

The image shows the cover of a spiral-bound notebook. The cover is a light beige or tan color with a fine, woven fabric texture. A silver metal spiral binding is visible along the left edge. The notebook is set against a solid dark brown background. The text is centered on the cover in a black, serif font.

# Chevron Phillips Chemical Co.

PCN Architecture Design and  
Philosophy

# CPChem PCN Cyber-Security

---

- Policy Adopted 3<sup>rd</sup> Qtr 2002
- Joint IT & Process Control effort
- General Philosophy
  - No changes to process controls from outside the PCN
  - PCN must operate independently from the business network
  - Controls and APC applications go in the PCN. Everything else goes in the business network.
  - No business computing done on PCN computers (i.e., e-mail, Word, Excel, Internet, intranet)

# PCN Policy Highlights

---

- No network connections to PCN except the local CPChem Business Network (BN) LAN
- Firewall between BN and PCN
  - All inbound traffic blocked
  - Only required outbound traffic allowed
  - Central firewall management
  - Standard hardware across enterprise

# PCN Policy Highlights

---

- PCN Network may not physically extend outside the process area. Exceptions must be approved by Plant Manager and IT.
- Computers may not be connected to the BN and PCN simultaneously
- No control changes made from outside the PCN
- Anti-virus in PCN required
- Password security rules

# PCN Policy Highlights

---

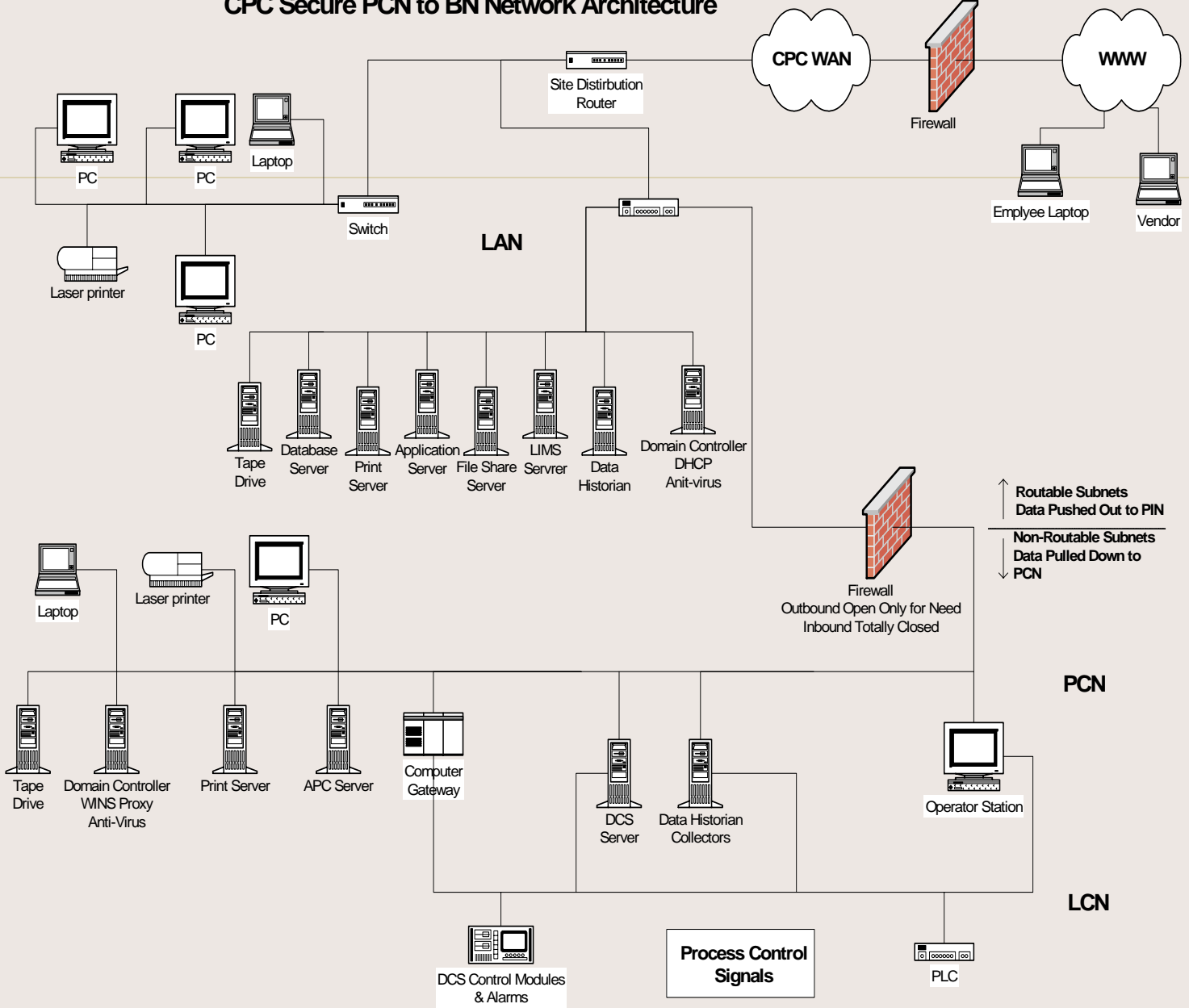
- No modems in the PCN
- Remote Access requires IT and Plant Manager approval
- Remote access to PCN only via VPN with two-factor authentication
  - Non-employees token held by CPChem employee
  - 1<sup>st</sup> choice is SSL VPN with Terminal Session access
  - 2<sup>nd</sup> choice is IP-Sec VPN with IP address restricted access

# Remote Access Balance

---

- Need for Security
  - Low probability but high consequences
  - Open system propagation
  - Unknown threat source
- Need for Access
  - High benefit applications
  - Limited expert support
  - Reliability required for Operator confidence
  - Systems may not be as robust as Business Apps.

# CPC Secure PCN to BN Network Architecture





# CPCChem Vendor Expectations

---

- Stay more current with other vendor upgrades and patches (Microsoft, Oracle, etc.)
- Design for remote support via VPN, not modems.
- Do not design PCN hardware and software expecting MS Office, email, Instant Messaging, Intranet access, or Internet access.

# CPCChem Vendor Expectations

---

- Applications on the BN should not need to access the PCN for reporting and analysis.
- Design to OPC standards
- Design software that will connect to any major brand of data historian (OPC connections)

# Summary

---

- Suppliers need to address PCN security during design
  - ISA SP 99
  - NIST SPP-ICS
  - NIST SCP-ICS
- Suppliers need to stay current if using open systems