



Idaho National Laboratory

Process Control System Forum Information Sharing

Rita Wells

SCADA and Power Systems

October 27, 2005



Information Sharing Agenda

- **Liability**

Whitepaper on Liability of Best Practices

Disclaimers

- **Currently Recommended Best Practices**

Clear Text Communications

Accounts/Passwords

Authentication

Un-Patched Applications

Proprietary Protocols

Buffer Overflows

Liability of Best Practices

From the Liability Issues and Information Sharing paper on www.pcsforum.org/

“When a member organization discloses its recommended practices to other forum members, this does not create a contractual obligation between the parties. The lack of a contractual agreement serves to limit the potential for liability.”

Disclaimer for Best Practices

Disclaimer text should include:

- Disclaimer of liability for any personal injury, property or other damage
- No warranty of accuracy or completeness
- Usage of the standard is entirely voluntary
- Users of the standard agree to “hold harmless”
- The publishing organization does not certify compliance or render professional services in association with the standard

Disclaimer

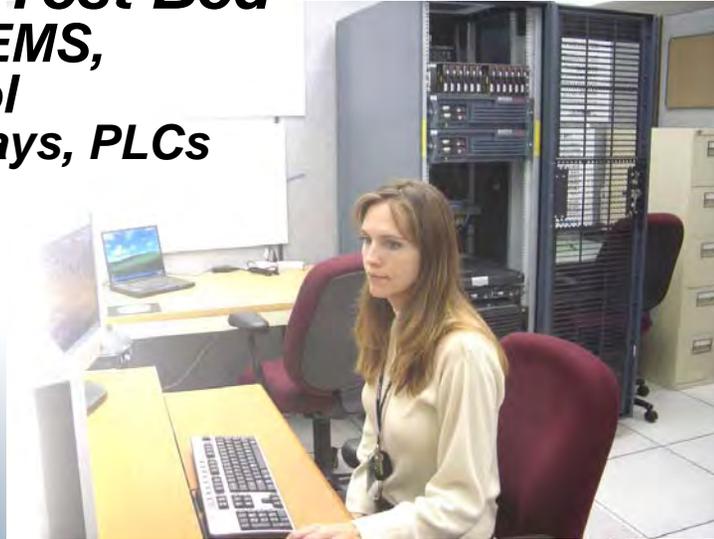
References made herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government, any agency thereof, or any company affiliated with Idaho National Laboratory.

Disclaimer 2 – For Discussion

‘ABC’ organization accepts no liability for any personal injury, property or other damage resulting from the use of currently recommended best practices, no warranty of accuracy or completeness for these entirely voluntary currently recommended best practices. Users of these currently recommended best practices agree to “hold harmless” the authors and the publishing organization does not certify compliance or render professional services in association with these currently recommended best practices.

Idaho National Laboratory

SCADA Test Bed
SCADA, EMS,
Control
RTUs, Relays, PLCs



Cyber Security Test Bed



**Communications
Test Bed**

Wireless: Cellular, HF,
Microwave, 802.11
Network: Copper,
Fiber, RF

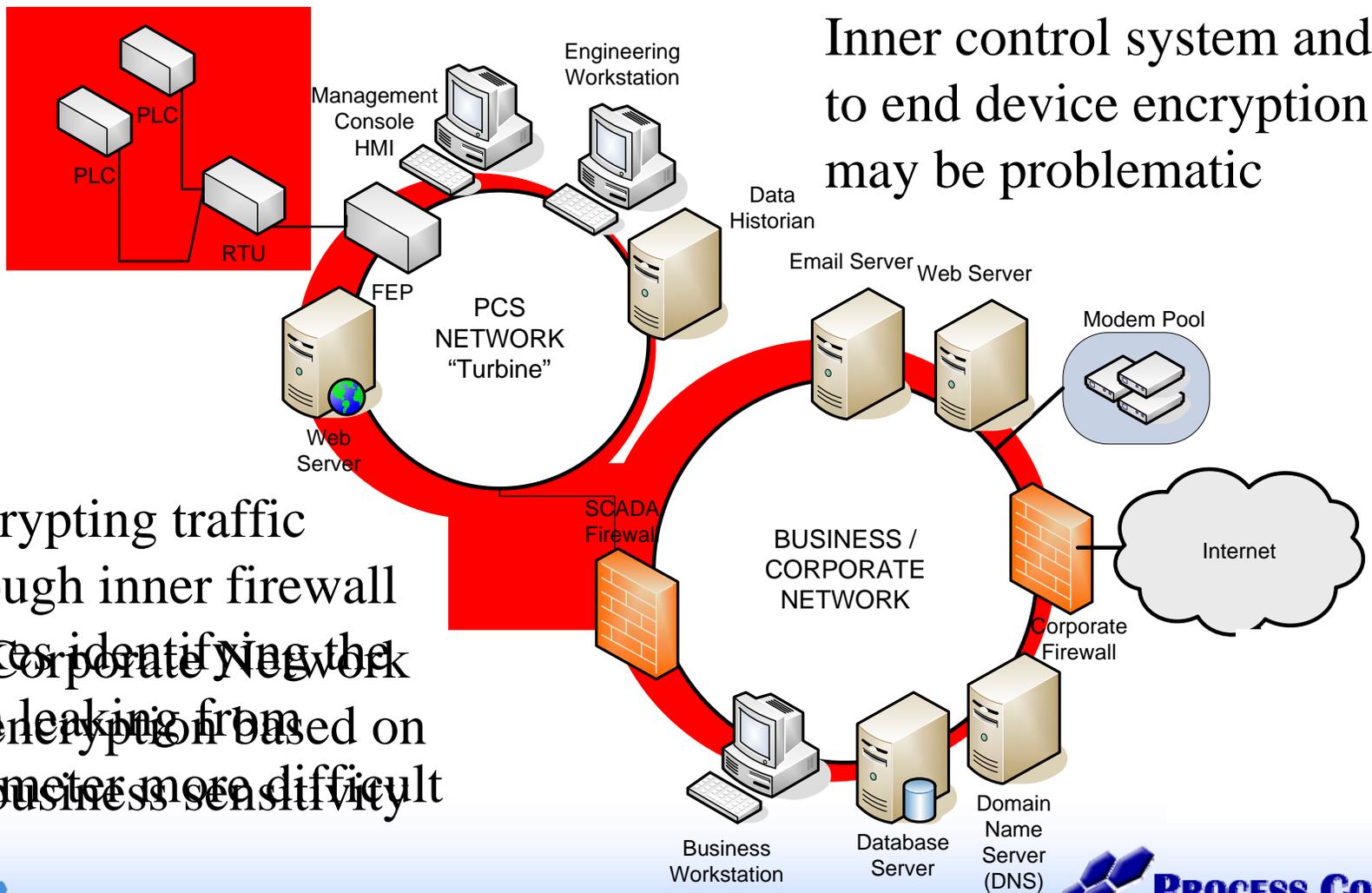


**Power Grid
Test Bed**
61 miles of 138
kV
Isolatable
substation

Currently Recommended Best Practices

- Clear Text Communications
- Accounts/Passwords
- Authentication
- Un-Patched Applications
- Proprietary Protocols
- Buffer Overflows

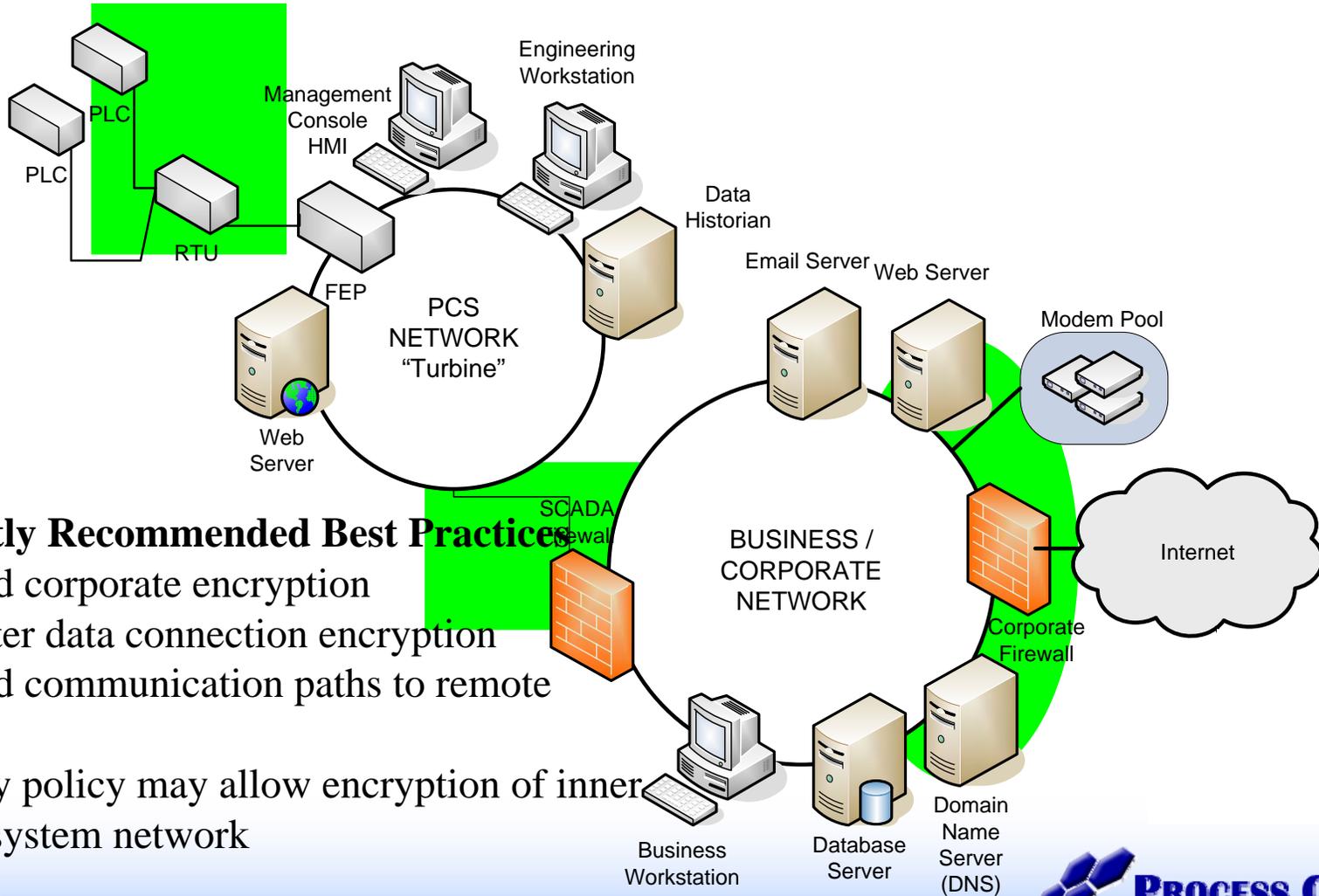
Clear Text



Inner control system and to end device encryption may be problematic

Encrypting traffic through inner firewall makes identifying the data leaking from perimeter more difficult

Clear Text



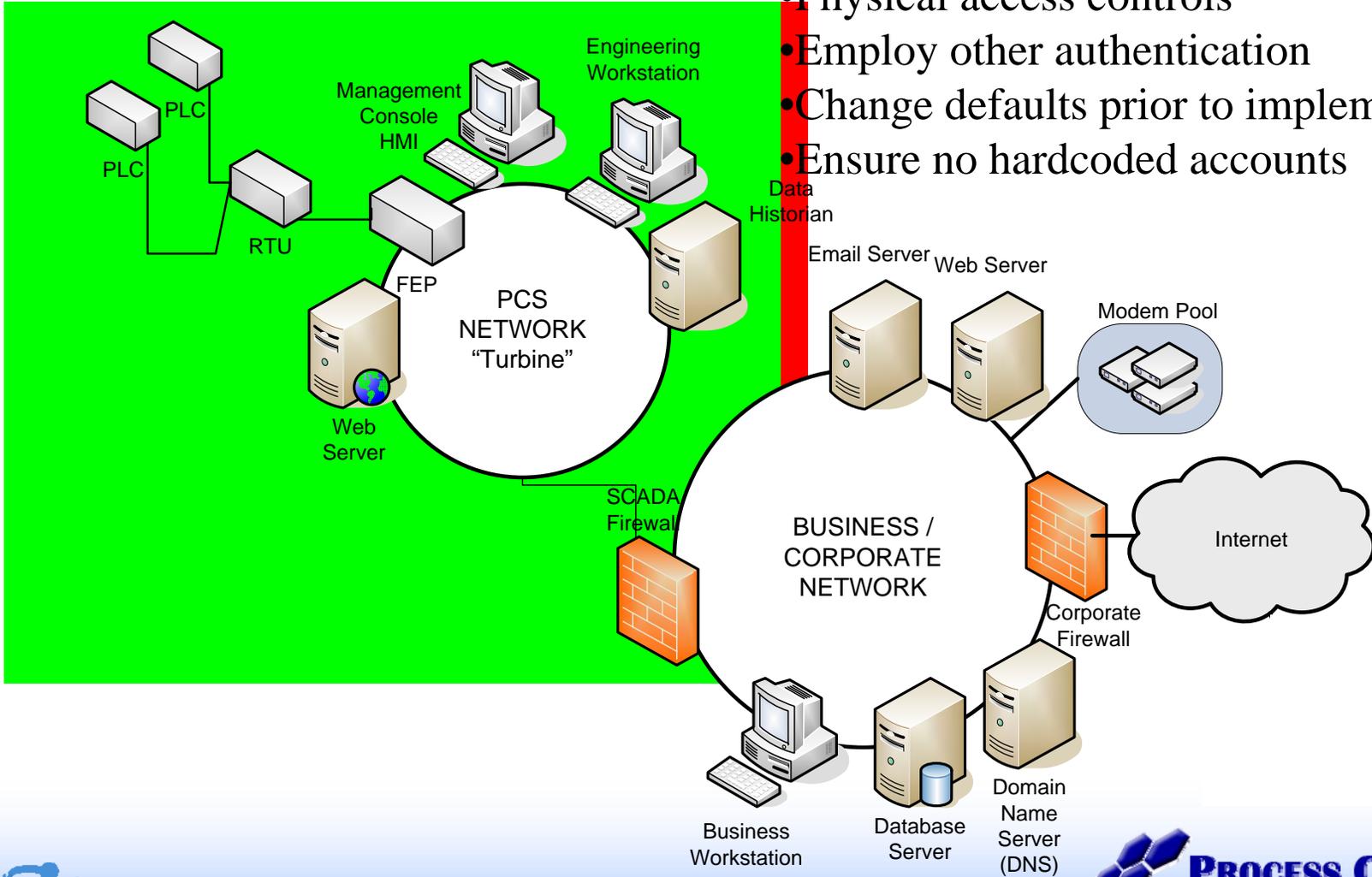
Currently Recommended Best Practices

- Selected corporate encryption
- Perimeter data connection encryption
- Selected communication paths to remote devices
- Security policy may allow encryption of inner control system network

Accounts/Passwords

Currently Recommended Best Practices

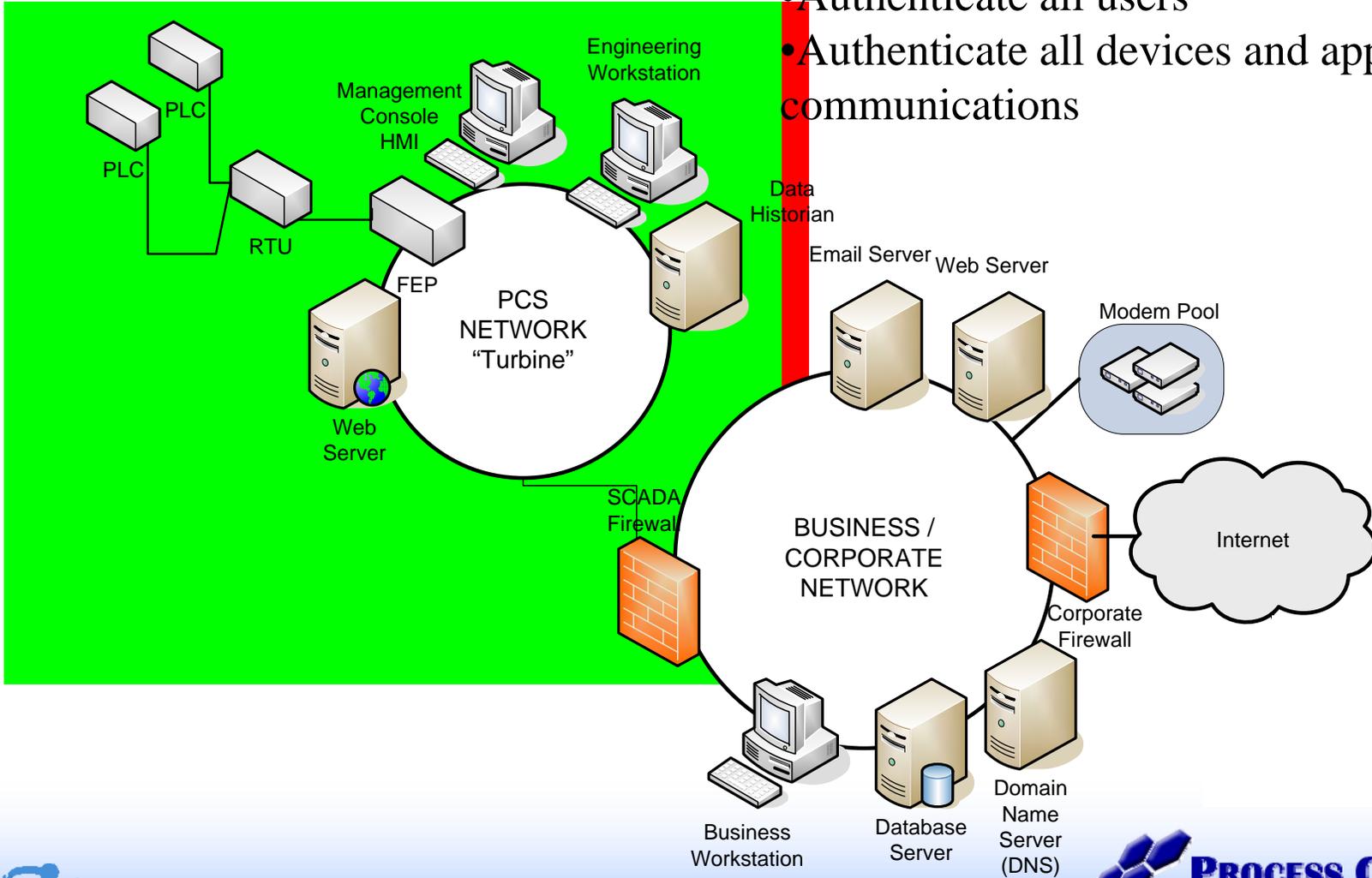
- Physical access controls
- Employ other authentication
- Change defaults prior to implementation
- Ensure no hardcoded accounts



Authentication

Currently Recommended Best Practices

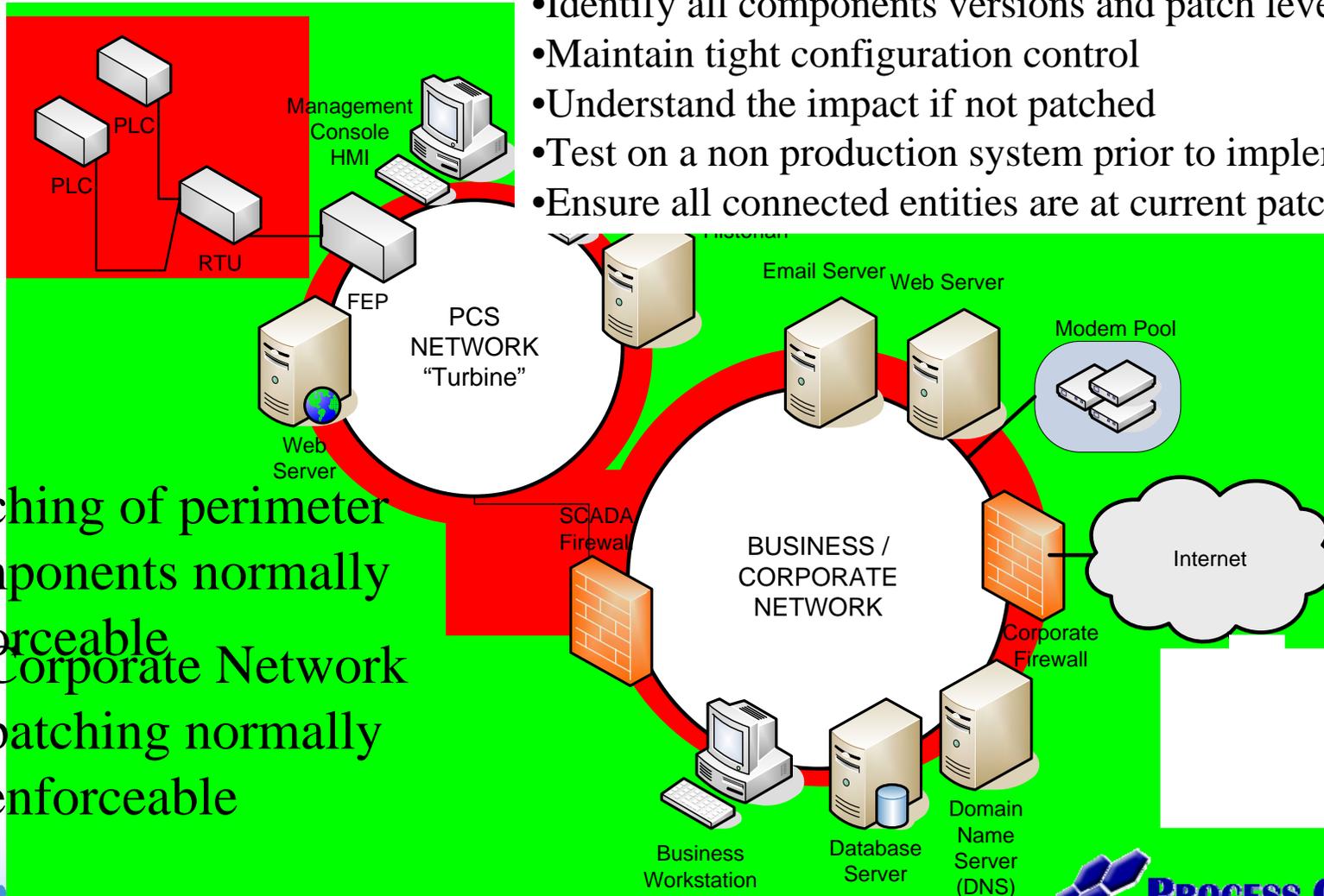
- Authenticate all users
- Authenticate all devices and application communications



Un-Patched Components

Currently Recommended Best Practices

- Identify all components versions and patch levels
- Maintain tight configuration control
- Understand the impact if not patched
- Test on a non production system prior to implementation
- Ensure all connected entities are at current patching levels

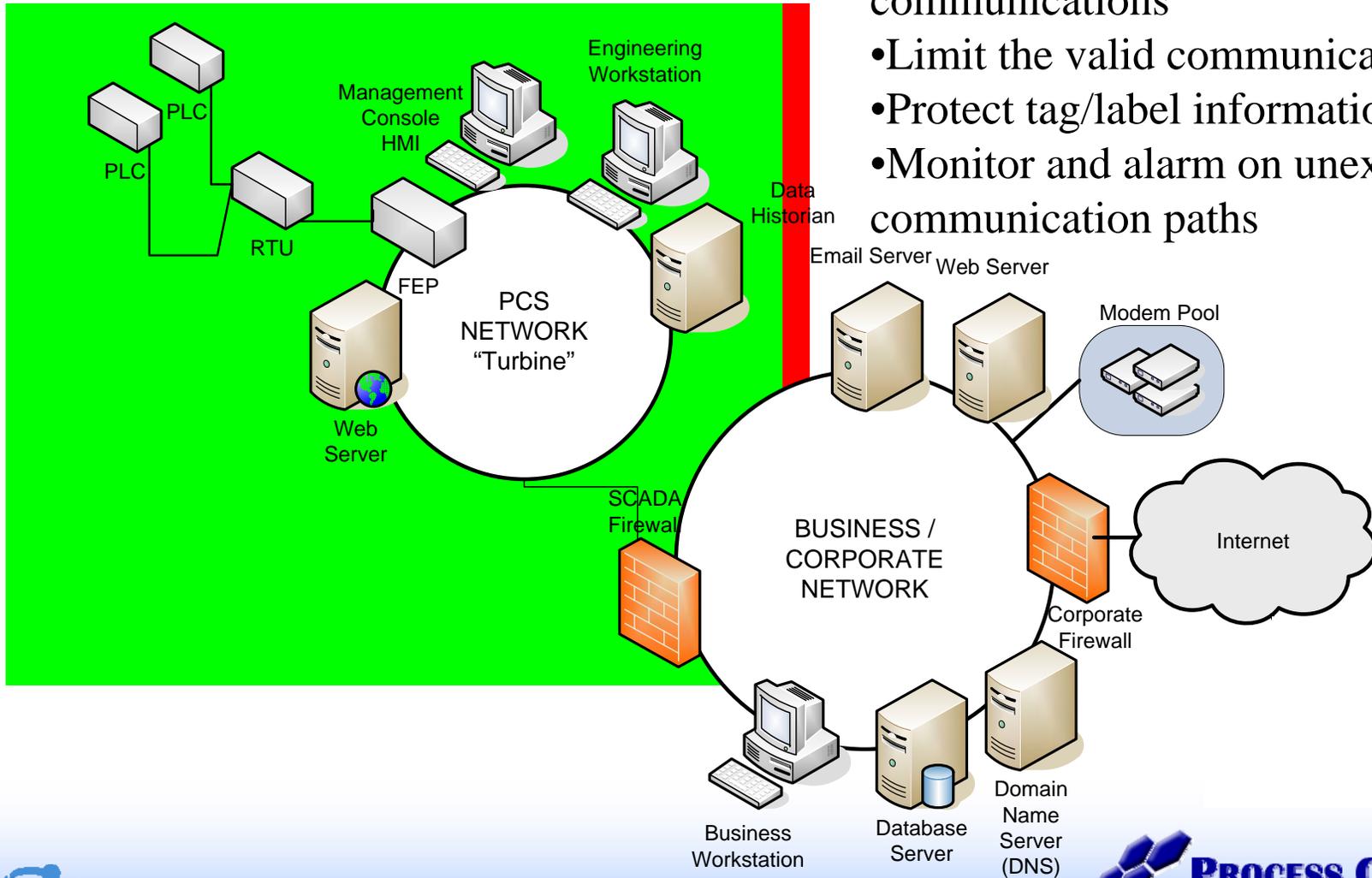


Patching of perimeter components normally enforceable
Corporate Network patching normally enforceable

Proprietary Protocols

Currently Recommended Best Practices

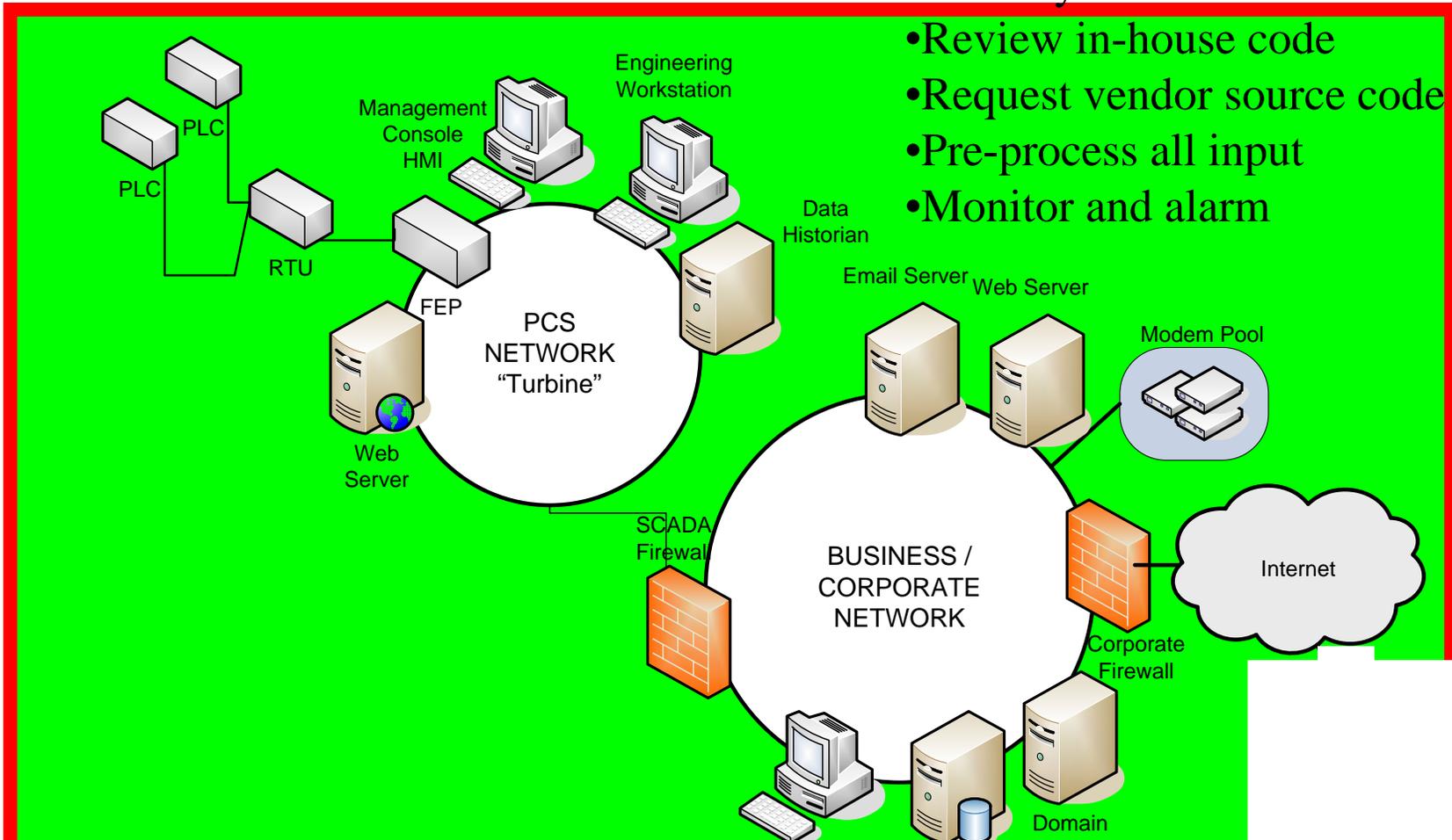
- Authenticate all network communications
- Limit the valid communication paths
- Protect tag/label information
- Monitor and alarm on unexpected communication paths



Buffer Overflows

Currently Recommended Best Practices

- Patch systems
- Review in-house code
- Request vendor source code review
- Pre-process all input
- Monitor and alarm



Contact Information

Rita Wells

SCADA and Power Systems

Advisory Engineer

(208) 526-3179

rita.wells@inl.gov