IT/OT Systems Integration and Planning

Hoot Royer, CISM, PMP, GCIP, ITIL, GSEC

About Me

Currently working within the electric utility space managing IT, cybersecurity, and telecommunications.

Areas of expertise:

- Governance, Risk, Compliance
- Project Management
- Audits
- IT/OT Planning and Strategy
- Tabletop Exercises

BS in Information Technology from WGU. Certifications: PMP, CISM, ITIL, GSEC, Security+, Network+, GCIP, GICSP, FCC GROL.

What are we talking about?

Information Technology (IT) covers areas of technology within the organization that interact primarily with corporate users, whereas Operational Technology (OT) covers areas of the organization that interact with field personnel.

Source: cisa.gov
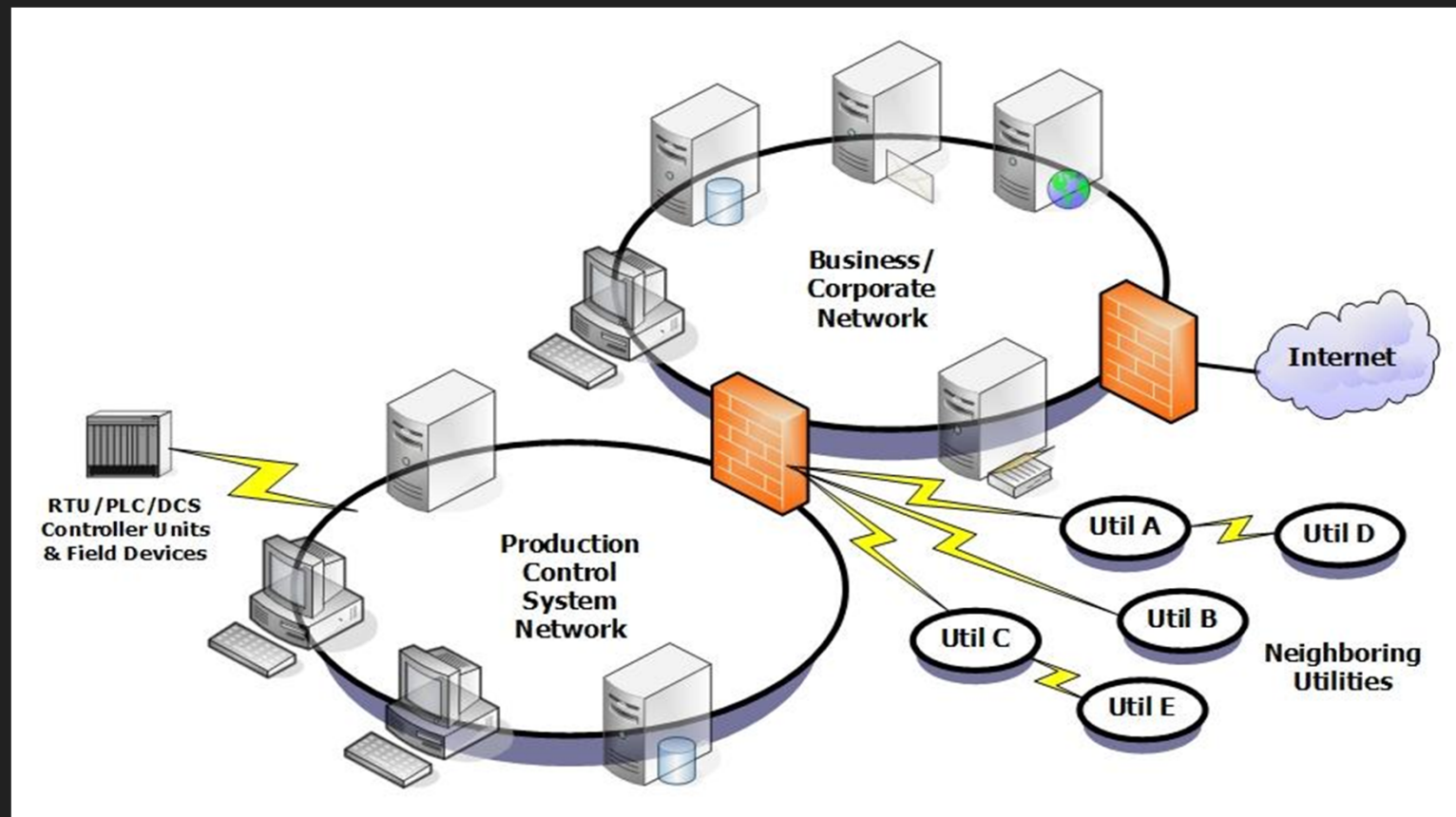
Challenges and risks

Securely integrate Operational Technology (OT) environments with Information Technology (IT) systems. While balancing the right amount of data and access with the appropriate level of security to ensure systems meet regulatory compliance requirements.

Where to start

Source: Sean Gallup/Getty Images

- Know what you have
- Know key stakeholders
- Identify lines of demarcation
- Determine business needs of IT/OT integration
- Determine regulatory compliance requirements
- Build security from the ground up–not as an afterthought
- Develop, implement, and test disaster recovery and incident response plans
- Have a plan to perform OT functions manually (switching circuits, redirecting power, etc)

Ongoing considerations

- Perform annual disaster recovery and incident response plan testing.
- Conduct regular reviews of what current business needs are–as business needs change, system integration and levels of access should be adjusted to meet needs.
- Monitoring of system use, access of critical system resources using logs and through tuning of notifications to make them actionable.
- Ongoing threathunting using current indicators of compromise (IOC's)
- Backup configuration for not only IT systems, but OT systems.
- Regulatory compliance requirements. Compliance does not automatically equal security.

Areas of Support:

- NERC CIP Implementation and Compliance Review
- Tabletop Exercises
- Cybersecurity Planning and Strategy
- Disaster Recovery and Incident Plan Development
- OT/IT Integration Planning and Testing
- Compliance Support
- Security Framework Implementation

Happy to connect! https://www.linkedin.com/in/hoot-royer/