

# Protecting SCADA From the Ground Up

Aaron Bayles

DC101 @ DEF CON 22

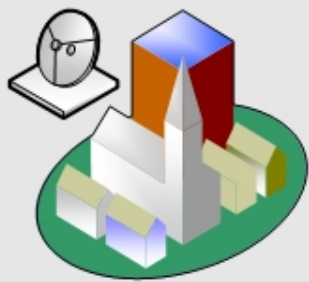
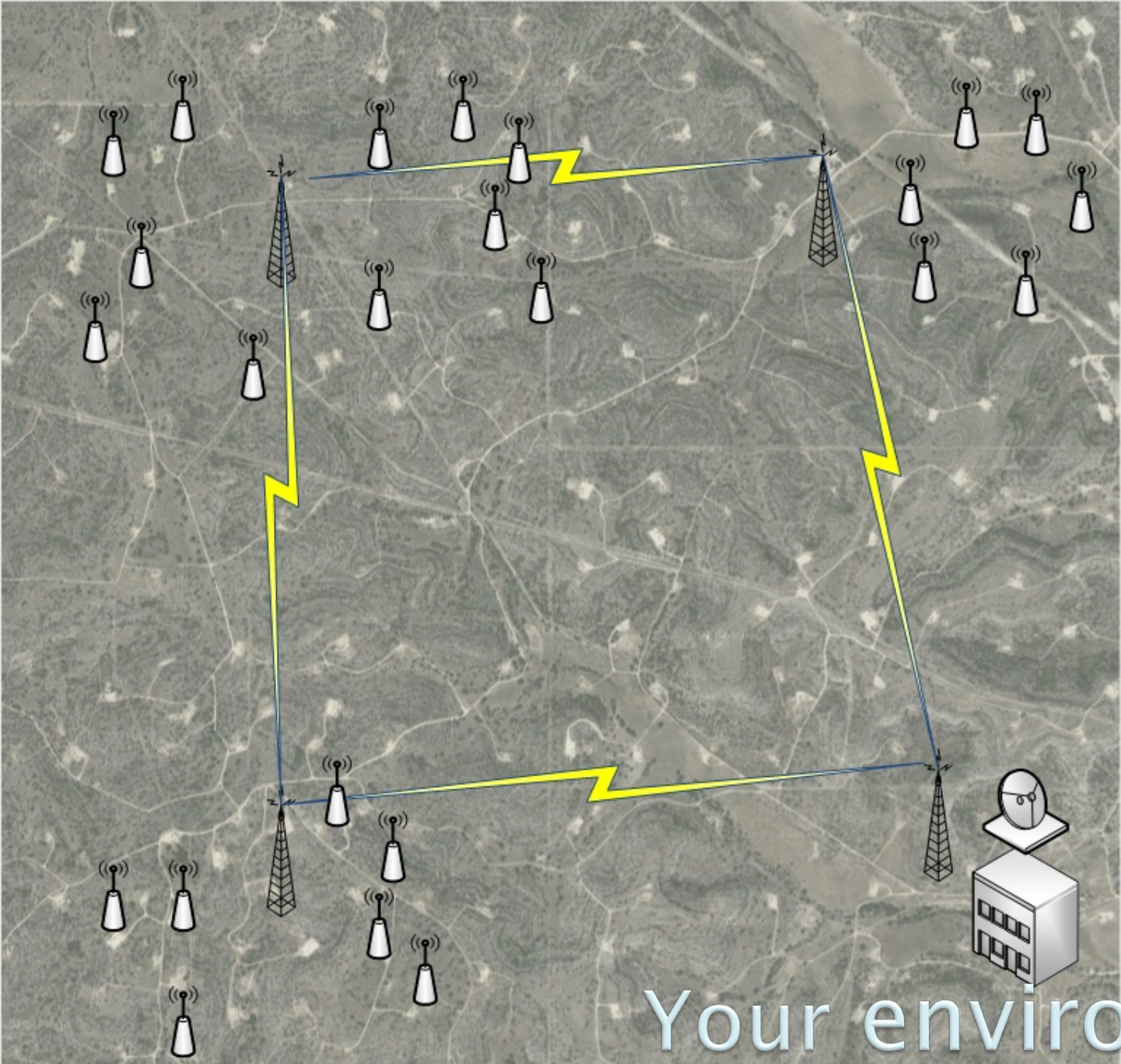
# whoami && id

- ▶ 19 years in IT/Infosec
- ▶ Worked in Oil & Gas (O&G) last 8 years
- ▶ Along the way
  - Penetration testing
  - Vulnerability assessment
  - Network architecture, design & implementation
  - Risk assessment

# What's the problem?

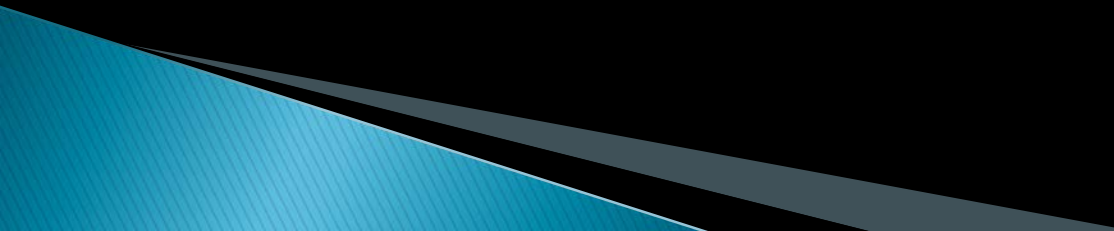
- ▶ Legacy equipment/comms
- ▶ Remote (geographic) connectivity
- ▶ Availability, not confidentiality or integrity is key (control)
- ▶ Power/space is a premium
- ▶ Life safety can be dependent

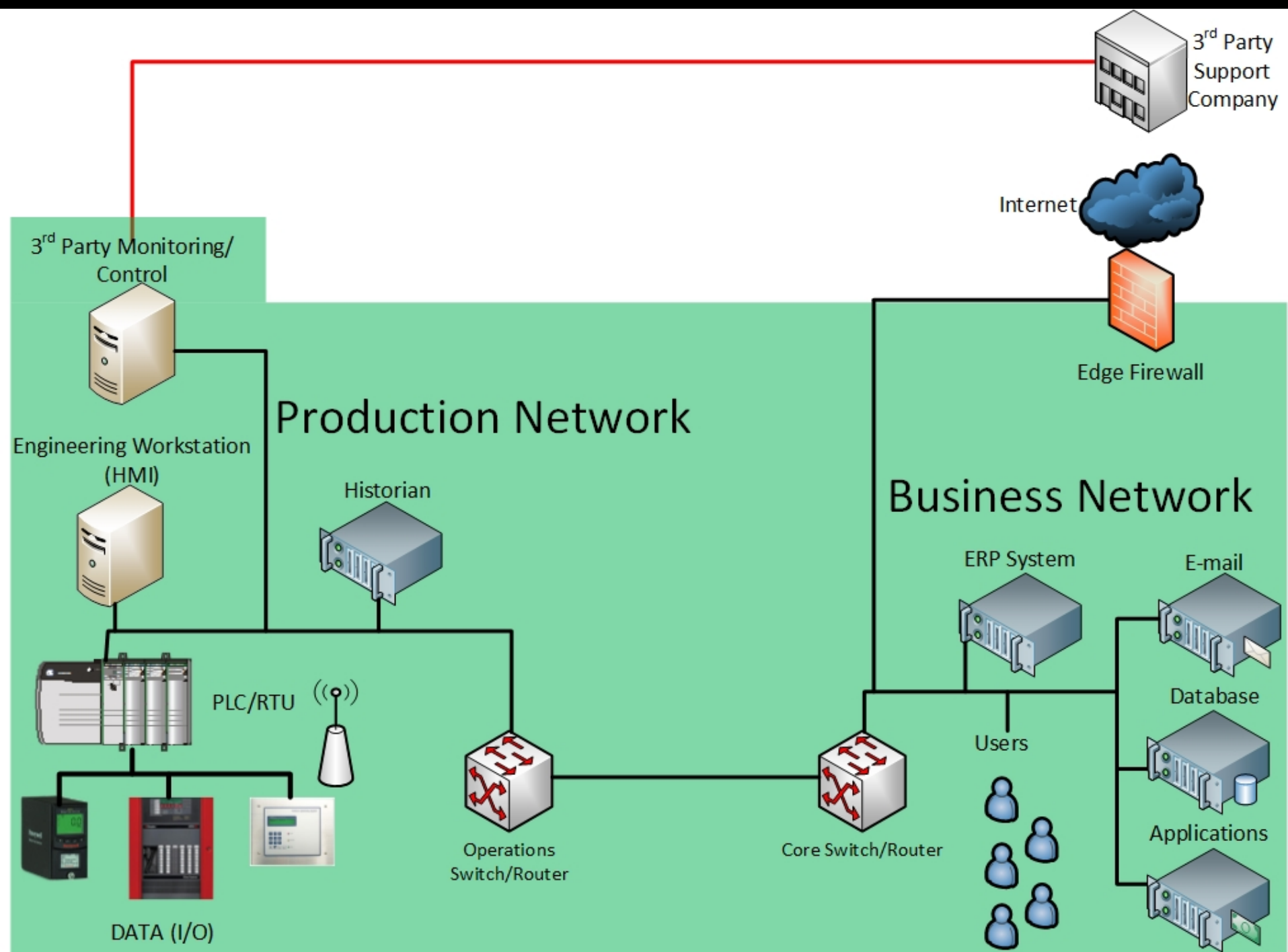
**The demands placed on Industrial Control Systems (ICS) & SCADA networks don't match up with security requirements**



Your environment

# First steps

- ▶ Understand your network & data flows
  - ▶ Does not require expert knowledge
  - ▶ Start with the basics
  - ▶ Some concepts for enterprise IT can be used, **with modification**
  - ▶ Build relationships between enterprise IT and industrial IT
- 



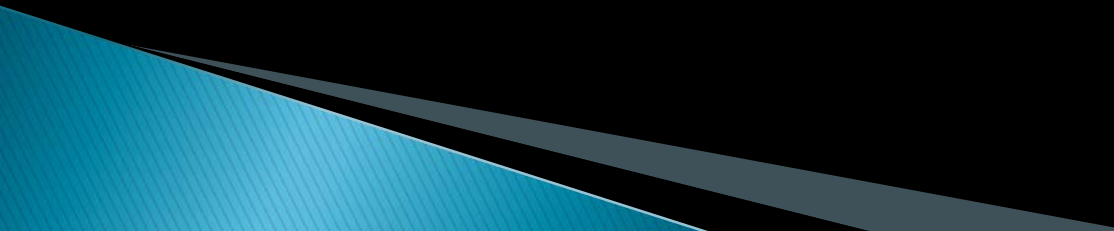
# Best practices

- ▶ Network segmentation
- ▶ Portable media control
- ▶ Configuration management
- ▶ Patch management
- ▶ Disaster recovery (DR) planning
- ▶ Workforce development/training

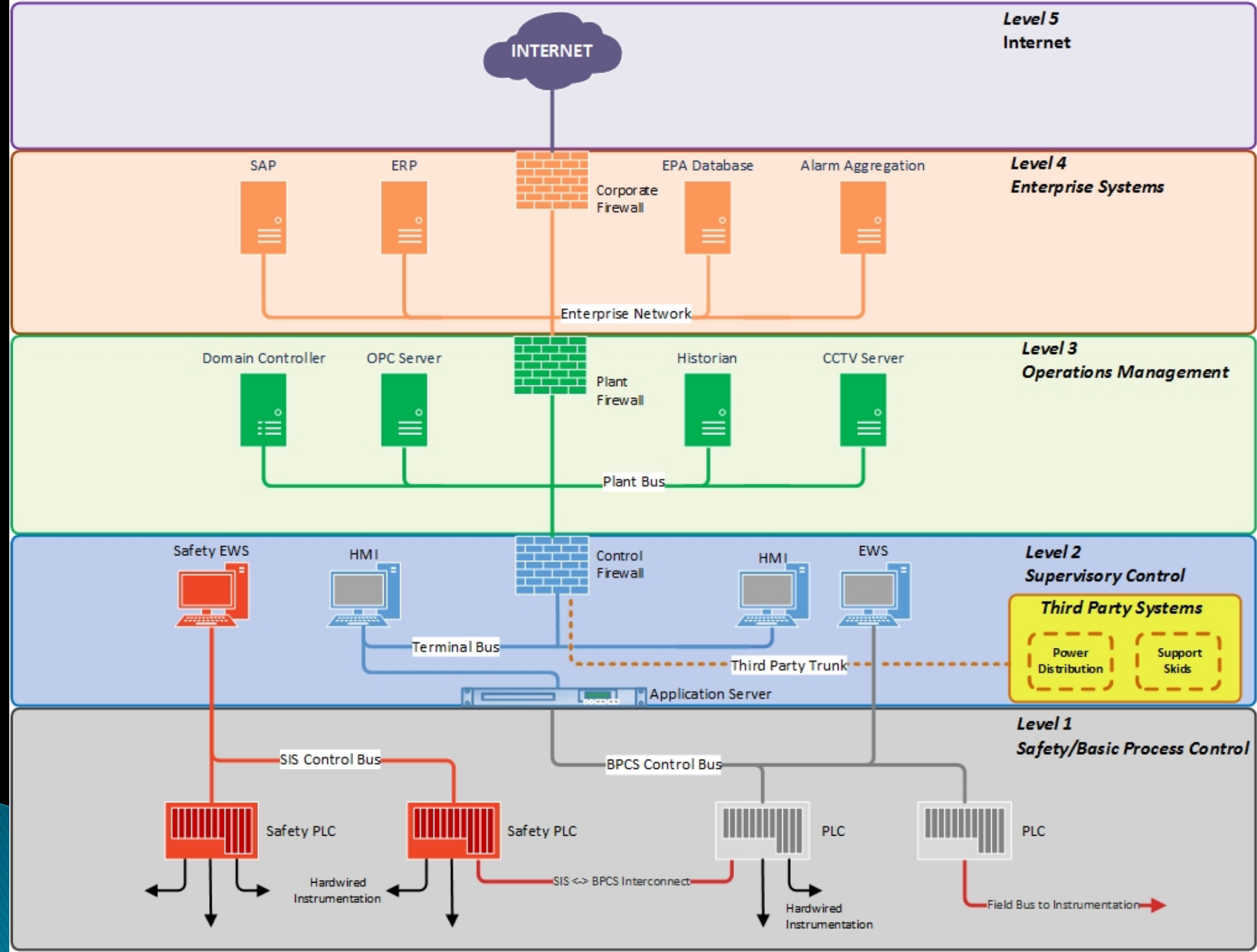
**Although these may be similar,  
significant differences exist**



# The Purdue Model

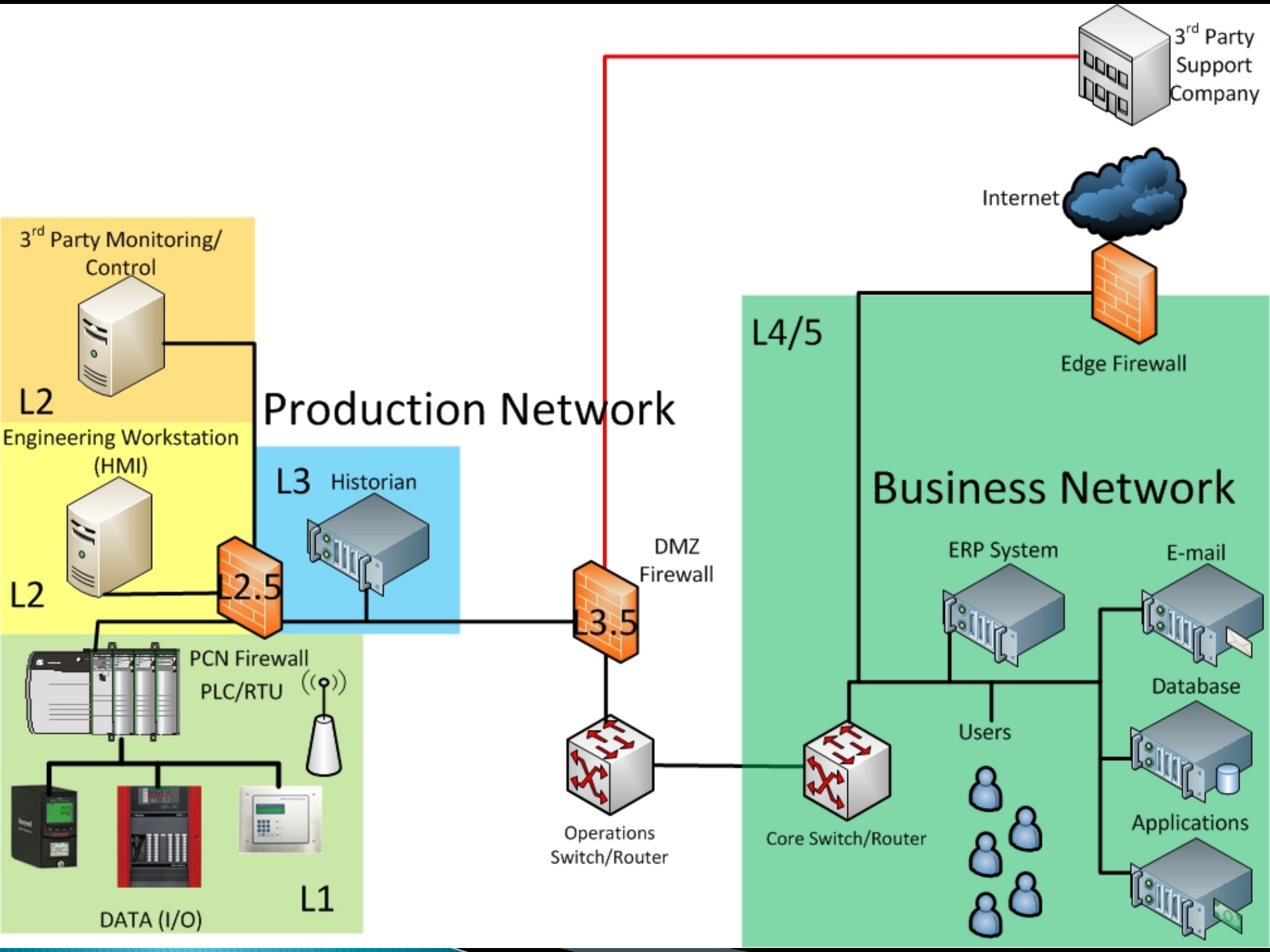
- ▶ Formally the Purdue Enterprise Reference Architecture (PERA)
  - ▶ Widely accepted within ICS industry
  - ▶ Compatible with multiple standards, ISA95, ISA99, and IEC 62443
  - ▶ Works with zone & conduit concepts
  - ▶ Represented by Layers 0/1–5
  - ▶ Starting point for ICS network segregation
- 





# Purdue continued

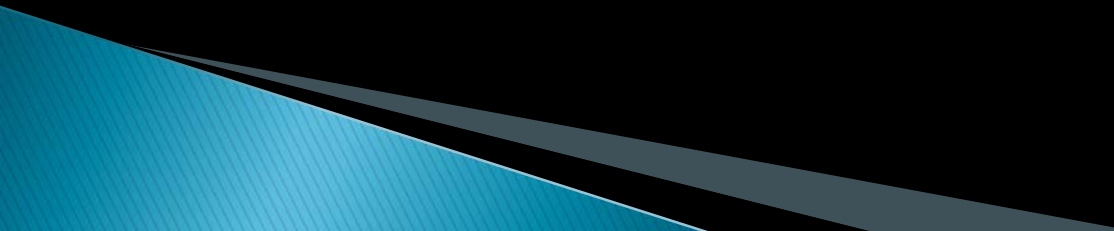
- ▶ Traffic within same zone is allowed
- ▶ Traffic passing between zones via conduits are controlled
- ▶ Layer 2 (L2) can **SET/CHANGE** values on L1
- ▶ L3 can only **READ** values from L2 & L1
- ▶ Control points also allow for reporting



# Firewalls

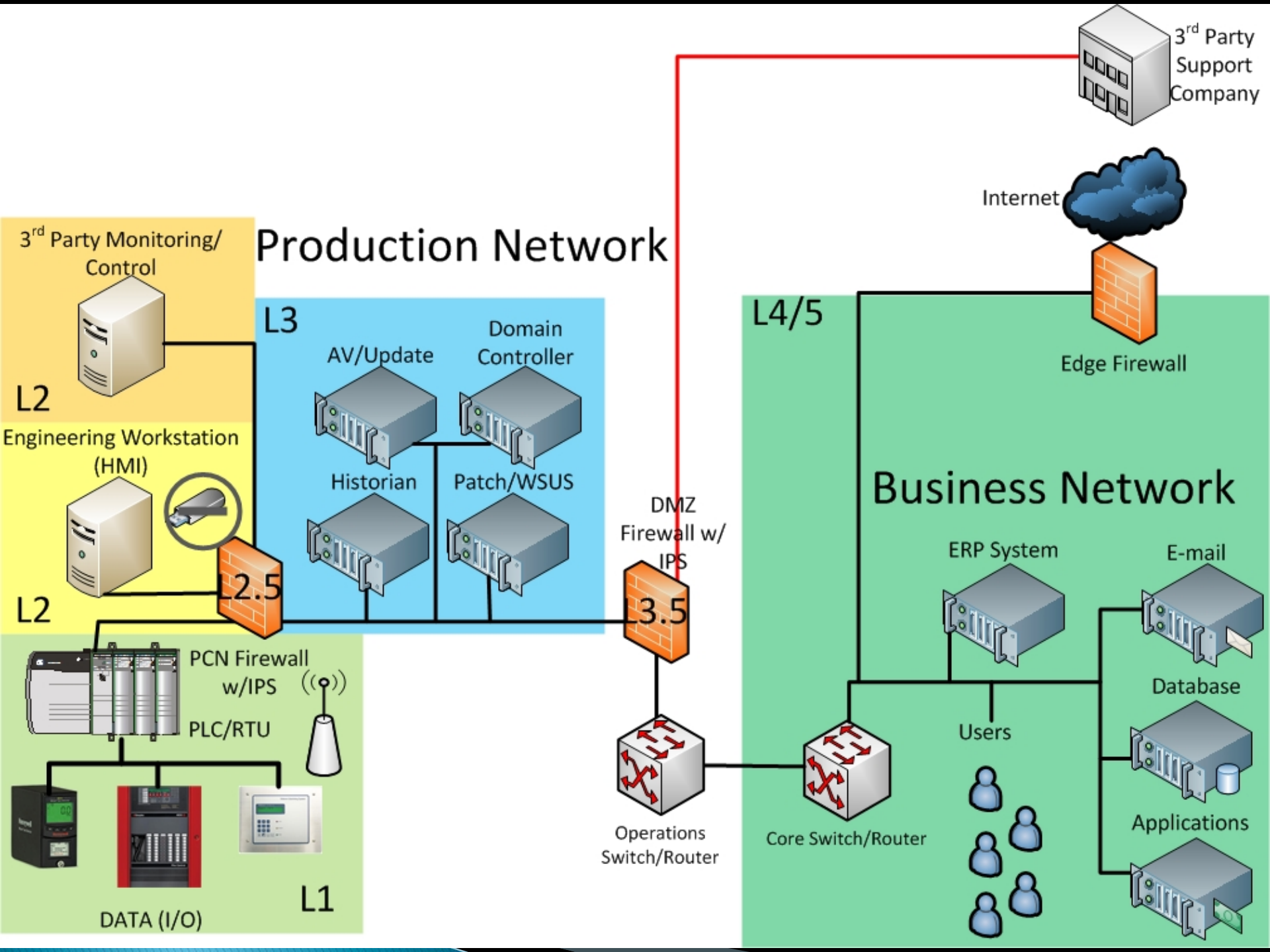
- ▶ ICS applications often misbehave
  - OPC (Object Linking and Embedding for Process Control) uses MS DCOM
  - They don't always communicate statefully
- ▶ Protocols have been subverted
  - MODBUS
  - DNP3
- ▶ Some vendors have started to adapt to ICS
  - Tofino (C1D2, DIN rail mount)
  - Palo Alto (Rack mount only for now)
- ▶ Do not install in blocking mode without extensive testing & tuning

# Patch management

- ▶ #1 thing that worries field personnel
  - ▶ Due to software issues, vendors **MUST** approve OS/app patches
  - ▶ Cannot patch monthly
  - ▶ Time for testing environment
- 

# Host-based security

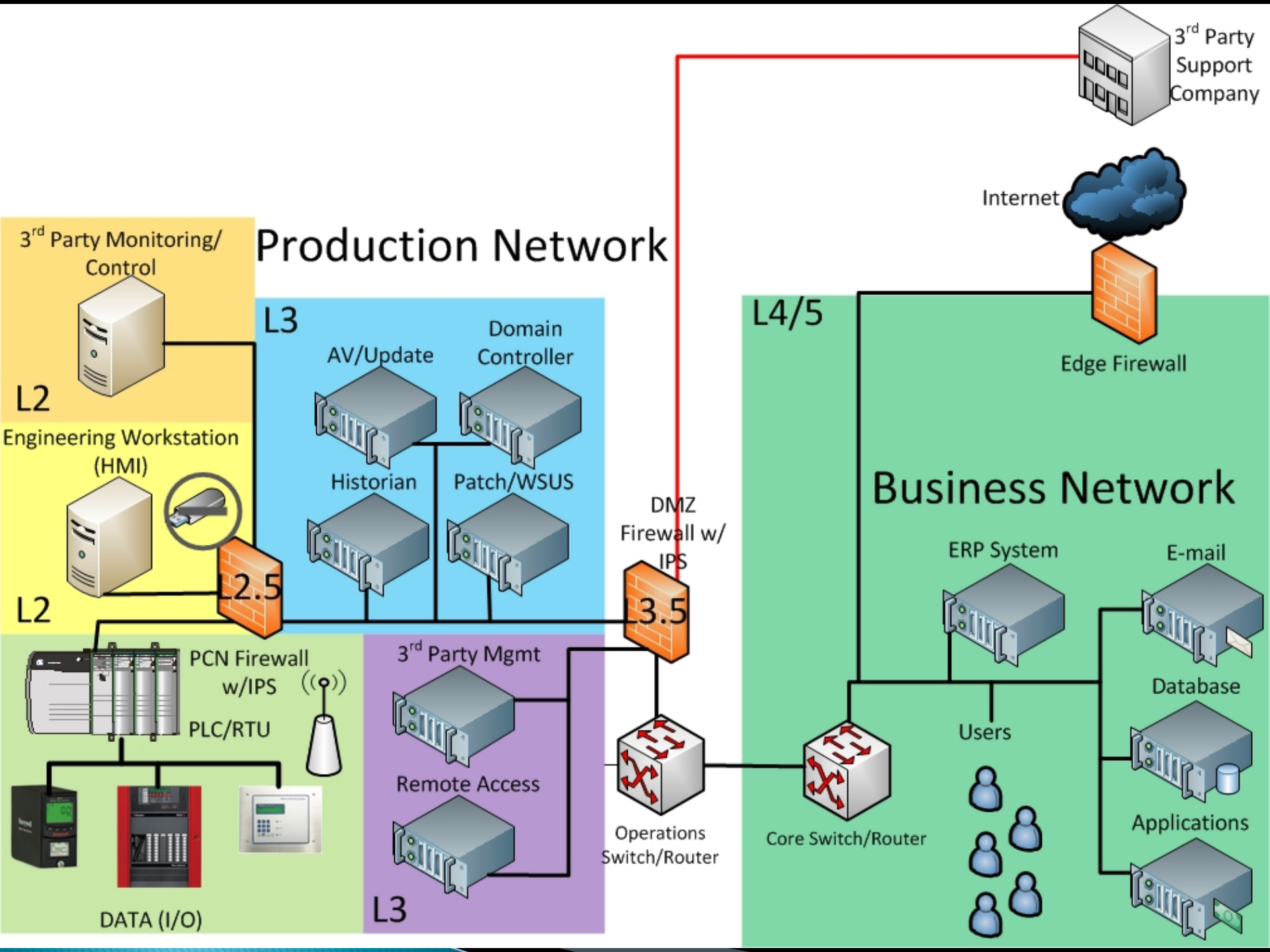
- ▶ USB & removable media control
- ▶ Anti-virus / anti-malware
- ▶ Application whitelisting
- ▶ Patch management for EWS & servers
- ▶ Corporate IT has these systems, BUT
  - ICS cannot patch as frequently
  - Application & OS security models differ
  - Dependent on directory services (AD)
- ▶ Build your own!



# 3<sup>rd</sup> party & remote access

- ▶ Like enterprise IT, ICS requires remote support and maintenance
- ▶ There have been breaches from this
  - Telvent
  - Target
- ▶ Vendors often will not recommend a security architecture
- ▶ Build your own!





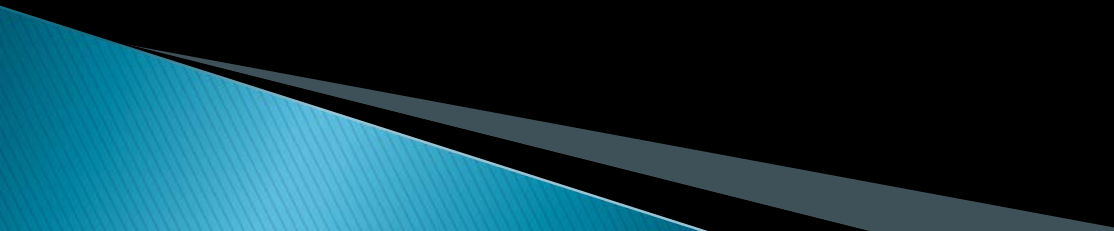
# When it goes wrong

- ▶ Incident response requires DATA
  - Centralized logging
  - Traffic analysis
  - Logstash, elasticsearch, and cacti
- ▶ Restoring PLC programming or device configs can be difficult
- ▶ Specialized ICS Configuration Management software exists
  - MDT AutoSave
  - Siemens TeamCenter

# Training / Certifications

- ▶ Specific ICS security trainings & certifications are uncommon
  - SANS/GIAC
  - Idaho National Laboratory (INL)
- ▶ 3<sup>rd</sup> Party Training
  - Offered by consulting/services companies
- ▶ Blends Infosec with ICS sensitivities
- ▶ Targeted for existing IT skillsets

# Disaster recovery considerations

- ▶ For some, DR is simply considered as having equipment spares on site
  - ▶ Ability to rapidly restore services may not be planned
  - ▶ Business impact analysis is key
  - ▶ Updated lists of vital assets and personnel must be maintained
- 

# Would you like to know more?

- ▶ My presentation from last year  
<http://evul.procfail.net/dc21/og-infosec-101.pdf>
- ▶ Co-workers' presentation from BH '13  
<https://media.blackhat.com/us-13/US-13-Fornier-Out-of-Control-Demonstrating-SCADA-Slides.pdf>
- ▶ Latest copy of these slides at  
<http://evul.procfail.net/dc22/protecting-scada-101.pdf>

# Questions?

- ▶ [aaron@procfail.net](mailto:aaron@procfail.net)
  - ▶ @AlxRogan
  - ▶ Visit the ICS Village, lots to explore and learn!
- 

# References

- ▶ Telvent breach – <http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/>
- ▶ MDT AutoSave – <http://www.mdt-software.com/Products/AutoSaveFeatures.html>
- ▶ Siemens TeamCenter – [http://www.plm.automation.siemens.com/en\\_us/products/teamcenter/](http://www.plm.automation.siemens.com/en_us/products/teamcenter/)
- ▶ Logstash & Elasticsearch – Log aggregation, searching, and visualization <http://www.elasticsearch.org/overview/>
- ▶ Cacti – Network statistics (and much more) graphing – <http://cacti.net>
- ▶ DNP3 – <http://www.digitalbond.com/blog/2013/10/16/why-crain-sistrunk-vulns-are-a-big-deal/>