Easy-to-Guess Passwords
- Null-Session Authentication
- Local Security Policy left with defaults
- Security Event Logging Often Not Enabled
- Domain Security Policy often not used in real-time systems due to multiple domains
- Heavy use of Shared Folders on workstations
- Shared Folders have access set to “Everyone”
- Dual-Network cards installed and in use
- Most Critical Servers Not Being Monitored for Performance or Security Events

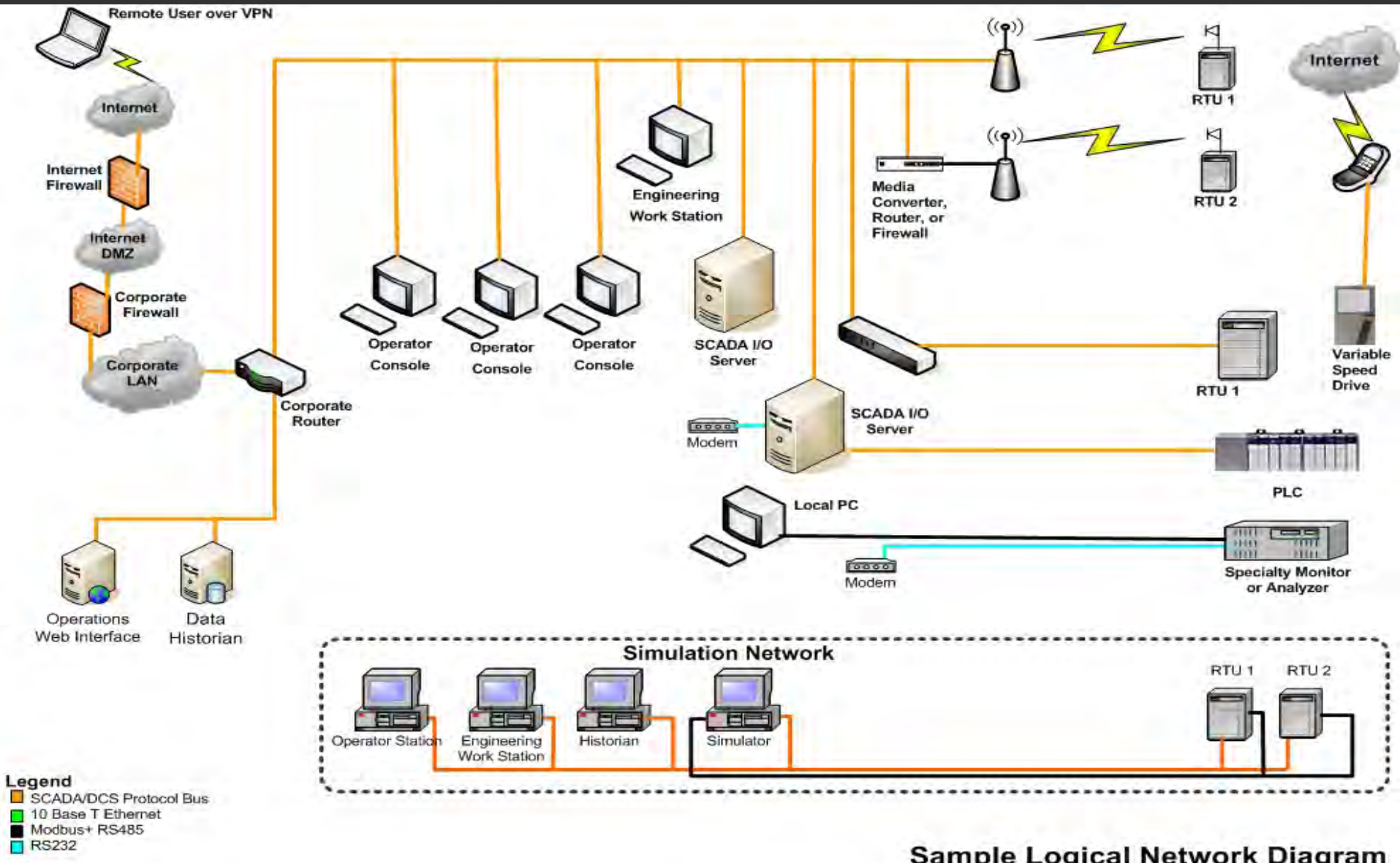
© 2005 PlantData Technologies

SCADA / DCS Applications

- SCADA applications running in Administrator Account session
- SCADA Systems broadcast their PC name
- Easy-to-Guess Hidden shares for tech support
- Remote Access to SCADA LAN not properly secured (VNC, pcAnywhere, etc…)
- Computers on SCADA LAN all share common account names and passwords
- Workstations / Servers running SCADA apps not properly patched
- No Antivirus or IDS deployed on SCADA LAN
- Access to Historical Databases Not Secured
- Critical Applications Not Monitored for Performance, and Critical Services Not Set to Auto-Restart

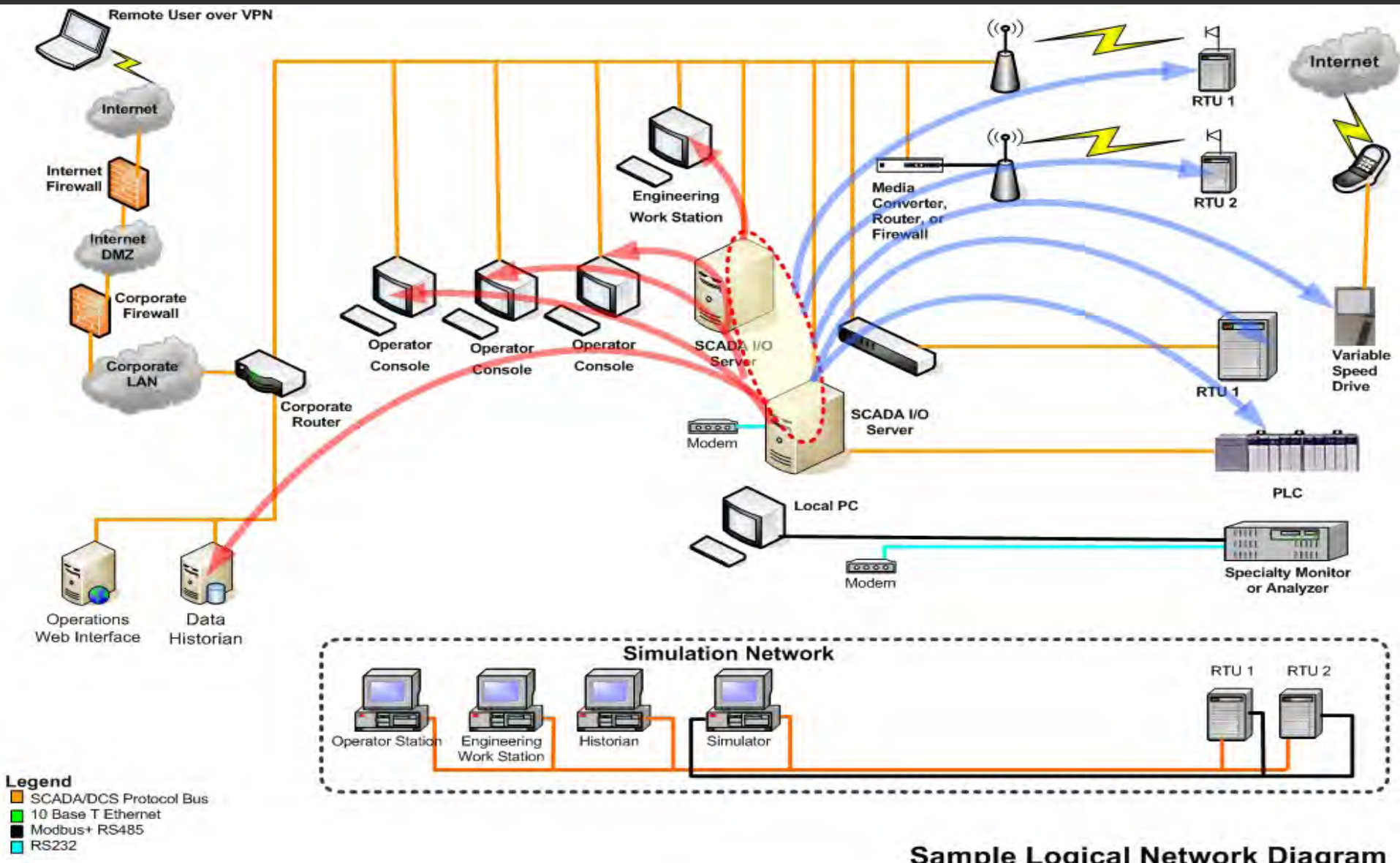
© 2005 PlantData Technologies

Typical SCADA/DCS Architecture



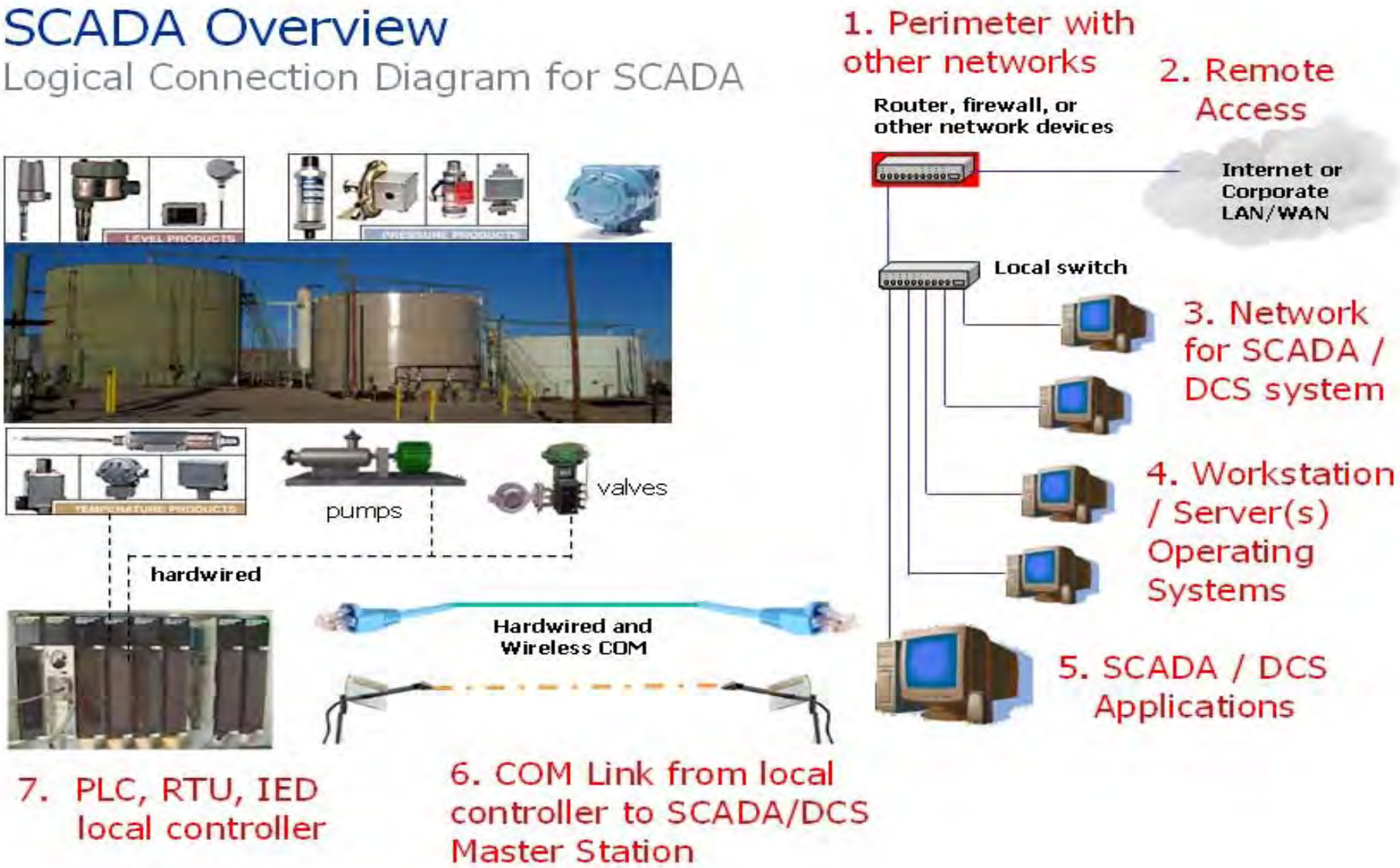
Sample Logical Network Diagram

Critical Communications Paths



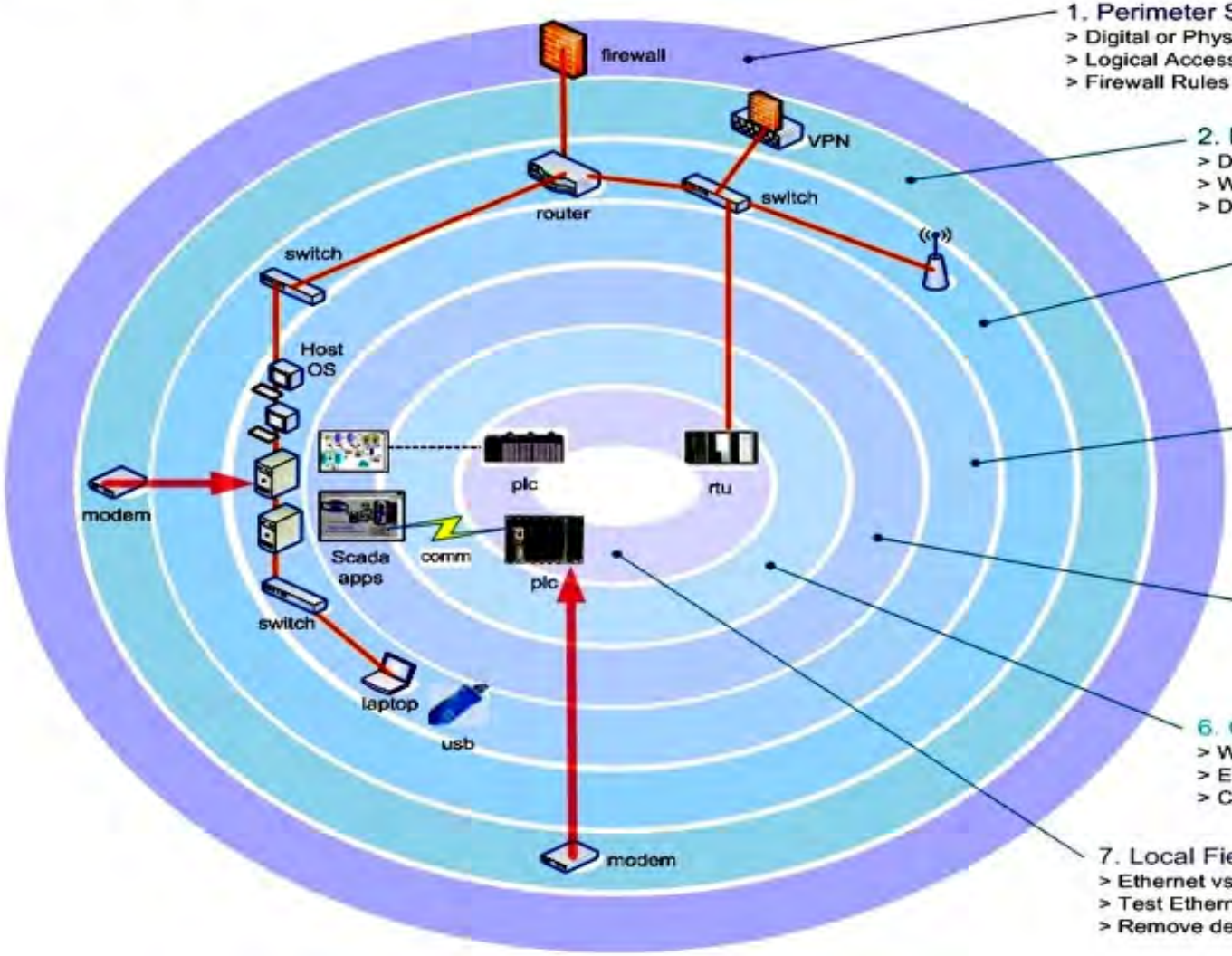
Sample Logical Network Diagram

SCADA System Functional Components



Each layer effects performance and security

Defense-in-Depth Approach
> Building Security into each SCADA System Component



1. Perimeter Security
> Digital or Physically Isolated
> Logical Access Controls
> Firewall Rules (map out open ports)

2. Remote and 3rd Party Access
> Document all remote access points
> War-dial for modems
> Document VPN or other Remote Access

3. Network Architecture
> Discover all network devices & hosts
> Conduct Protocol / Traffic Analysis
> Conduct Wireless Audit
> Analyze switch/router configurations

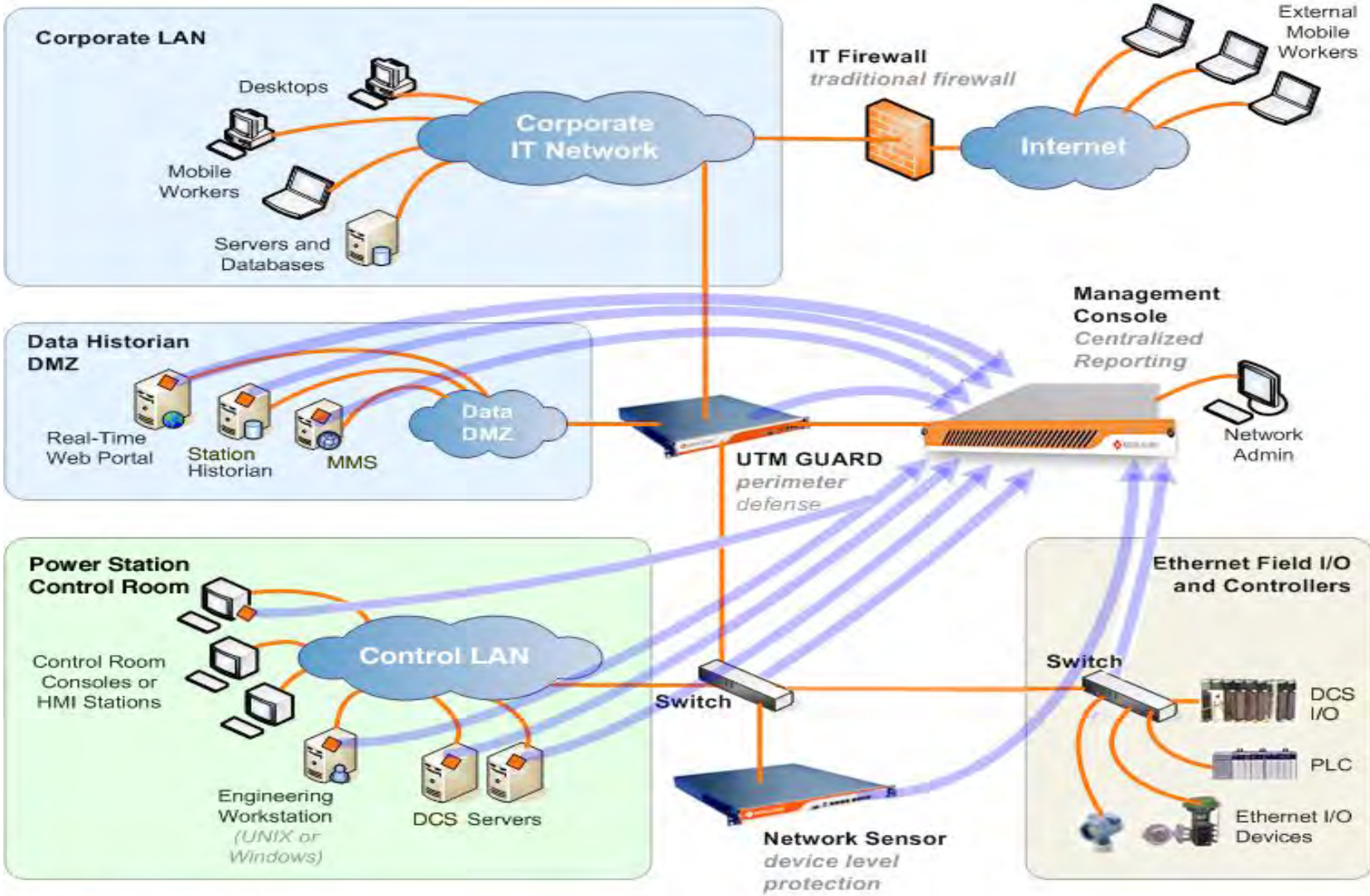
4. Host OS & Removable Devices
> Check OS for vulnerabilities
> OS Patch Management
> Prevent USB or Removable Devices from use inside Control Room
> Restrict foreign laptops from connecting

5. SCADA Applications
> Monitor network for clear text transfer
> Ensure use of individual accounts
> Test for access to desktop

6. Communications to Field Devices
> Wired vs. Wireless Communications
> Ethernet vs. Serial Communications
> Capture Traffic on Ethernet connections

7. Local Field Controllers
> Ethernet vs. Serial connected devices
> Test Ethernet devices in lab for vulnerabilities
> Remove default vendor passwords

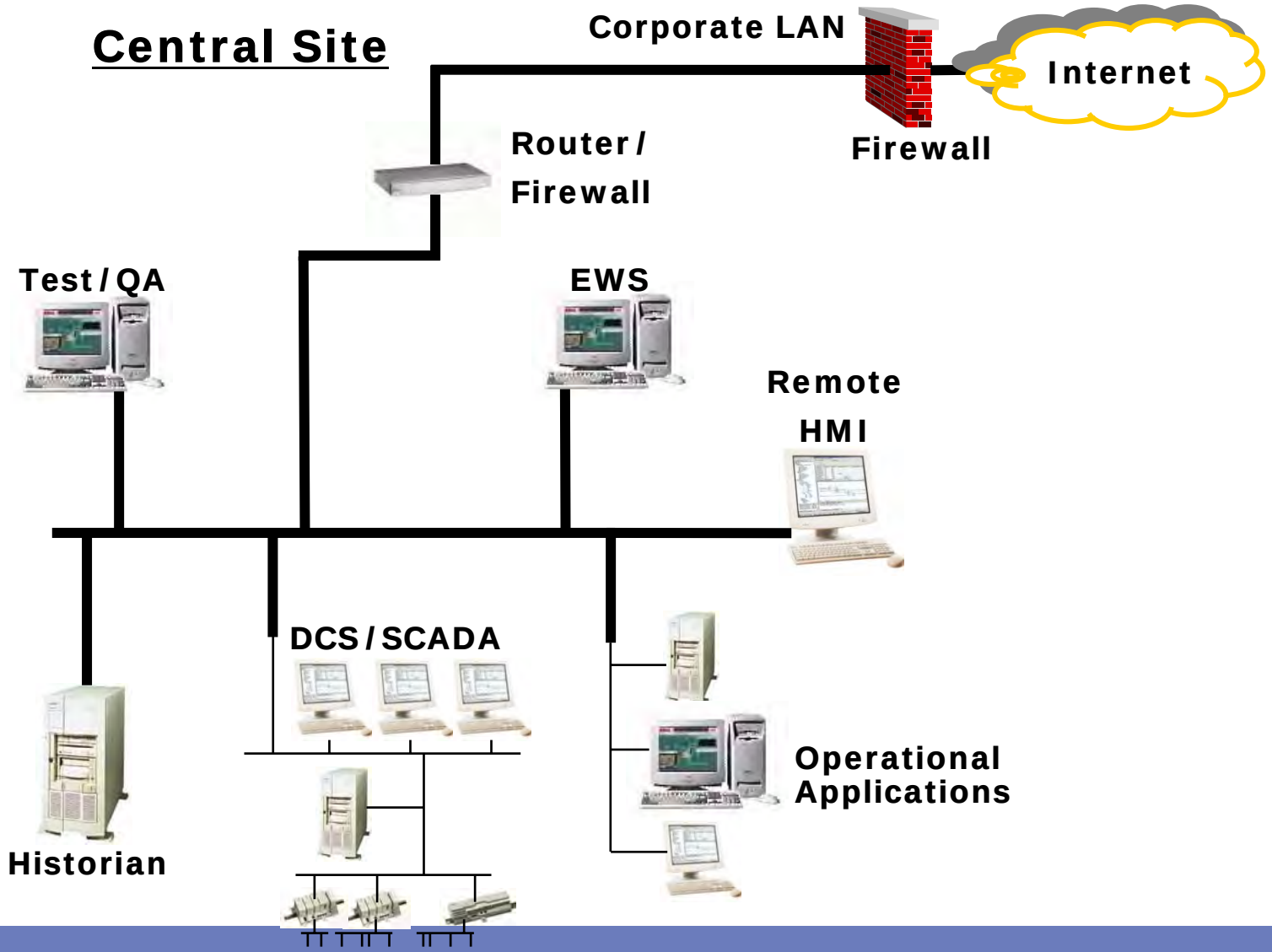
A Centrally Managed Comprehensive Solution is Ideal



Ethernet TCP/IP
Alert / Log Collection & Device Management
Host-based Agents Reporting Statistics & Logs

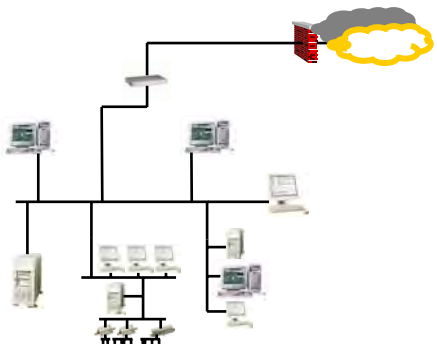
plantdata technologies

Typical Control System - Central Site

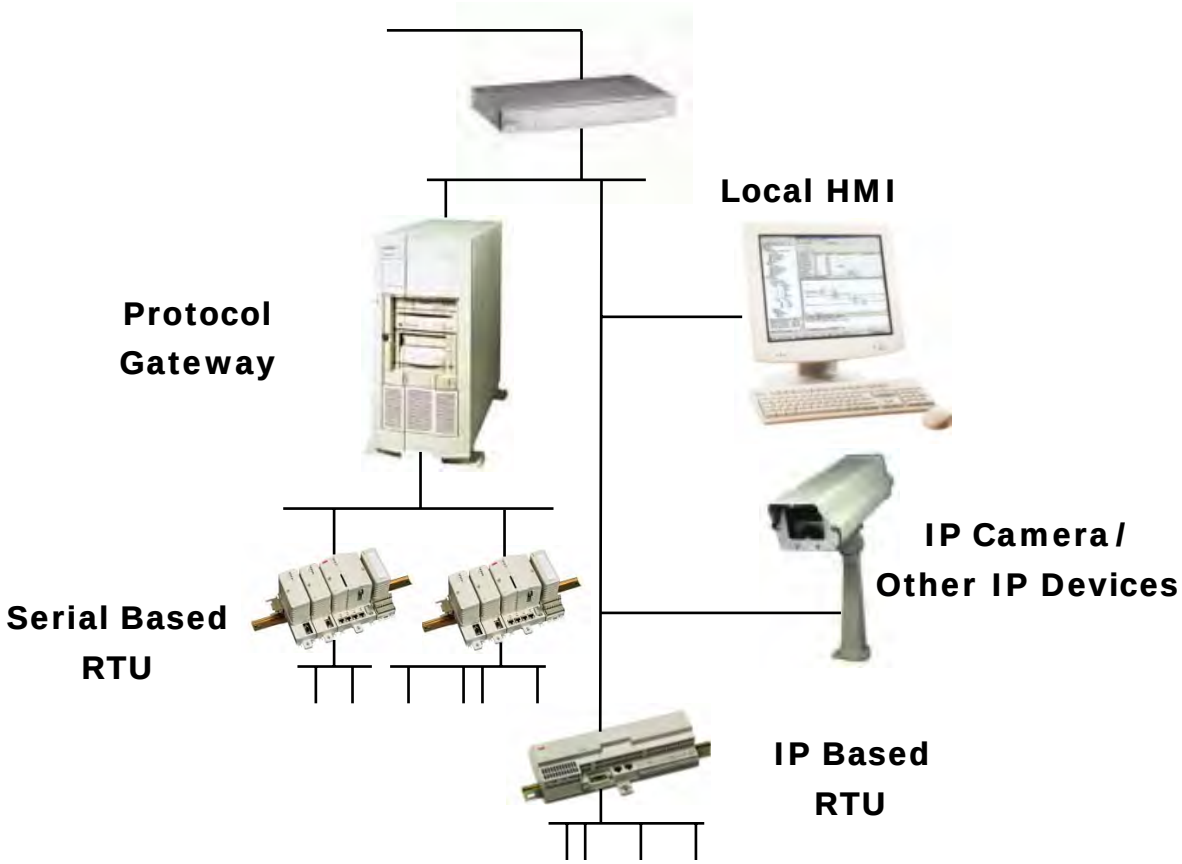


Typical Control System - Remote Site

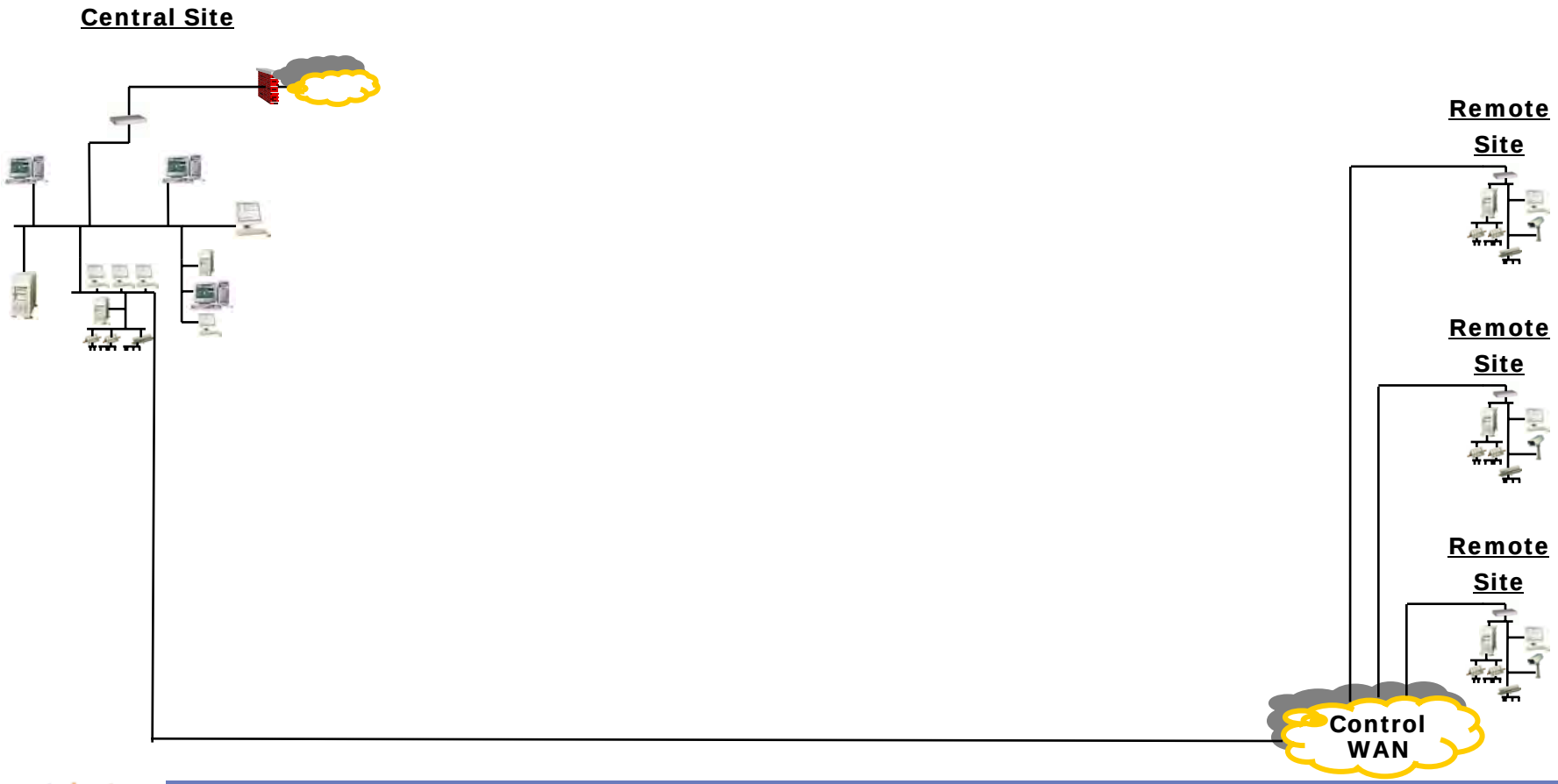
Central Site



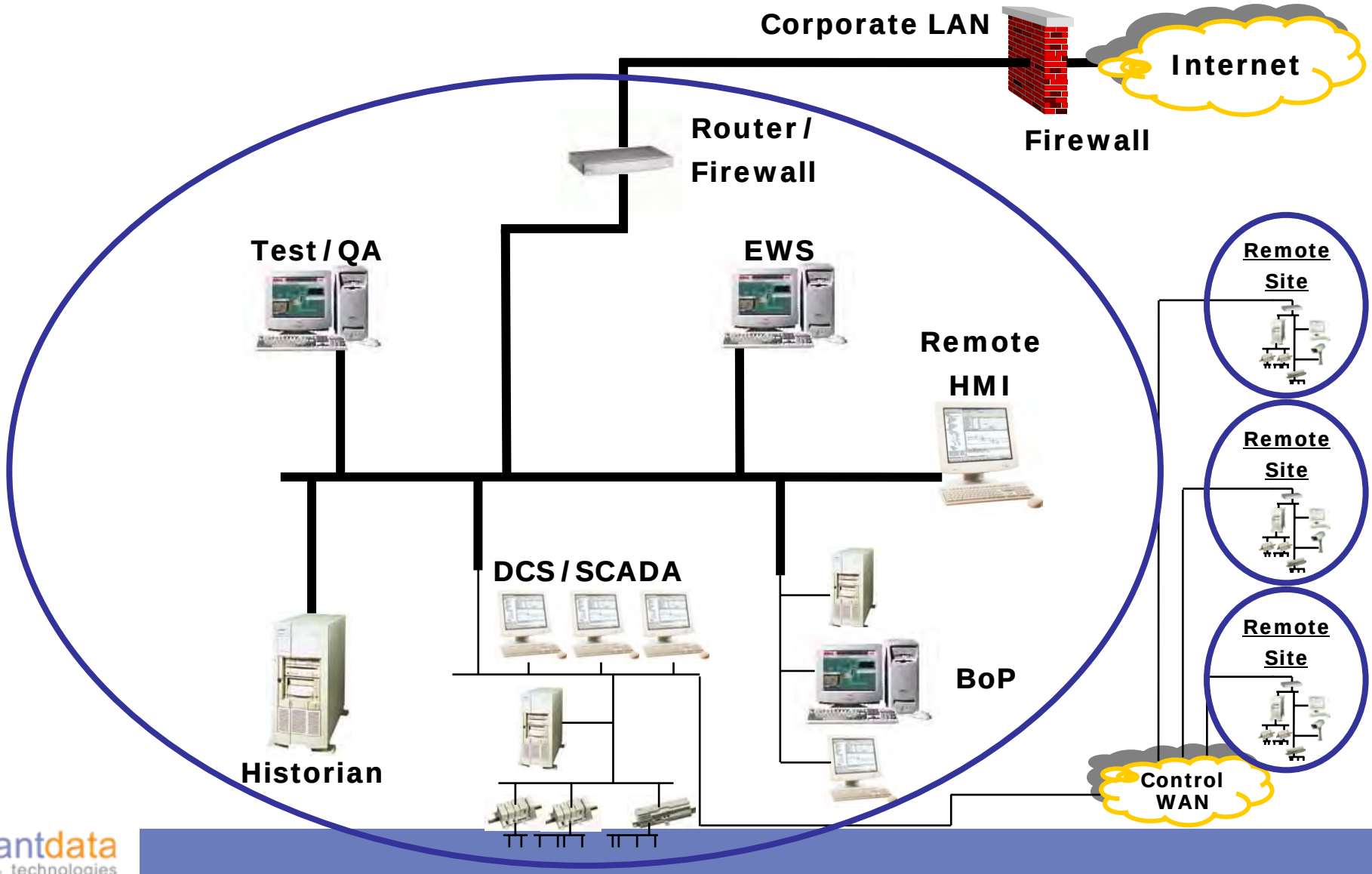
Remote Site



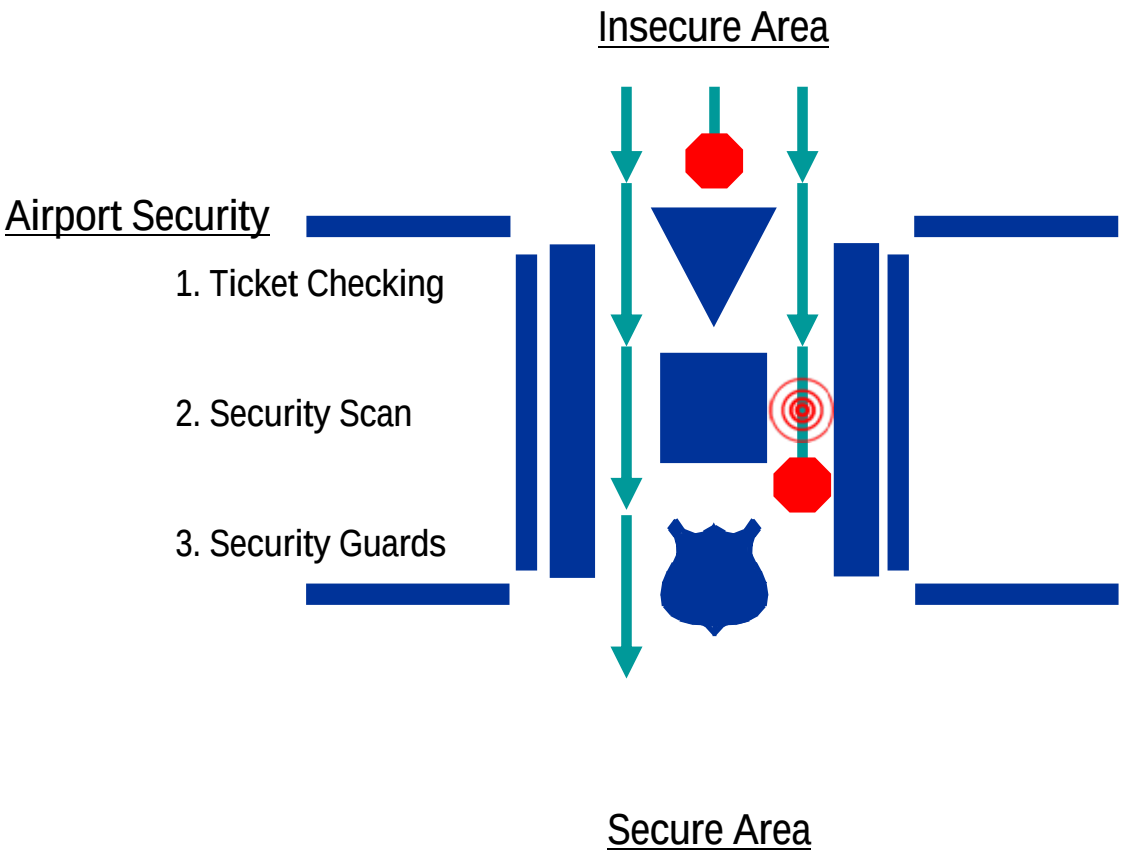
Typical Control System - Multiple Remote Sites



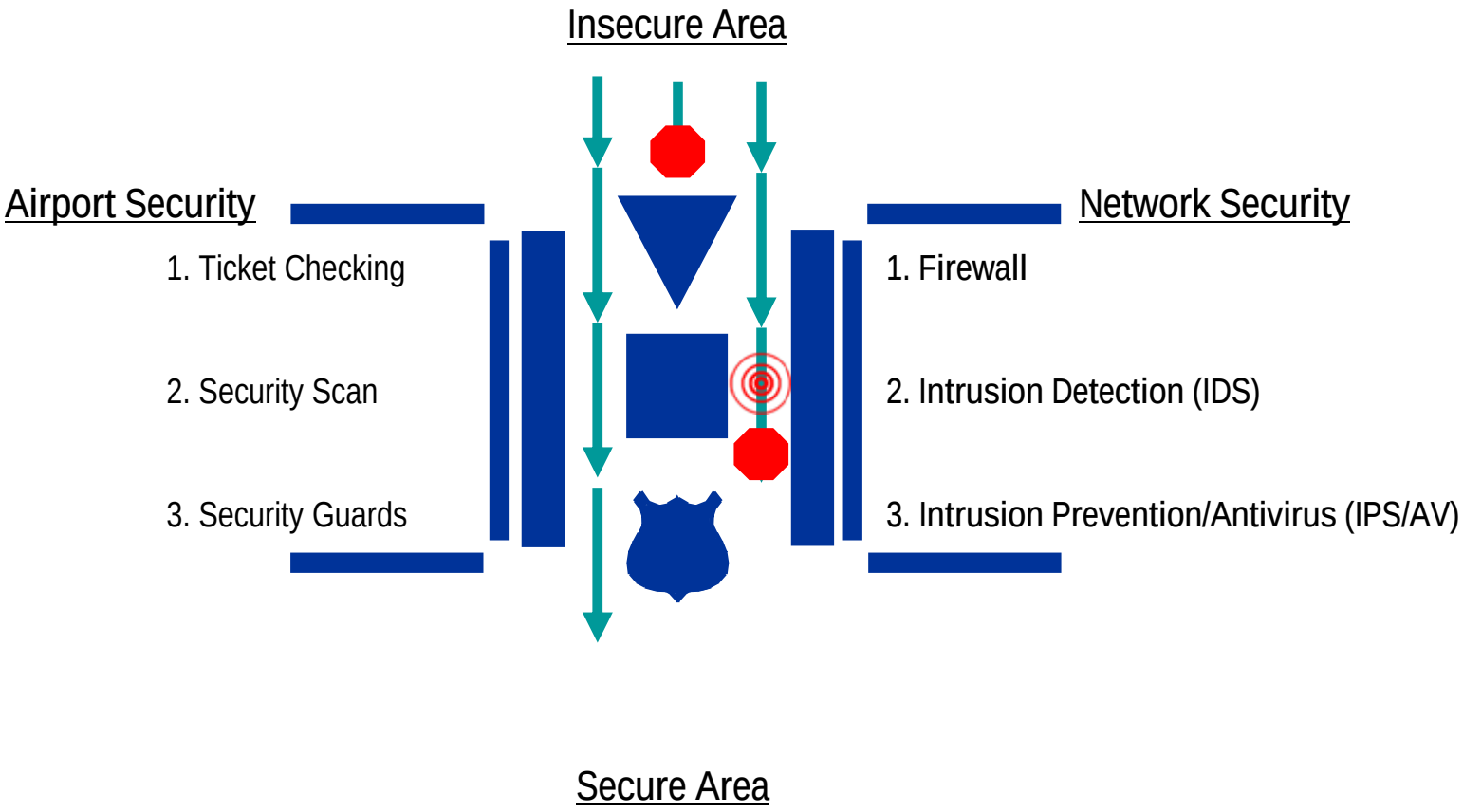
Perimeter Protection is the First Line of Defense



Controlling the Perimeter

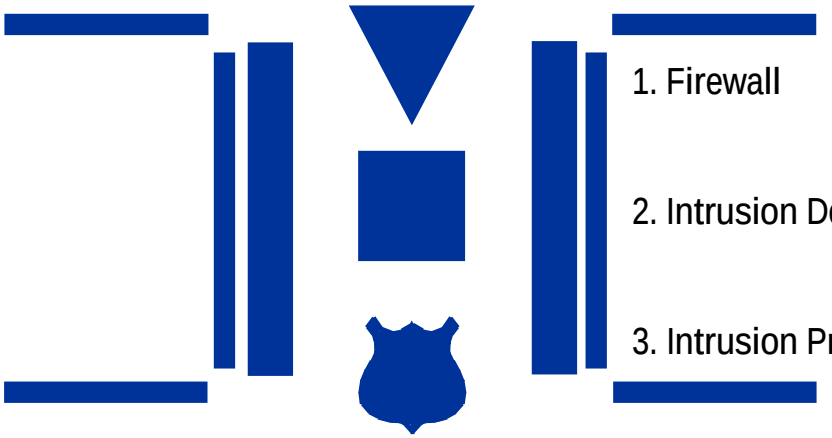


Controlling the Perimeter



Controlling the Perimeter

Insecure Area



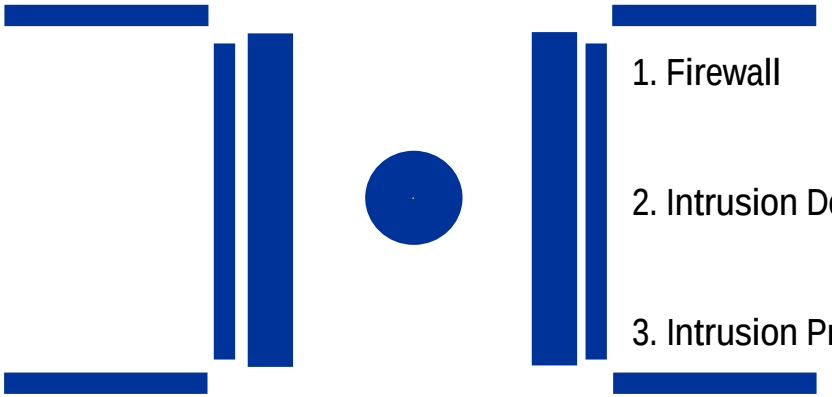
Network Security

1. Firewall
2. Intrusion Detection (IDS)
3. Intrusion Prevention/Antivirus (IPS/AV)

Secure Area

Controlling the Perimeter - UTM, the new Firewall

Insecure Area

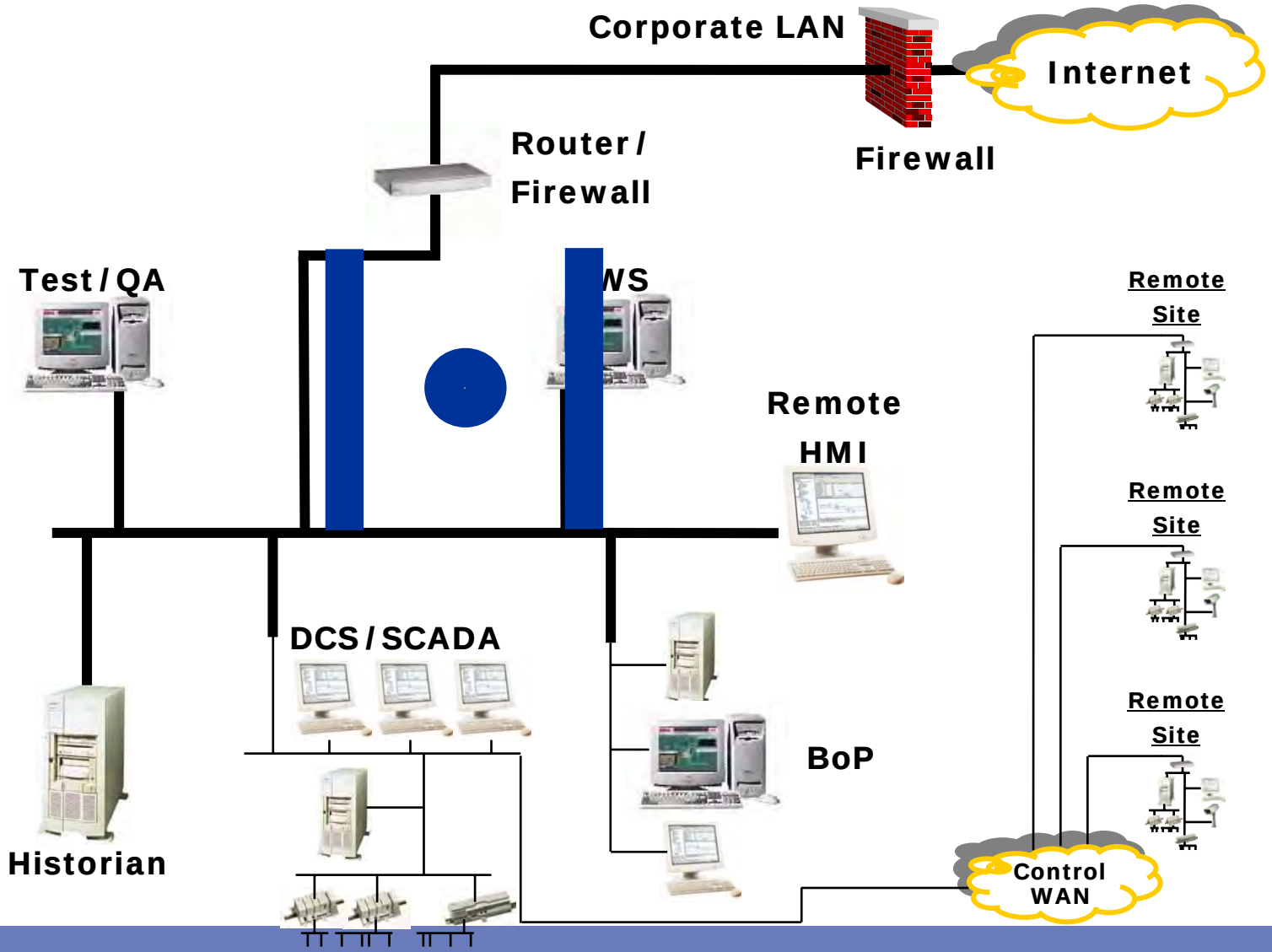


Network Security

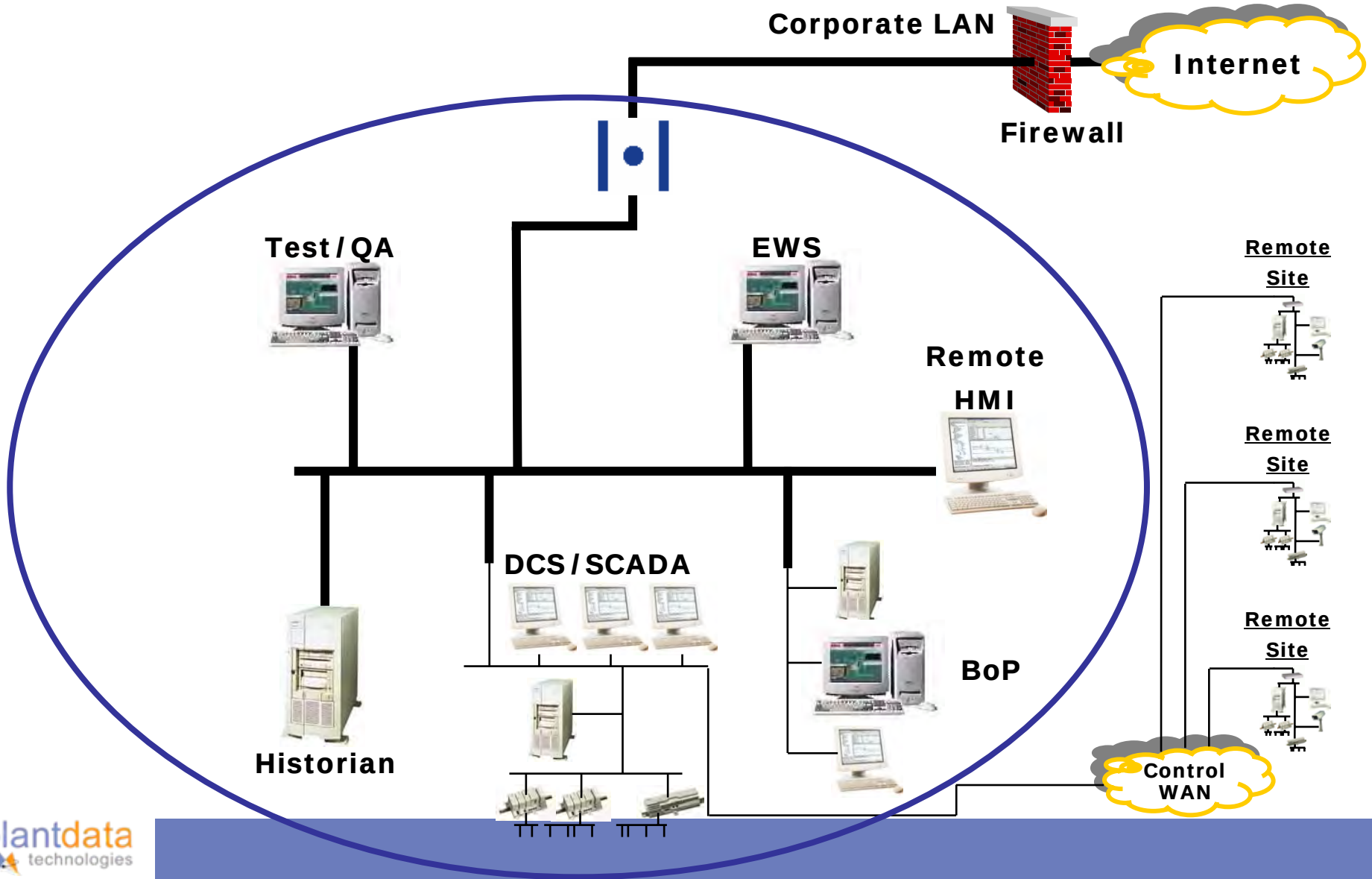
1. Firewall
2. Intrusion Detection (IDS)
3. Intrusion Prevention/Antivirus (IPS/AV)

Secure Area

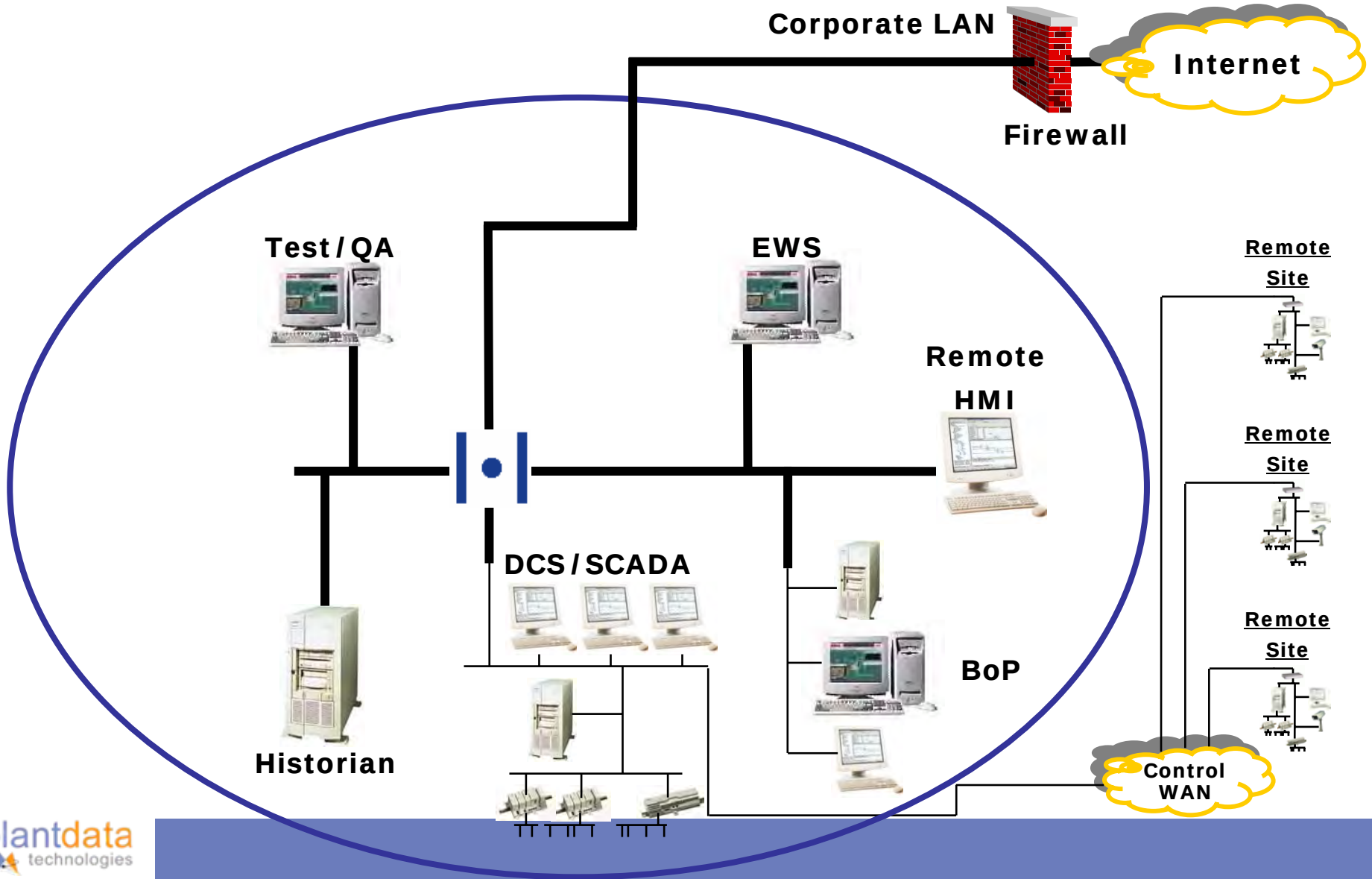
Typical Control System



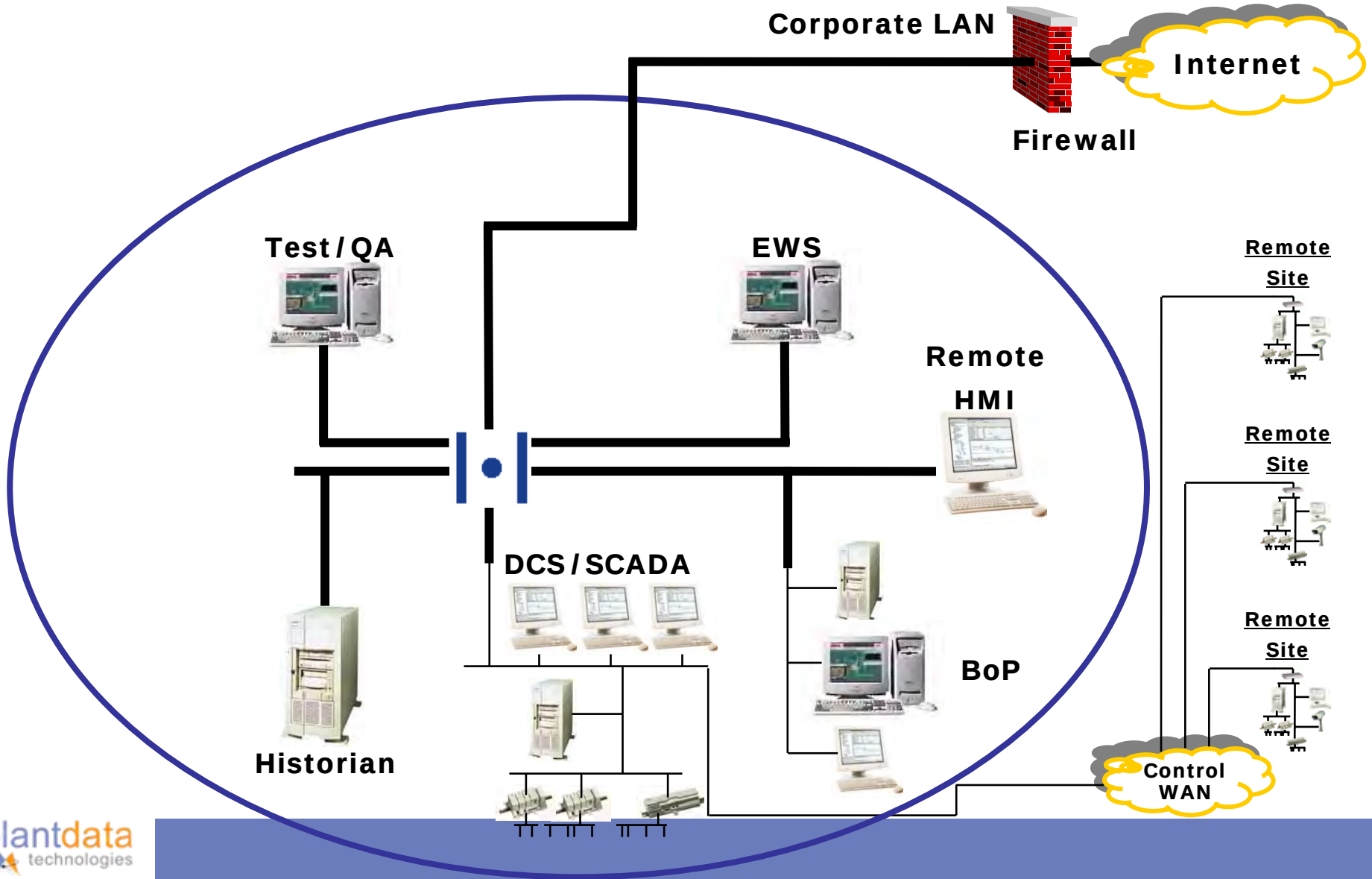
Perimeter Protection



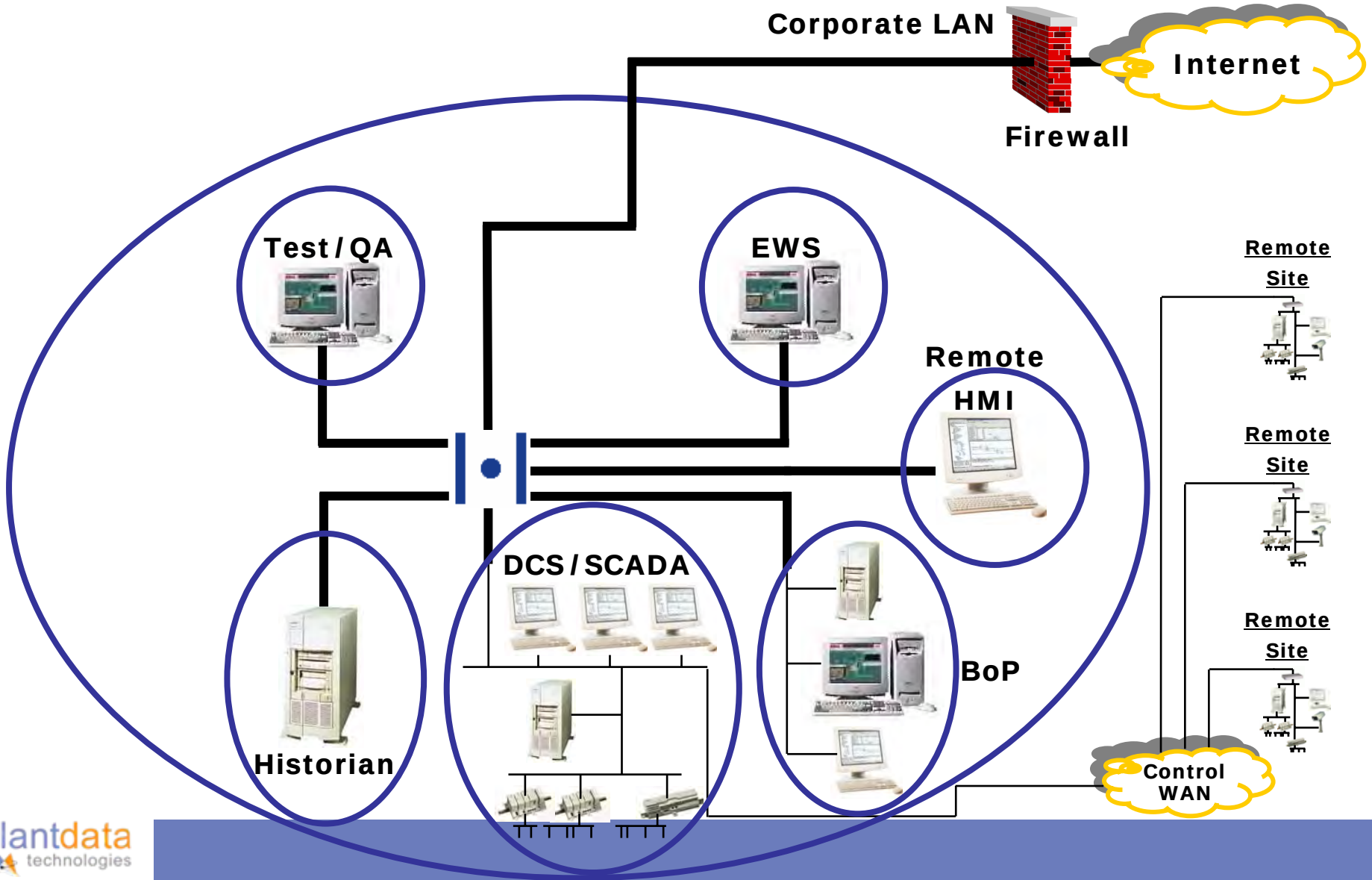
Subsystem Perimeter Protection



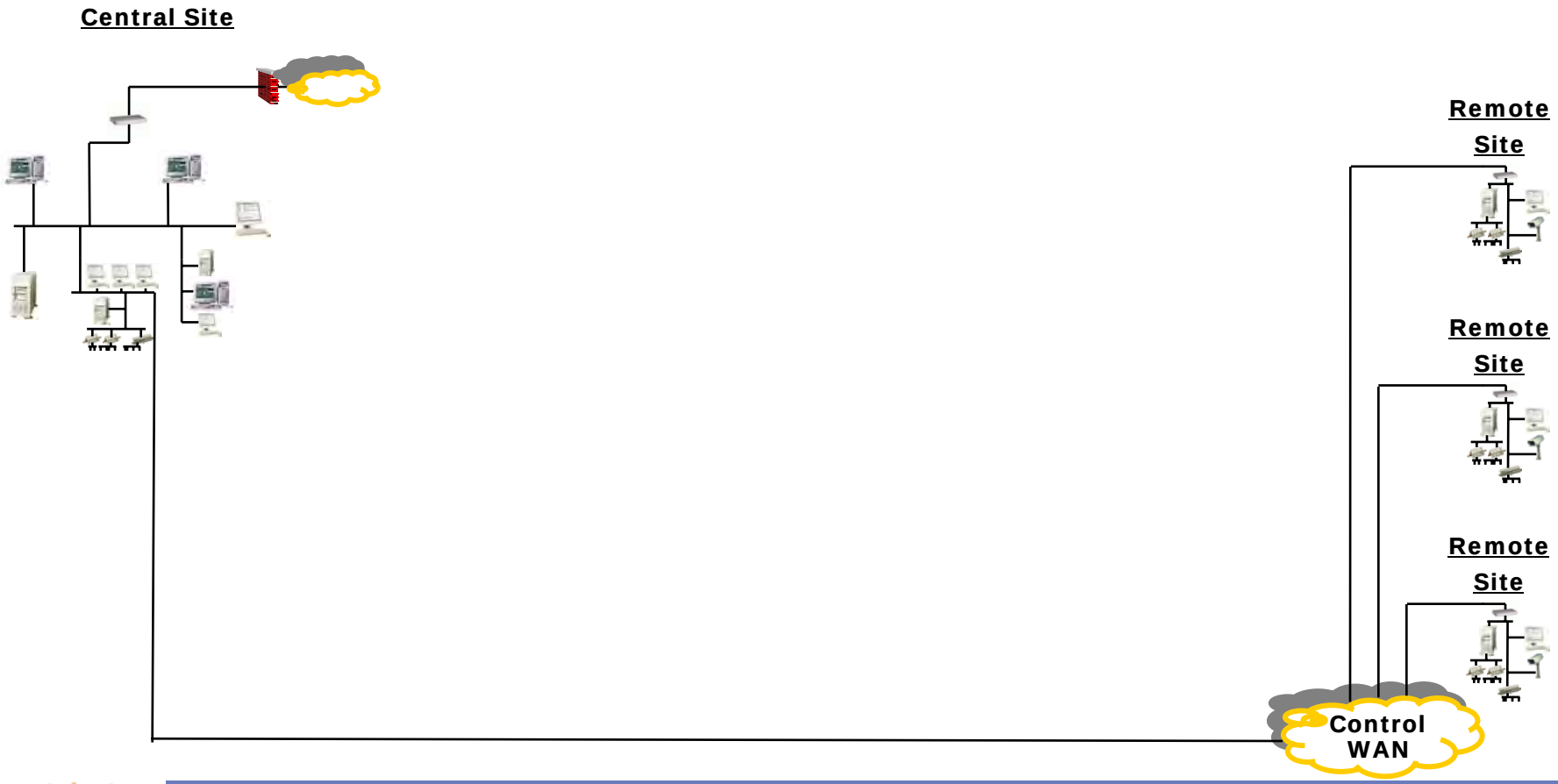
Subsystem Perimeter Protection



Subsystem Perimeter Protection

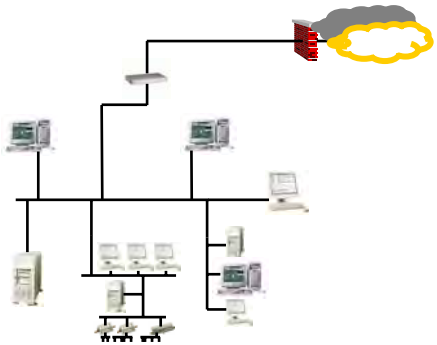


Subsystem Perimeter Protection

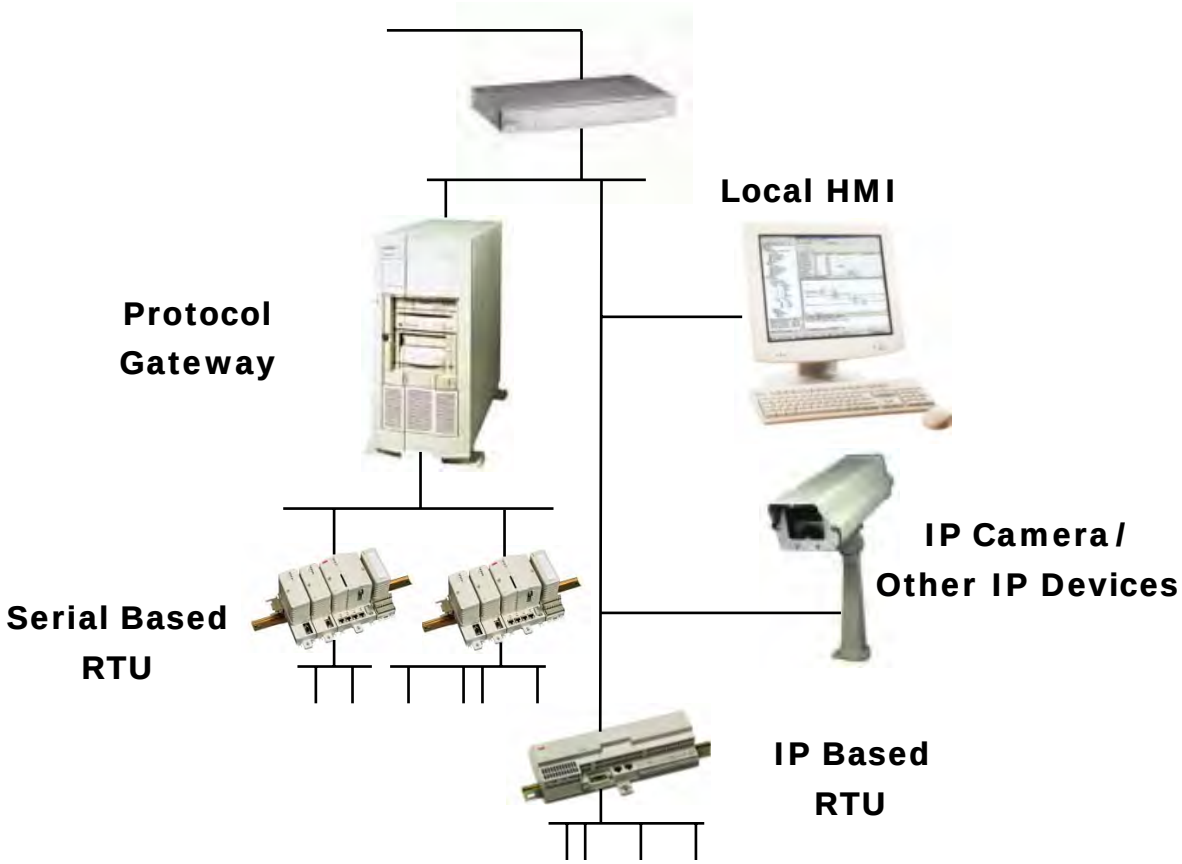


Subsystem Perimeter Protection - Remote Sites

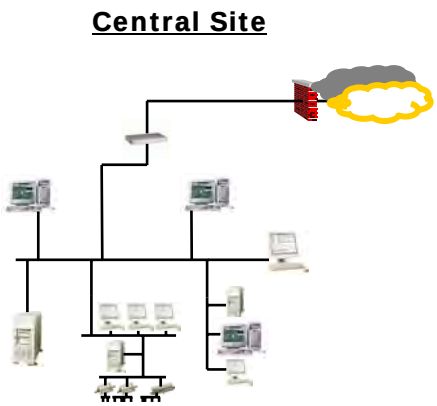
Central Site

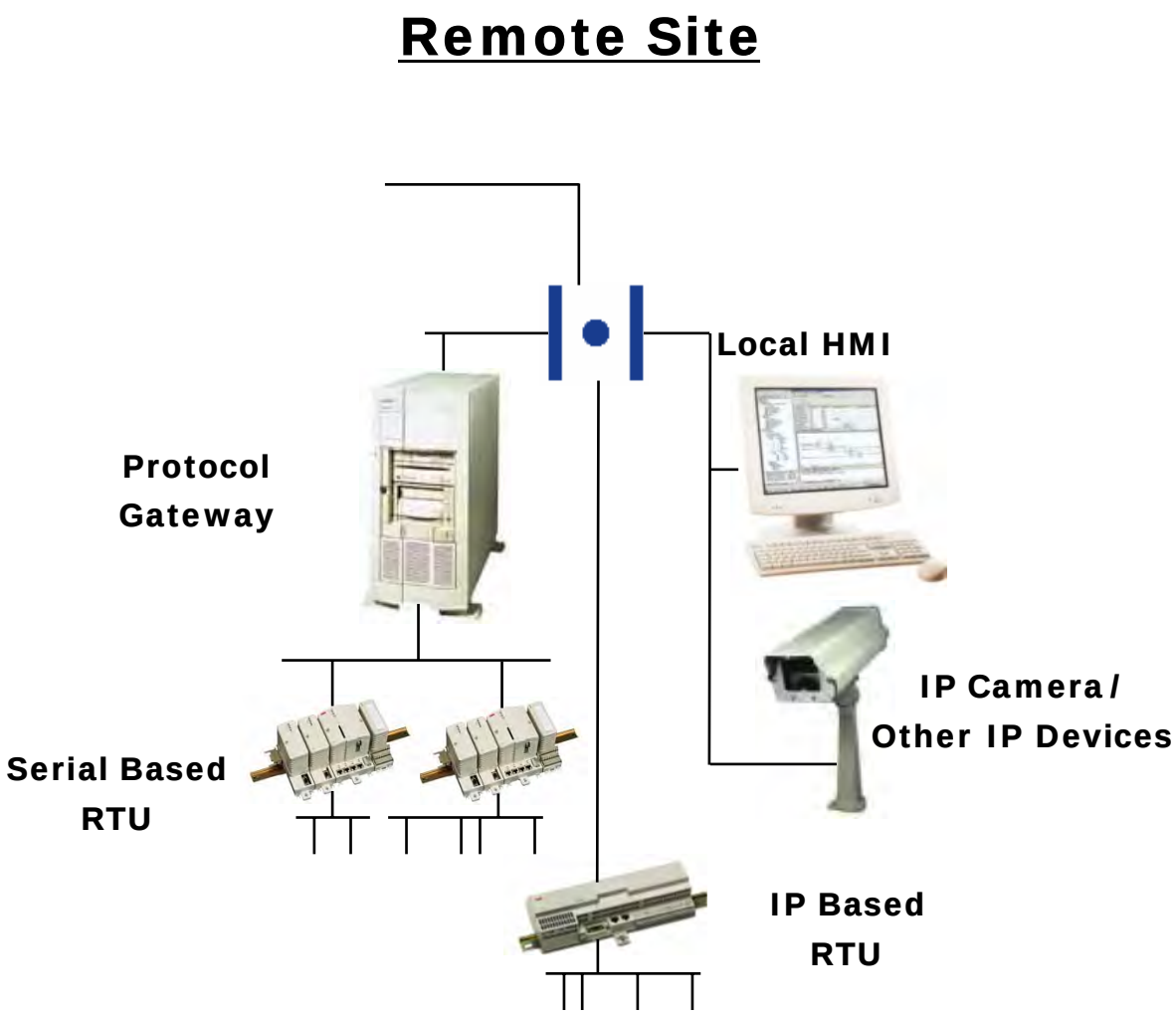


Remote Site

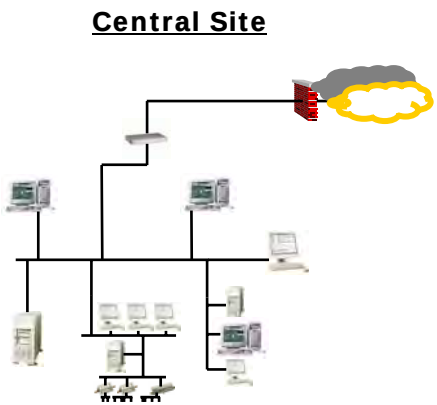


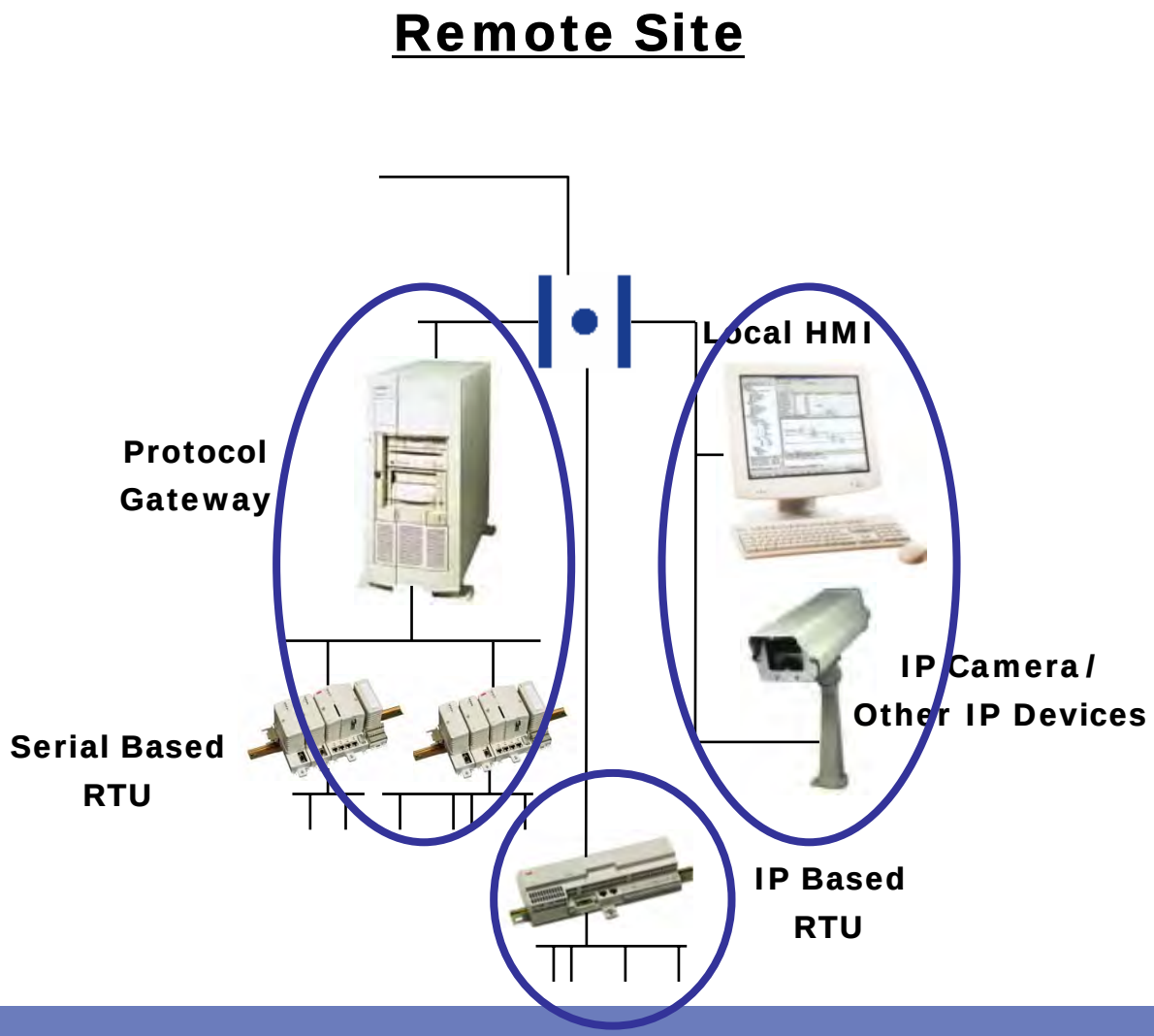
Subsystem Perimeter Protection - Remote Sites



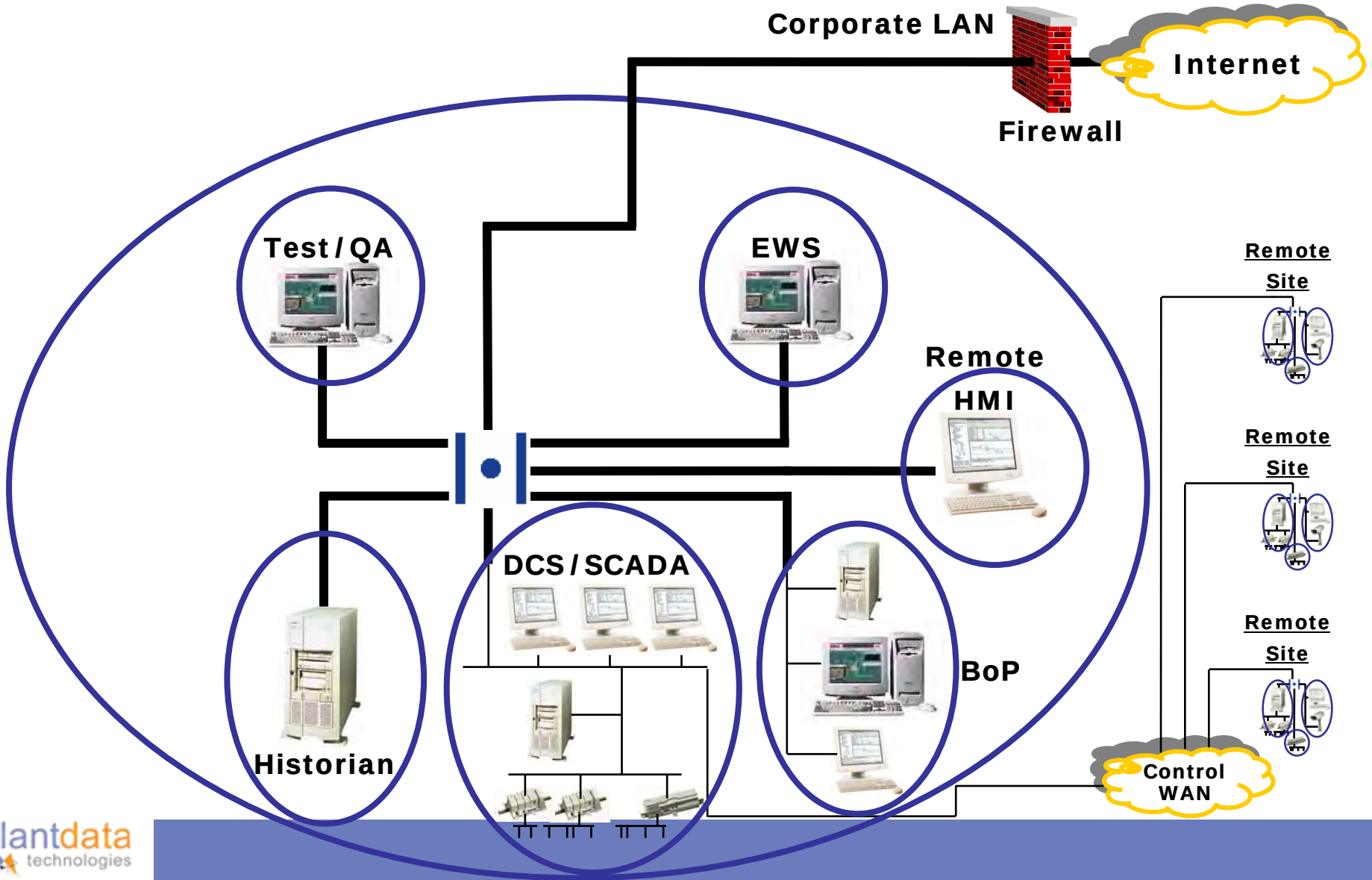


Subsystem Perimeter Protection - Remote Sites

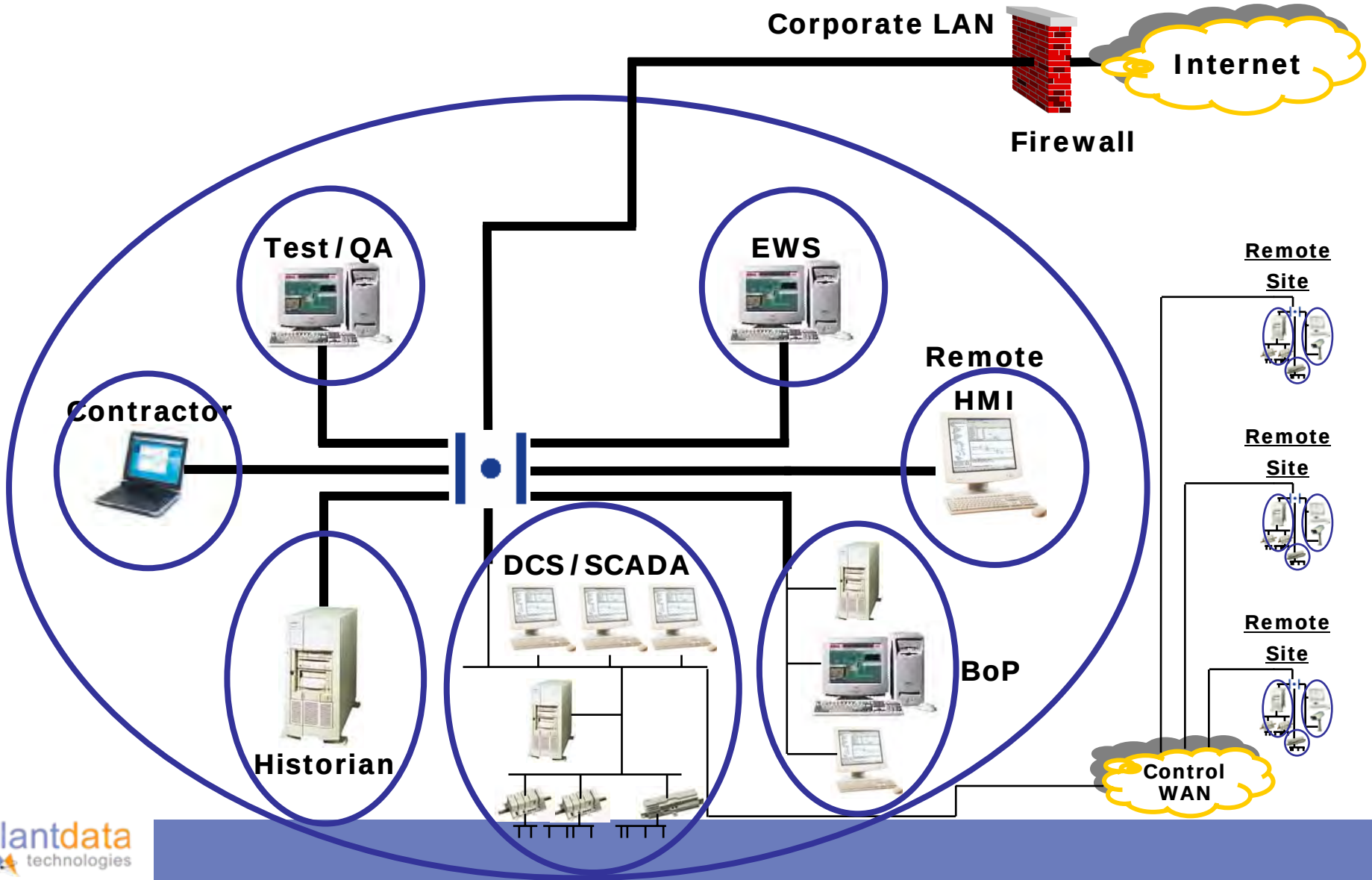




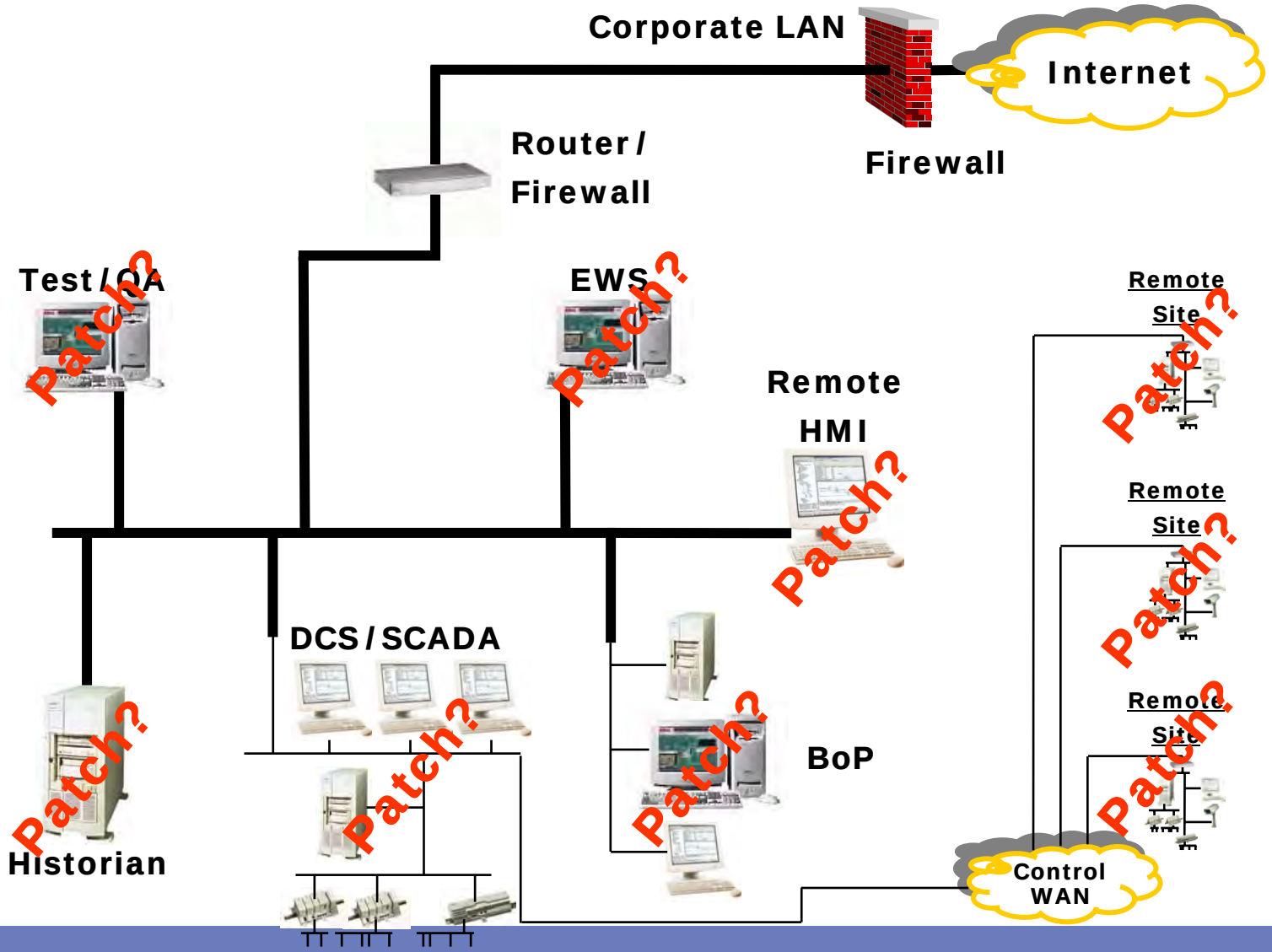
Subsystem Perimeter Protection



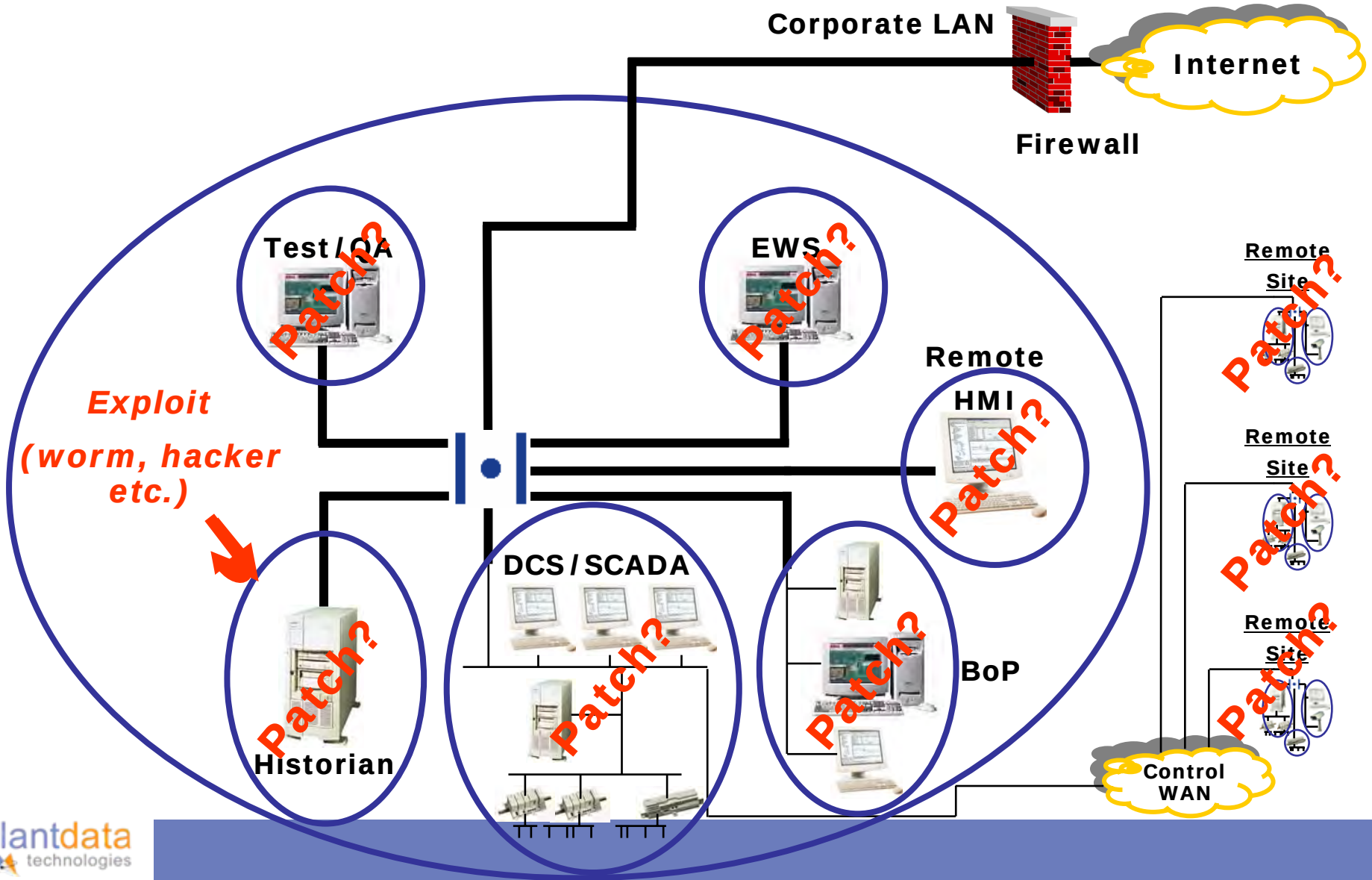
Subsystem Perimeter Protection - Contractor Containment



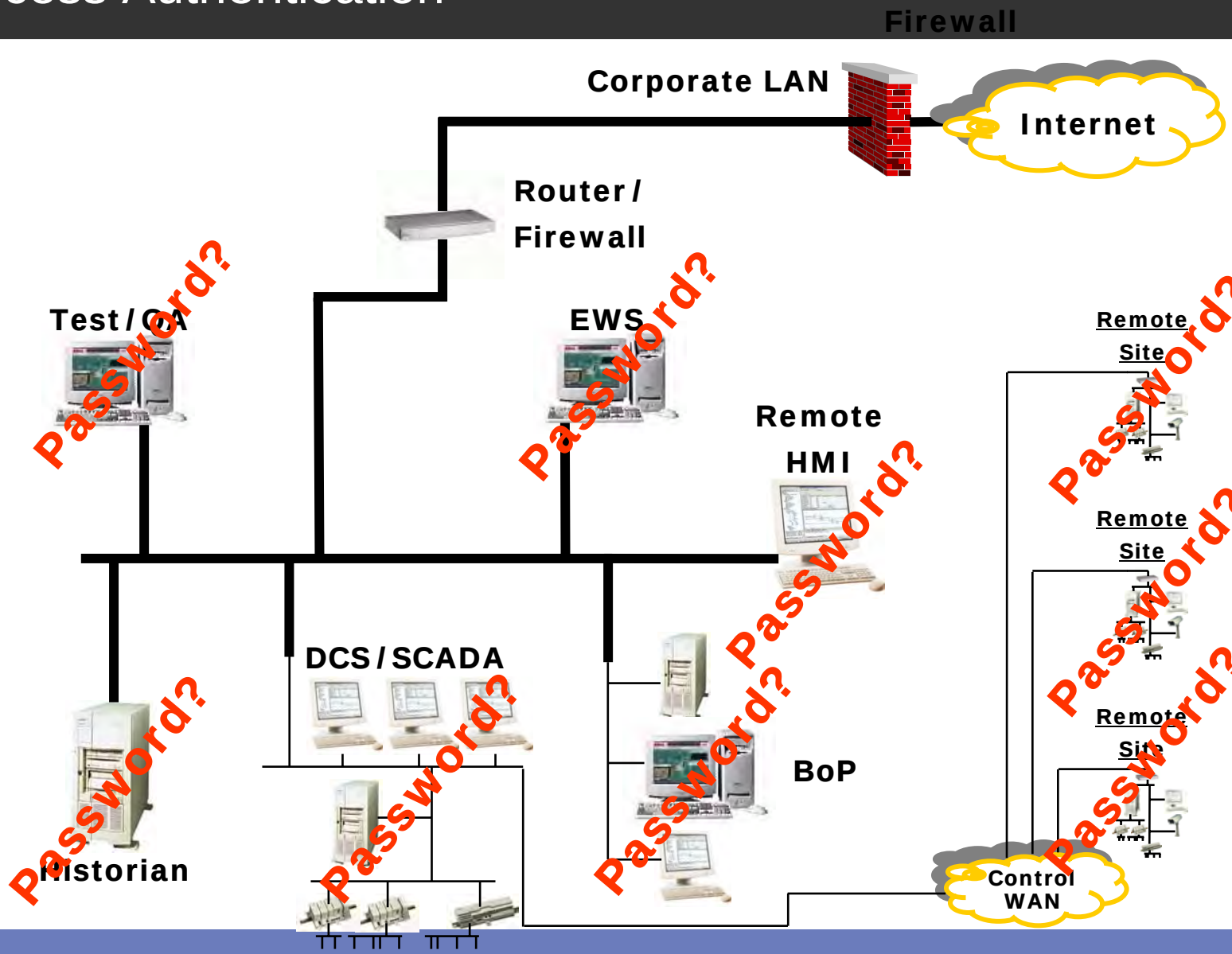
Patching Process Control Systems



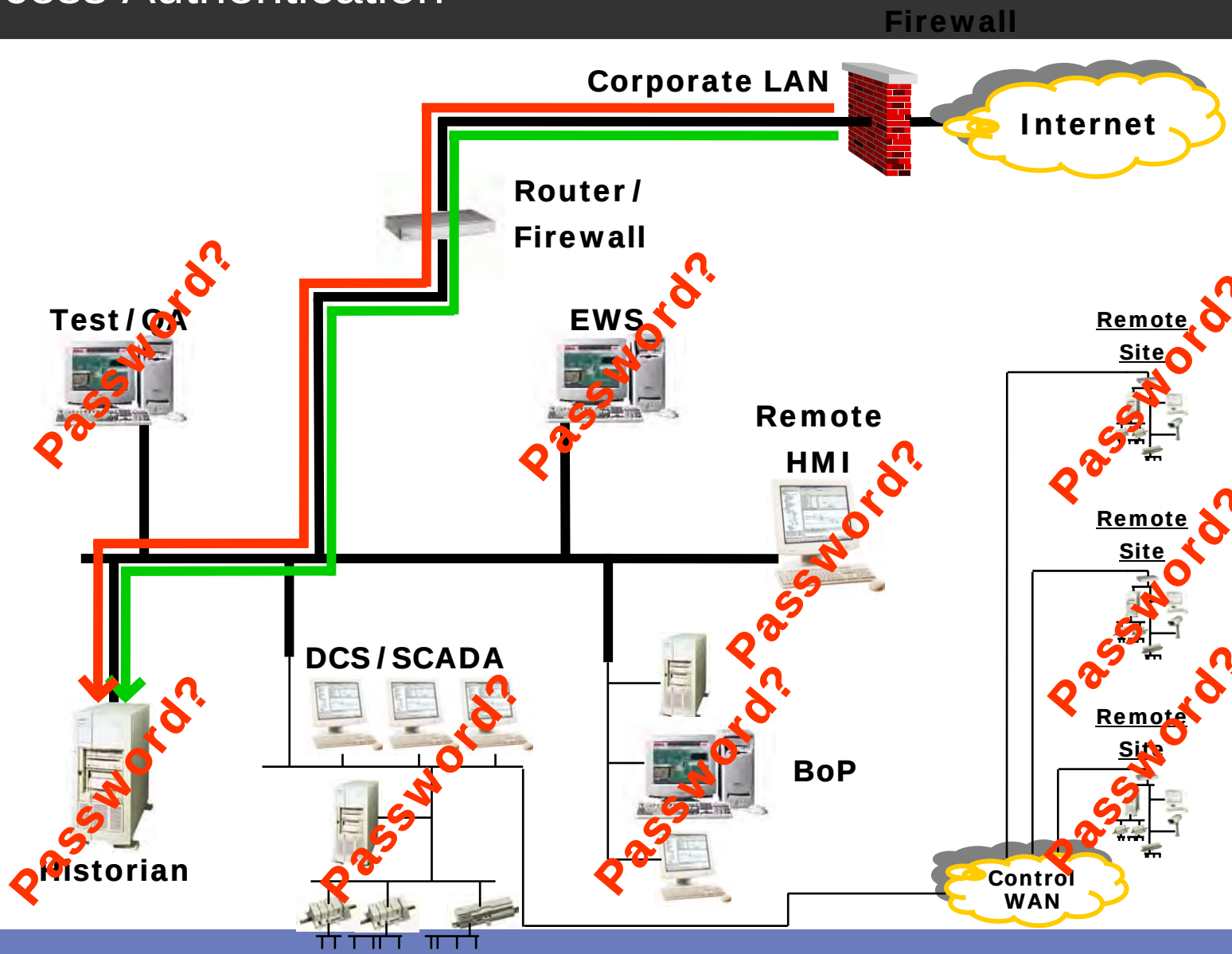
Leveraging Subsystem Protection for Virtual Patching



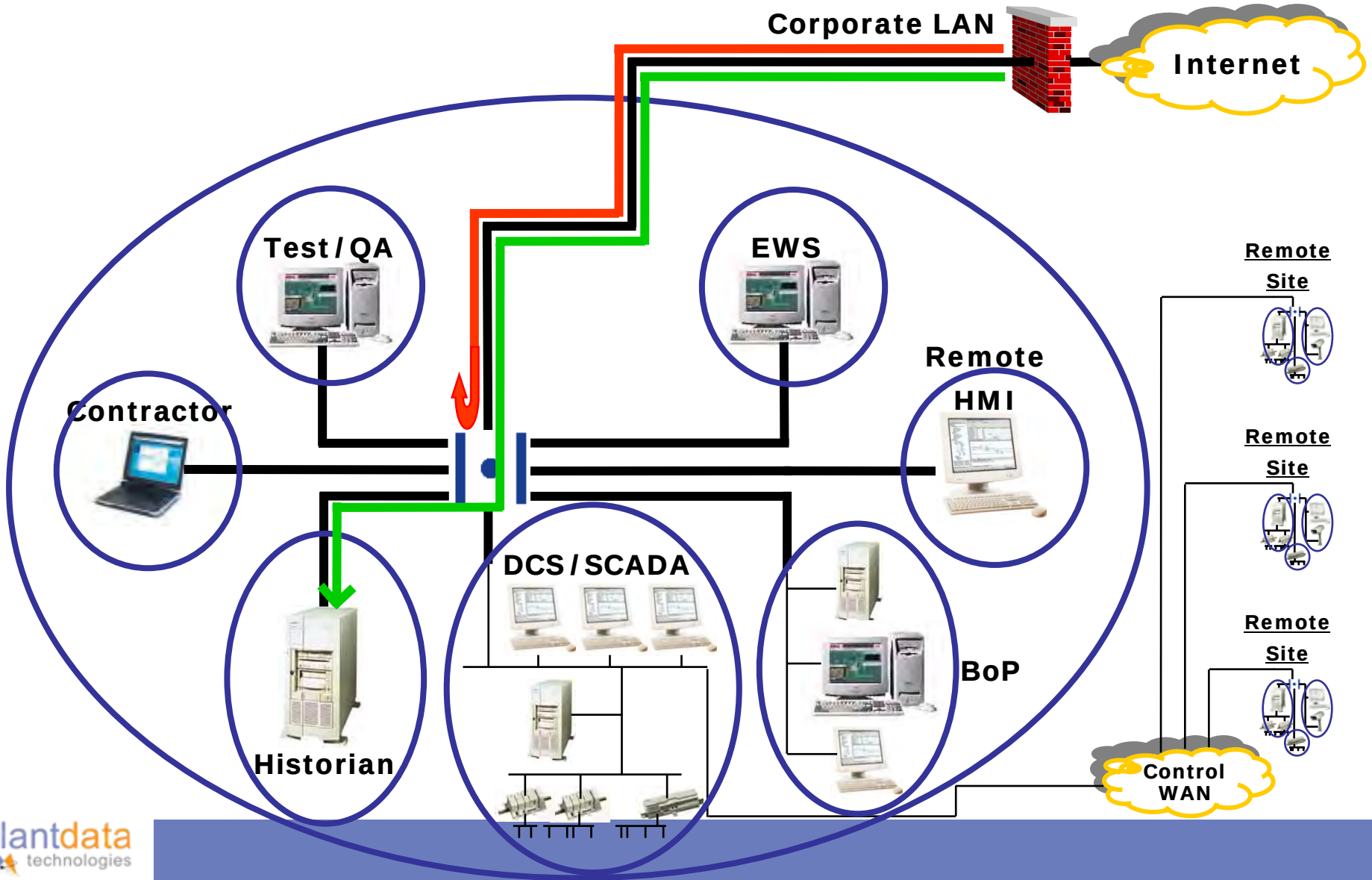
Remote Access Authentication



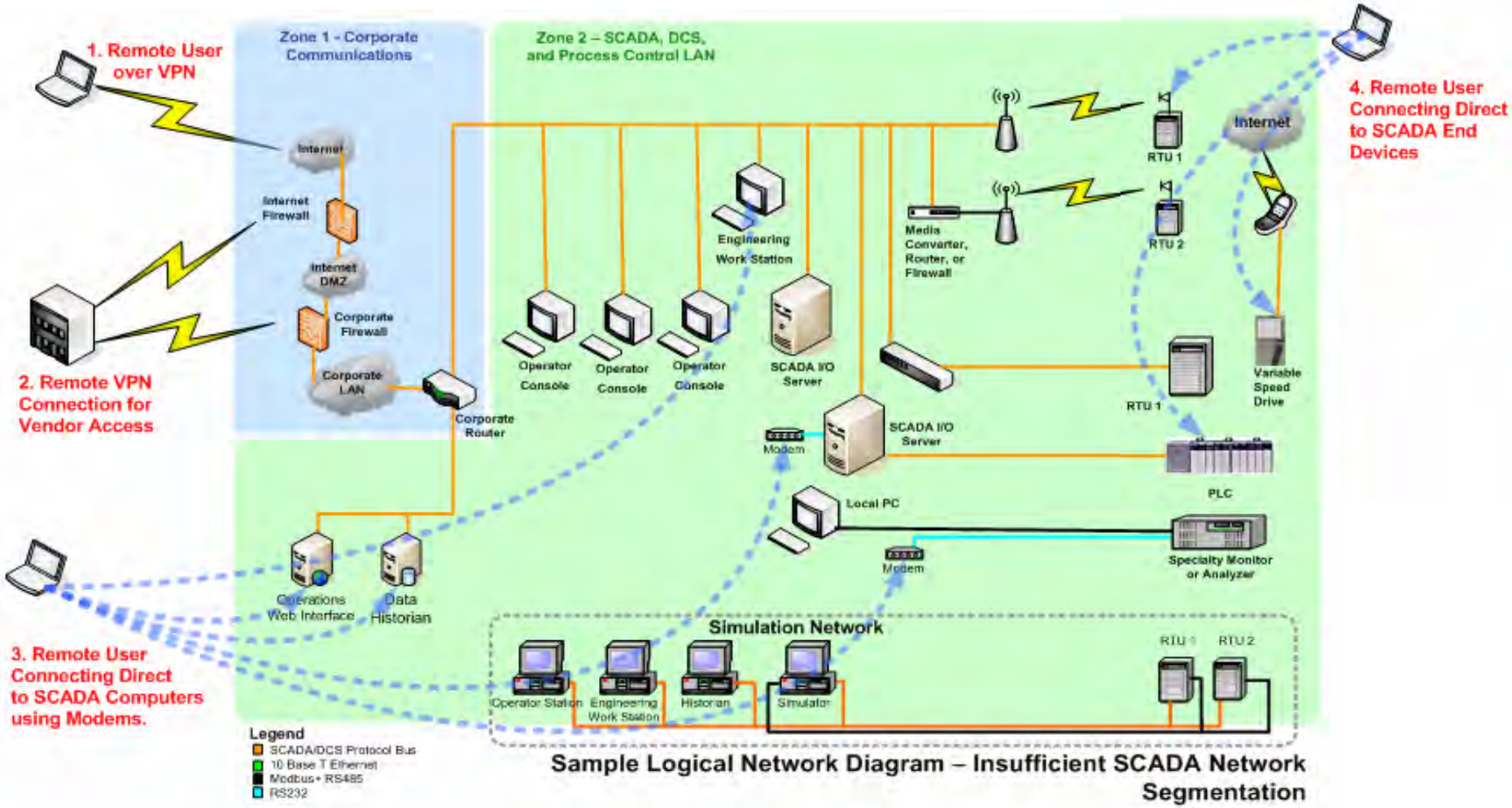
Remote Access Authentication



Remote Access Authentication



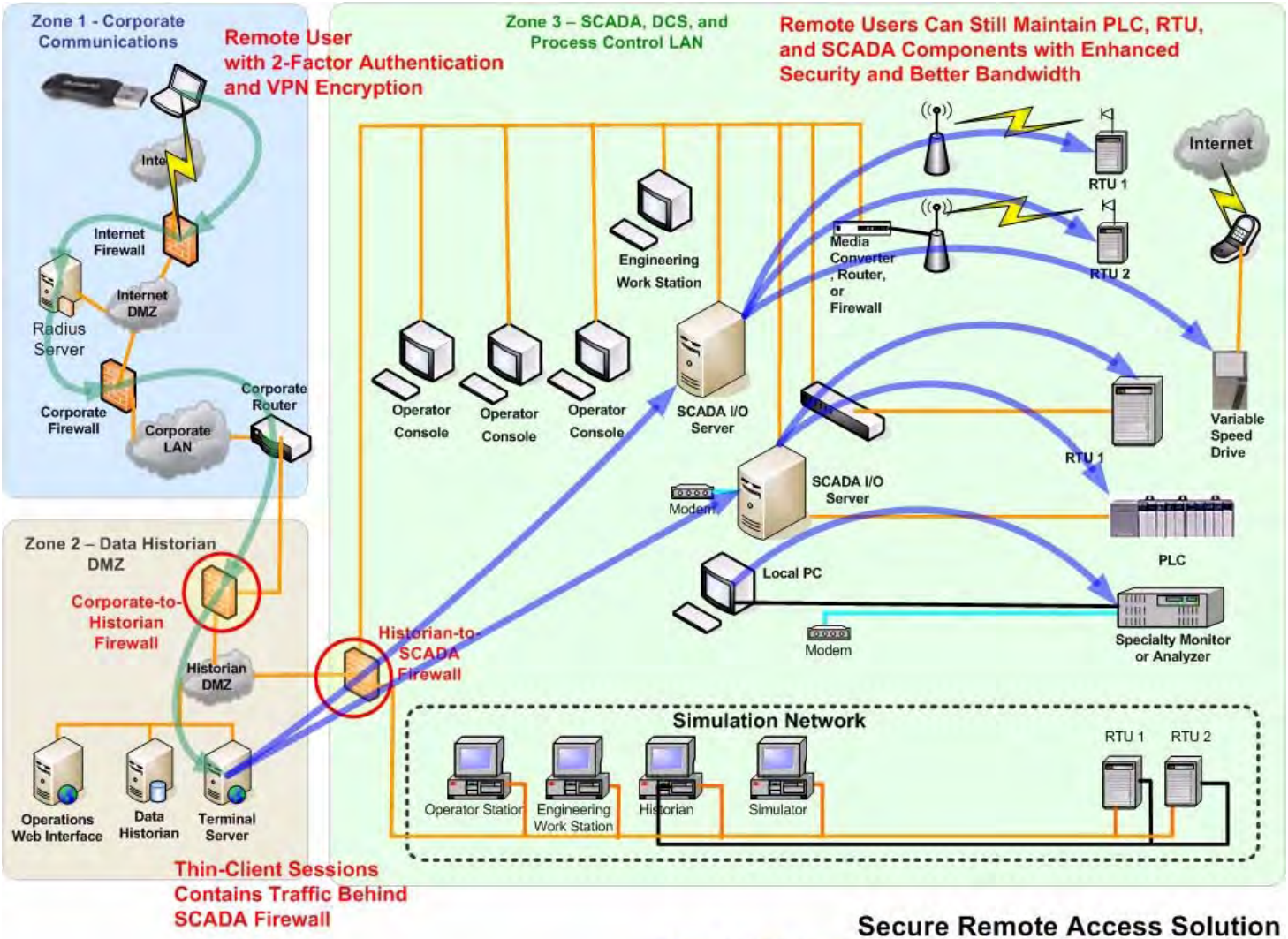
Insecure Access – Sample Insecure Remote Connections



Sample Logical Network Diagram – Insufficient SCADA Network Segmentation

© 2005 PlantData Technologies

Consider 2-Factor Authentication for Remote Access

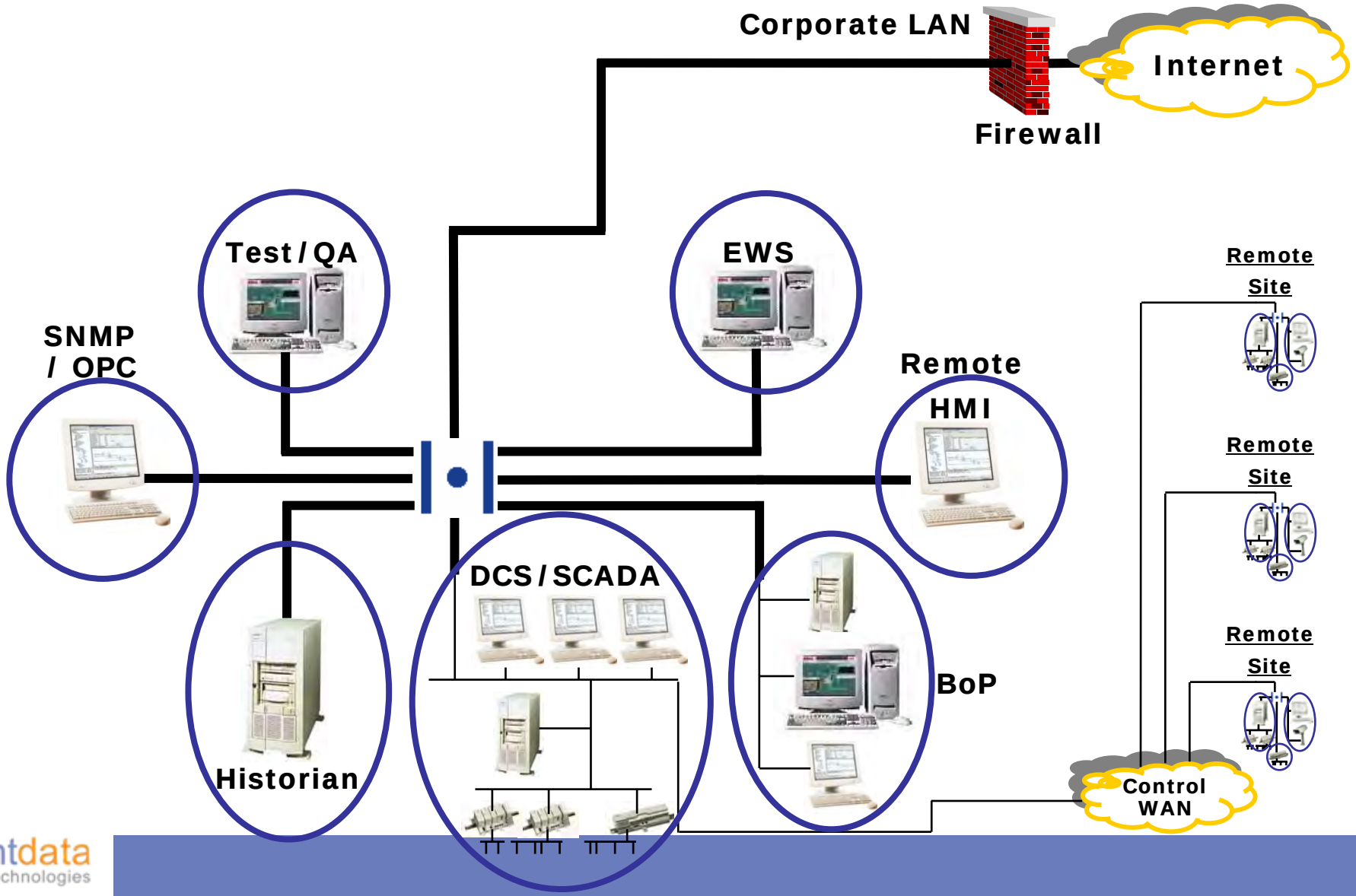


Secure Remote Access Solution

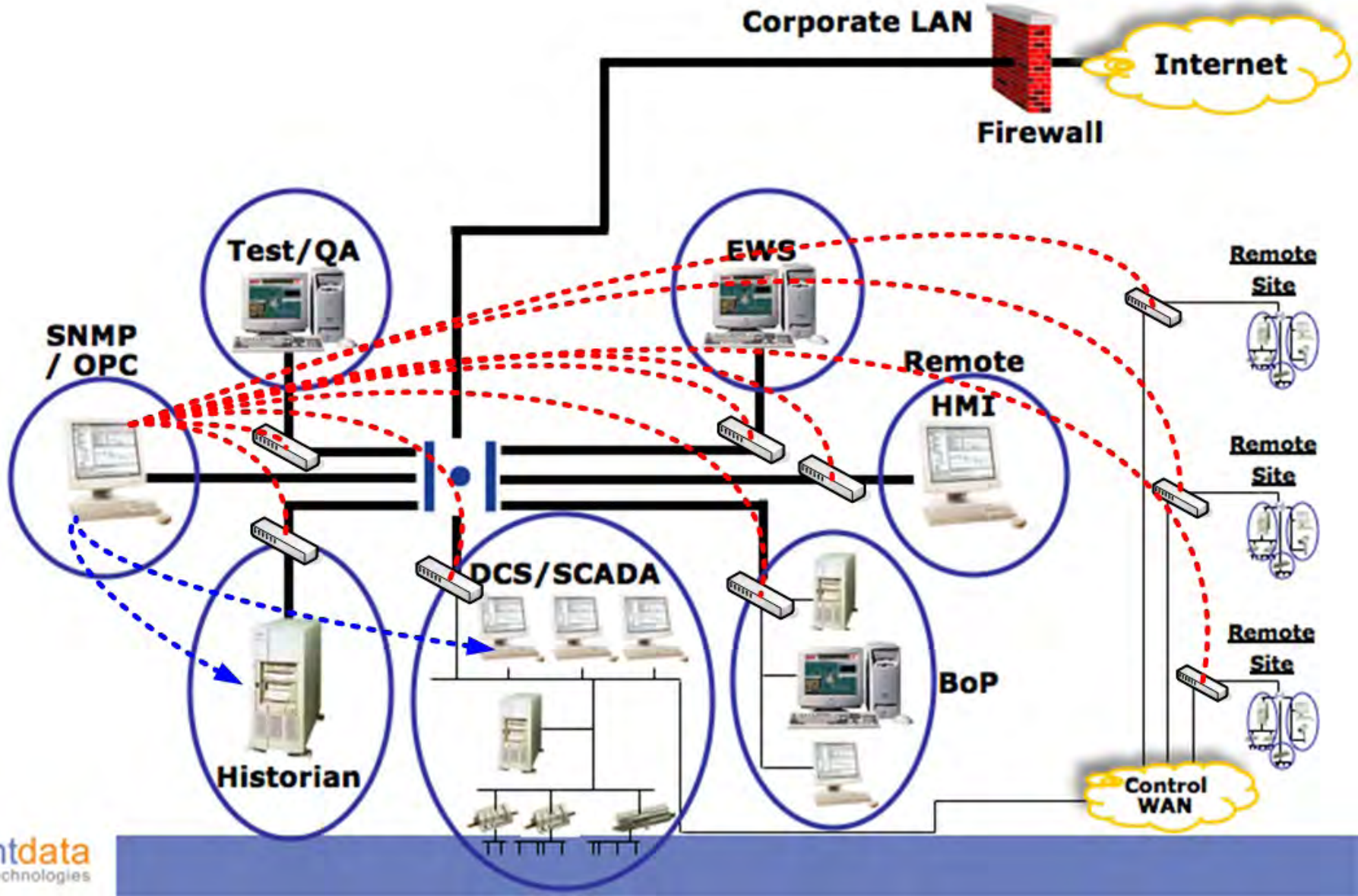
From ANY Location Regardless of Media or Bandwidth

© 2005 PlantData Technologies

After Perimeter - What's Going on in the Inside?

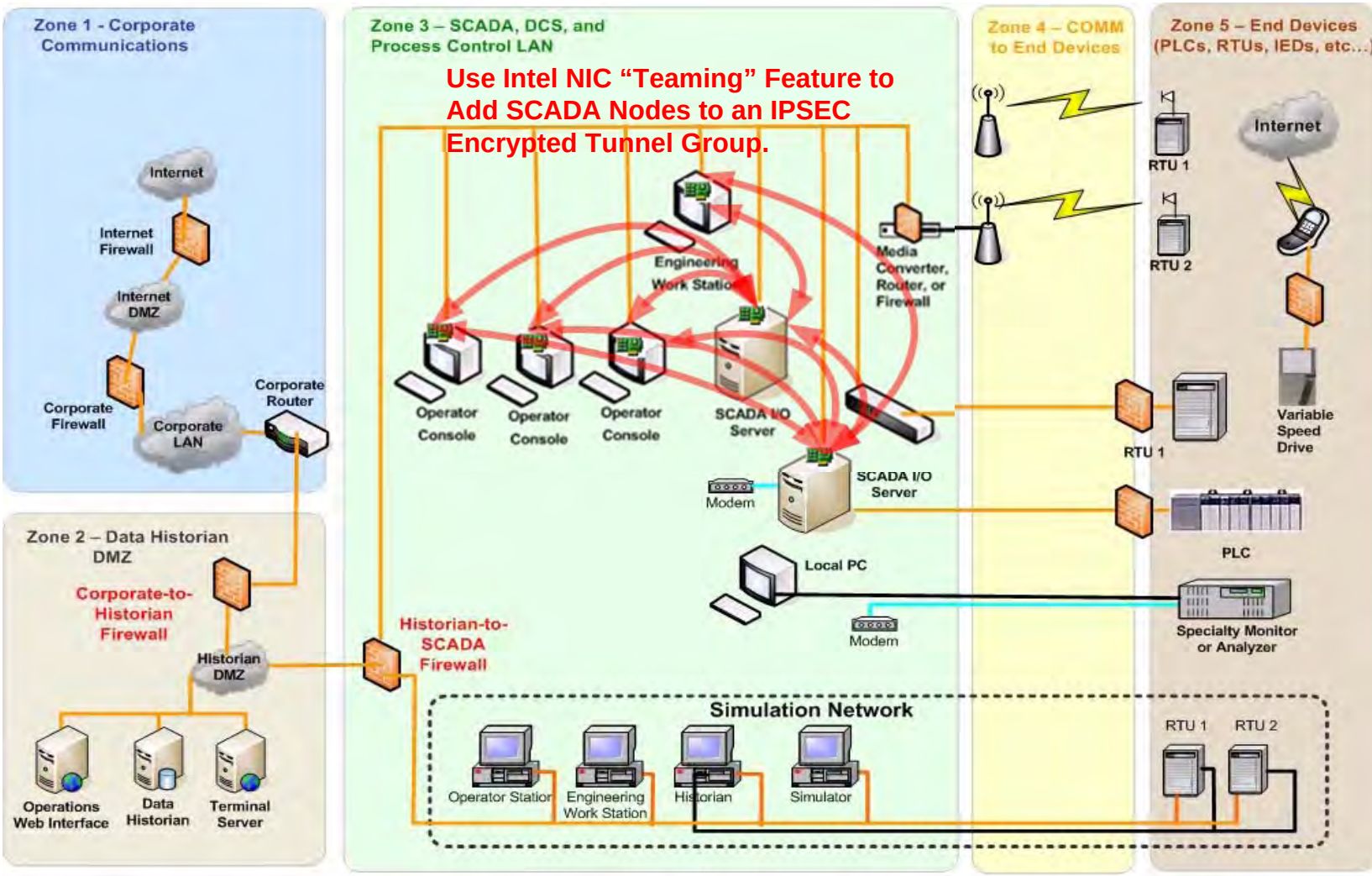


SNMP-to-OPC Gateway for Network Monitoring



plantdata technologies

IPSEC “Teaming” can allow SCADA Traffic to be Encrypted



Encrypt SCADA Traffic Within Process Control LAN

Using IPSEC to Encrypt all Traffic Between SCADA or DCS Computers

Additional Application Hardening Techniques

- **Typical Applications**
  - SCADA, DCS, or HMI Software
    - » Should be ran under a user account with least privileges
    - » Security Model of the software should be used for individual (not group) login accounts for accountability
    - » All user actions should be logged
    - » SCADA, DCS, or HMI software should be on a patch cycle based on the frequency of change from the vendor. BHP should not allow its software to get more than (3) revisions old, if an upgrade or patch can be safely made without affecting the operations of the facility
    - » Set key executables, services, and DLLs to auto-restart upon failure
  - Data Historian or Archival Applications
    - » Should be installed in a neutral DMZ network not in SCADA or in IT environments.
    - » Do not install multiple network cards in the historian server and directly connect it to all networks that it needs to communicate with
    - » Specific firewall rules should govern the flow of data from SCADA to the Data Historian servers
  - Other Critical Business Applications
    - » Ensure that the underlining Operating System is hardened
    - » Take advantage of security features within the application
    - » Restrict access to the desktop or operating system

© 2005 PlantData Technologies

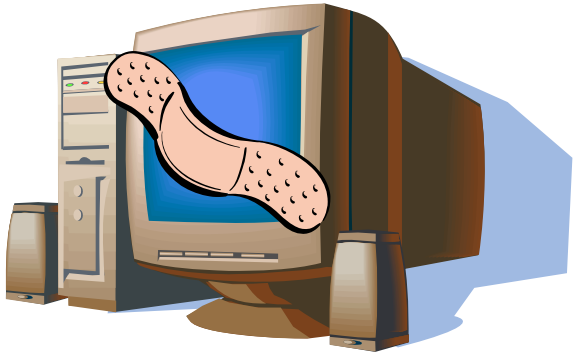
Security/Performance - Deterrence and Detection

- **Deterrence** > Firewalls are like locks - they are devices that actively “LOCK” out unauthorized attempts.
  - Like Locking Doors on Your Car
  - In most cases, just **locking the doors** will create enough hassles to deter most people from even attempting to break in.
  - The alarm light blinking on the dash or stickers on the car doors are additional deterrence.
  - Having banners on all digital access that indicate that any unauthorized access will be prosecuted, and IDS systems in place let cyber criminals know that you mean business.
- **Detection** > IDS and Monitoring Systems are like Alarm Systems
  - Monitors the health and performance of the network, host systems, and even applications and devices, and send out alerts when anything is abnormal.
  - Provides notification if someone or something get through the defense
  - Allows historical trending of system performance and security

© 2005 PlantData Technologies

Creative Solutions - Host Performance Monitoring

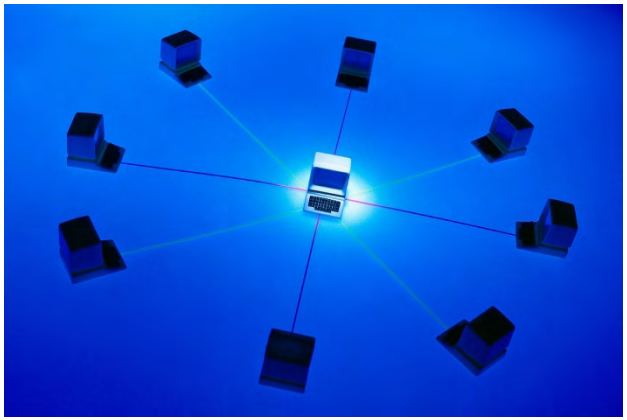
- System Security Monitoring Using the System Itself
  - Use native scripting and system tools to build a Host-based Intrusion Detection System (HIDS)
  - Shell Scripts (Unix/Linux)
  - Vbscript (Windows)
  - Perl (most Unix systems have Perl installed by default)
- Why?
  - Monitor critical system security and performance
  - No system performance hit
  - No software installation
  - No cost



© 2005 PlantData Technologies

Creative Solutions - Host Performance Monitoring

- What can be monitored
  - Accounts / Account Usage
  - User Access
  - Network Access
  - Critical files (rhosts, passwd, shadow, logs, etc.)
  - SUID/GUID files
  - NFS Mount Points
  - ARP Tables
  - World Writable and Executable Files
  - Windows Registry
  - Processes
  - System Performance
- This can all be monitored with native scripts
- Alerts can be emailed



© 2005 PlantData Technologies

Creative Solutions - Host Performance Monitoring

- Example of ‘passwd’ file / accounts monitoring (Unix/Linux):
  - Compares the passwd file over a set amount of time, compares the difference, if any, and creates a report.

```
#!/bin/ksh

mv userwatch.log userwatch.log.old
cat /etc/passwd > userwatch.log
diff userwatch.log userwatch.log.old > userwatch.report
chmod 644 userwatch.log
chmod 644 userwatch.report
```


© 2005 PlantData Technologies

Creative Solutions - Host Performance Monitoring

- Example of SUID root monitoring (Unix/Linux):
  - Checks for changed SUID root permissions

```
#!/bin/ksh

if [ -f suidscan.log.old ]
then
rm suidscan.log.old
mv suidscan.log suidscan.log.old
fi
find / -type f \( -perm -2000 -o -perm -4000 \) -exec ls -l {} \; >
   suidscan.log
diff suidscan.log suidscan.log.old > suidscan.report
chmod 644 suidscan.log
chmod 644 suidscan.report
chmod 644 suidscan.log.old
```


© 2005 PlantData Technologies

Creative Solutions - Host Performance Monitoring

- Example of process monitoring (Windows VBscript):

```
for each objService in objServices
   WScript.Echo objService.Name
   if boolShowDetails = TRUE then
      for each objProp in objService.Properties_
         ' Print out NULL if the property is blank
         if IsNull(objProp.Value) then
            Wscript.Echo " " & objProp.Name & " : NULL"
         else
         ' If the value is an array, we need to iterate through each element
         ' of the array
            if objProp.IsArray = TRUE then
               For I = LBound(objProp.Value) to UBound(objProp.Value)
                  wscript.echo " " & objProp.Name & " : " & objProp.Value(I)
               next
            else
           ' If the property was  not NULL or an array, we print it
                wscript.echo " " & objProp.Name & " : " & objProp.Value
            end if
         end if
      next
      WScript.Echo ""
   end if
next
```


© 2005 PlantData Technologies

Creative Solutions - Host Performance Monitoring

- Example of Monitoring the Windows registry using native tools (regedit)
  - Open the Registry Editor (*regedit.exe*).
  - In the left pane, browse to the key you want to audit. (You can't audit individual registry values.)
  - Right-click on the key and select Permissions.
  - Click the Advanced button.
  - Click the Auditing tab.
  - Click the Add button.
  - Use the Object Picker to find the user or group for whom you want to audit access.
  - In the Auditing Entry box, select the types of things you want to audit. Success is audited separately from Failure, so be sure to check all the types you want to audit.
  - Click OK until all windows are closed.
  - Open the Local Security Policy snap-in (available from Administrative Tools).
  - In the left pane, expand Local Policies and click on Audit Policy.
  - In the right pane, double-click on Audit object access.
  - Check the box beside Success to audit successful actions.
  - Check the box beside Failure to audit failed actions.
  - Click OK.

© 2005 PlantData Technologies

Creative Solutions - Host Performance Monitoring

- There are hundreds more scripts and native tools to monitor, analyze, and report system function, activity, access, etc.
- Just about any system function can be monitored natively and automatically
- Results can be analyzed with a script and alert on changes, thresholds, and access
- For more information and downloadable scripts:

www.ci-institute.org

© 2005 PlantData Technologies

Conclusion

- Eliminating vulnerabilities is the best option in avoiding an attack
- Understanding and securing the critical communication paths for the system will ultimately ensure that the right people can access the system and others can not.
- Availability (uptime / performance) is directly tied to security
- Understanding each component or functional layer of a SCADA or DCS and how they can contribute to the performance and security of the system is important
- Properly securing and hardening each component of SCADA/DCS systems increases the availability of the system
- Properly isolating SCADA / DCS systems from all other non-critical environments is the first key step
- Consider creative solutions in the meantime while piloting new technology for securing process control systems
- Ensure that technical solutions involve both DETERRENCE and DETECTION capabilities - think of your car locks and alarm

© 2005 PlantData Technologies

Q & A

- **Contact Information:**
  - Jonathan Pollet, CAP, CISSP
  - PlantData Technologies, a division of Verano
  - Email: jonathan.pollet@plantdata.com
  - Phone: 877-302-DATA EXT 211
  - Cell: 281-748-6401
  - 1201 Louisiana St., Suite 400
  - Houston, Texas 77002

- **Services:**
  - Security Consulting
  - SCADA Security Roadmap Strategy
  - SCADA/DCS System Audits and Assessments
  - Network Architecture Reviews
  - Technology Deployment Services for Security Systems
  - Security Training
  - Red Team Penetration Testing
  - Gap Analysis and NERC Compliance Consulting

© 2005 PlantData Technologies

Questions and Answers

Contact Information:

Jonathan Pollet
PlantData Technologies, Inc.
Houston, Texas, U.S.A
(877) 302-DATA

PlantData Services:

Software Development
Windows Applications, Web Applications, Web Site Design (Flash, ASP, ASP.NET, JAVA, PHP) Database Solutions (Oracle, SQL Server, Microsoft Access, DB2), Custom .DLL design, Database Integration, and Data Restoration Services

Industrial Automation
PLC Programming, RTU Firmware Design, SCADA Systems Design, RF Communications, Plant Optimization, Operator Interface Design, and Plant-to-ERP Integration Services

Security and IT Consulting
Cyber Security Vulnerability Assessments, Cyber Security Penetration Testing, LAN/WAN Network Design, Firewall Design & Implementation, Windows 2000/20003 with Active Directory Migration, Exchange 2000/2003 Email Implementation, Terminal Services and Citrix MetaFrame Design and Implementation

© 2005 PlantData Technologies