



PCN Cyber-security Considerations for Manufacturers

Based on Chevron Phillips
Chemical Company PCN
Architecture Design and
Philosophy



Contents

- ◆ CPChem PCN Philosophy and Policy
- ◆ Remote Access Considerations
- ◆ CPChem PCN Architecture
- ◆ Our Expectations from the vendors
- ◆ Summary



CPChem PCN Cyber-Security

- ◆ Policy Adopted 3rd 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 if applications will handle it
- ◆ Password security rules same as BN except for Operator Stations



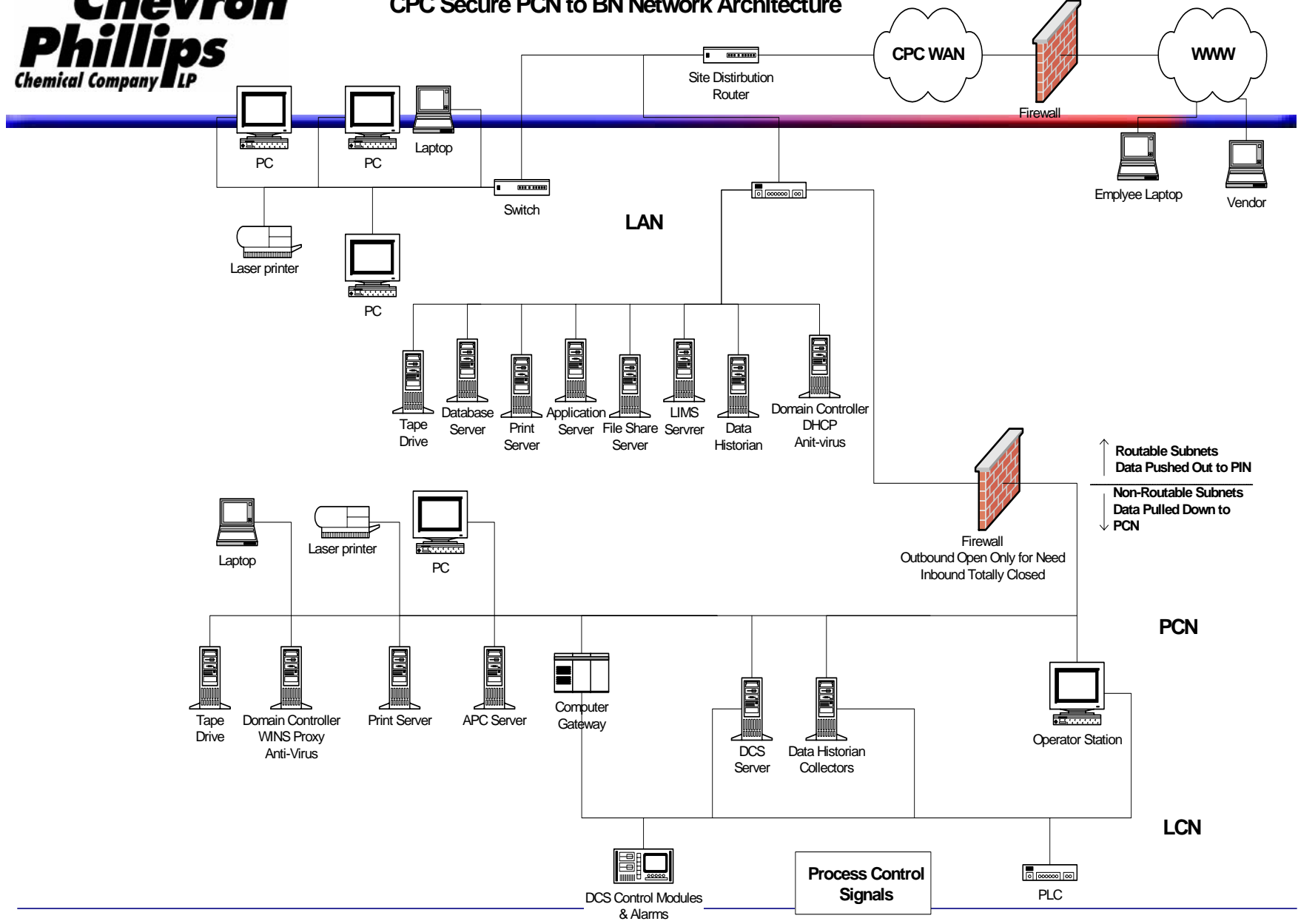
PCN Policy Highlights

- ◆ 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
 - ◆ 1st choice is SSL VPN with Terminal Session access
 - ◆ 2nd choice is IP-Sec VPN with IP address restricted access

- ◆ 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





CPChem 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.
- ◆ Design to push data out of the PCN



CPChem 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)
- ◆ For Microsoft platforms: Design security to connect to Active Directory and use the PCN domain network password for access to everything.



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