Protecting SCADA From the Ground Up

Aaron Bayles

DC101 @ DEF CON 22

whoami && id

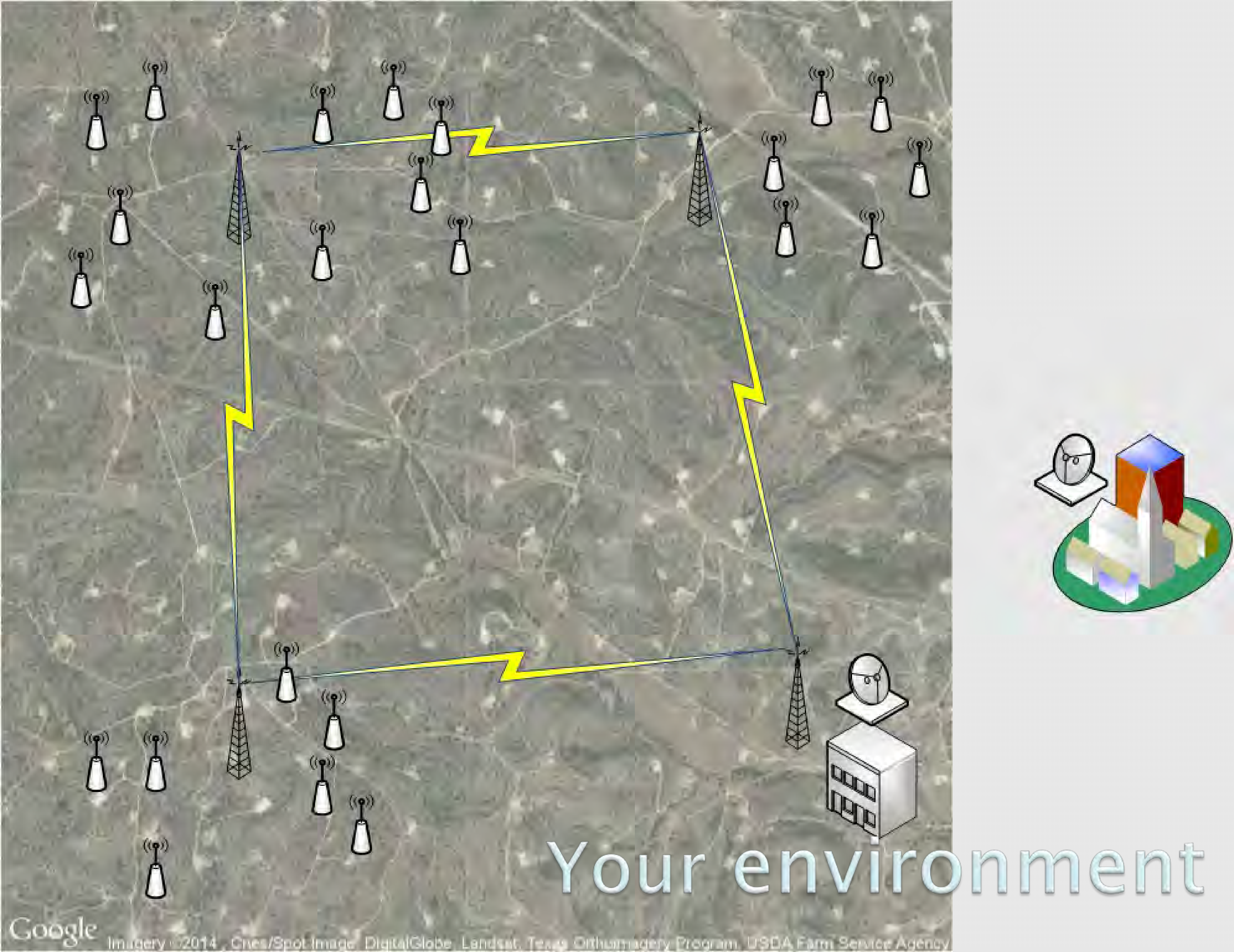
- 19 years in IT/Infosec
- Worked in Oil & Gas (O&G) last 8 years
- Along the way
  - Penetration testing
  - Vulnerability assessment
  - Network architecture, design & implementation
  - Risk assessment

What’s the problem?

- Legacy equipment/comms
- Remote (geographic) connectivity
- Long lifecycle
- 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

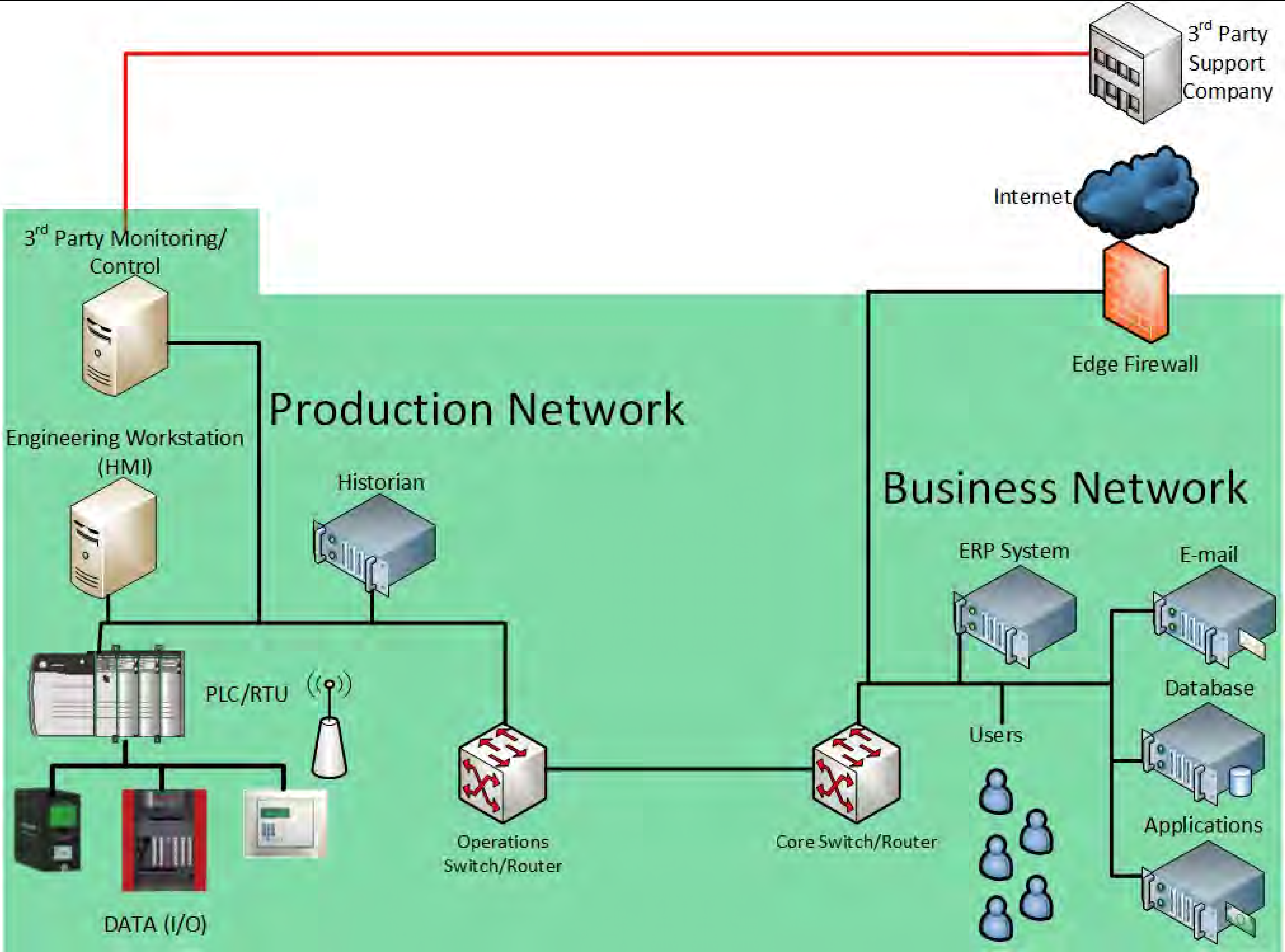
Your environment



Imagery ©2014 , Cnes/Spot Image, DigitalGlobe, Landsat, Texas Orthoimagery Program, USDA Farm Service Agency

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


3rd Party Support Company
Internet
Edge Firewall
3rd Party Monitoring/ Control
Production Network
Engineering Workstation (HMI)
Historian
Business Network
ERP System
E-mail
PLC/RTU
Database
Users
Applications
Operations Switch/Router
Core Switch/Router
DATA (I/O)

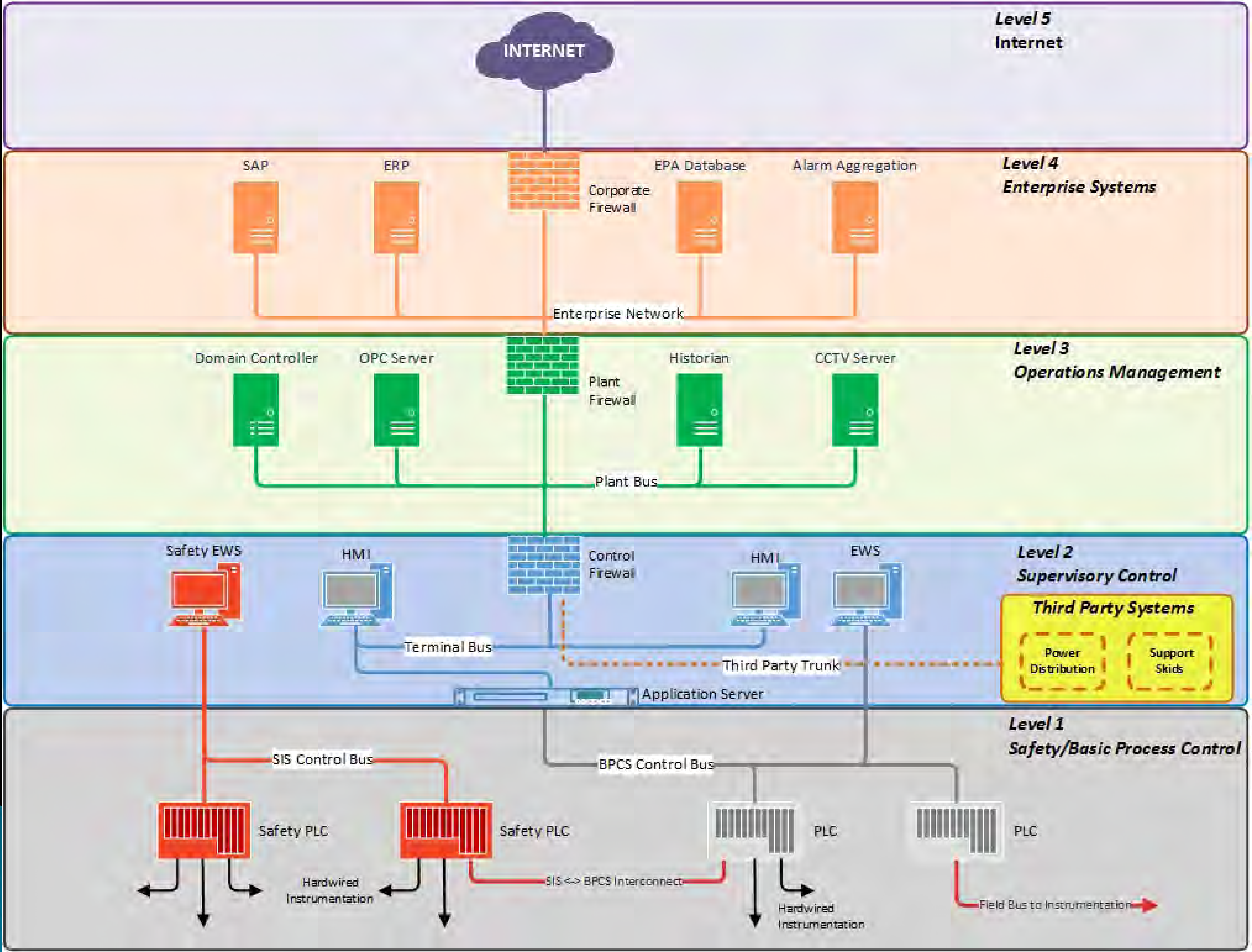
Best practices

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

Although these may be similar, significant differences exist

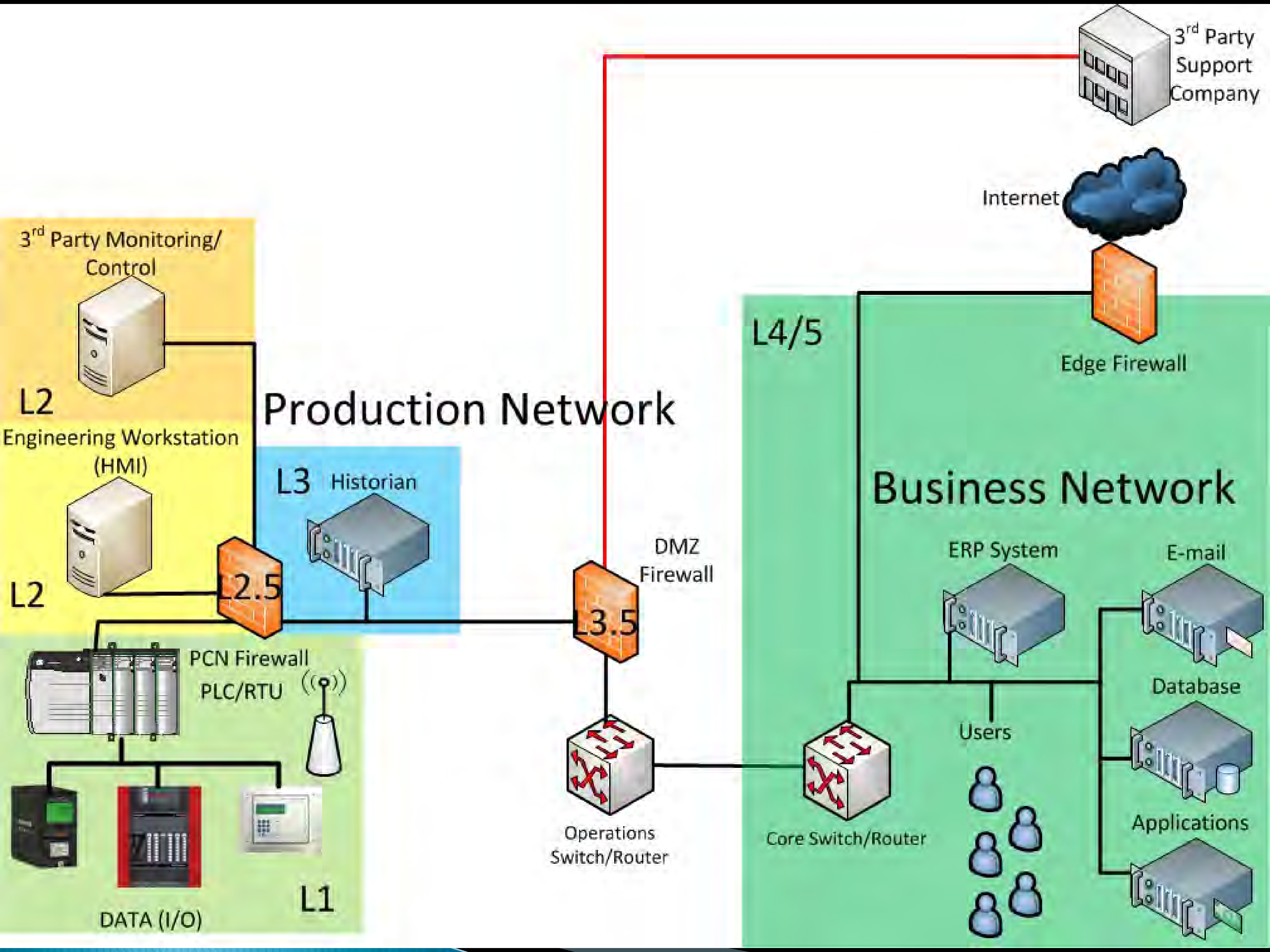
The Purdue Model

- 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


Level 5
Internet
INTERNET
Level 4
Enterprise Systems
SAP
ERP
Corporate Firewall
EPA Database
Alarm Aggregation
Enterprise Network
Level 3
Operations Management
Domain Controller
OPC Server
Plant Firewall
Historian
CCTV Server
Plant Bus
Level 2
Supervisory Control
Safety EWS
HMI
Control Firewall
HMI
EWS
Third Party Systems
Power Distribution
Support Skids
Terminal Bus
Third Party Trunk
Application Server
Level 1
Safety/Basic Process Control
SIS Control Bus
BPCS Control Bus
Safety PLC
Safety PLC
PLC
PLC
Hardwired Instrumentation
SIS <-> BPCS Interconnect
Hardwired Instrumentation
Field Bus to Instrumentation

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

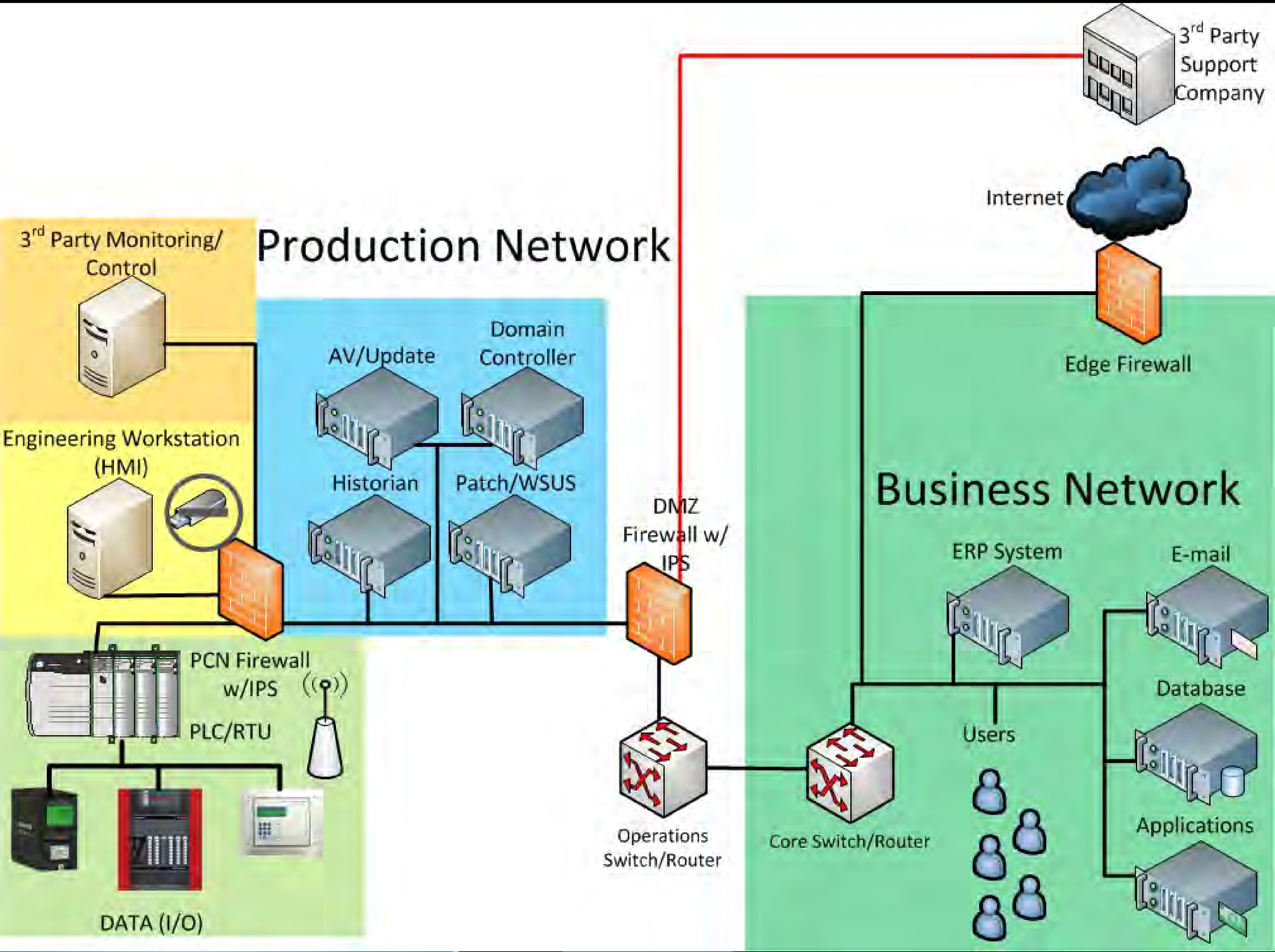

3rd Party Support Company
Internet
Edge Firewall
L4/5
Business Network
ERP System
E-mail
Database
Applications
Users
Core Switch/Router
Production Network
3rd Party Monitoring/ Control
L2
Engineering Workstation (HMI)
L2
L2.5
L3
Historian
DMZ Firewall
L3.5
PCN Firewall
PLC/RTU
Operations Switch/Router
DATA (I/O)
L1

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

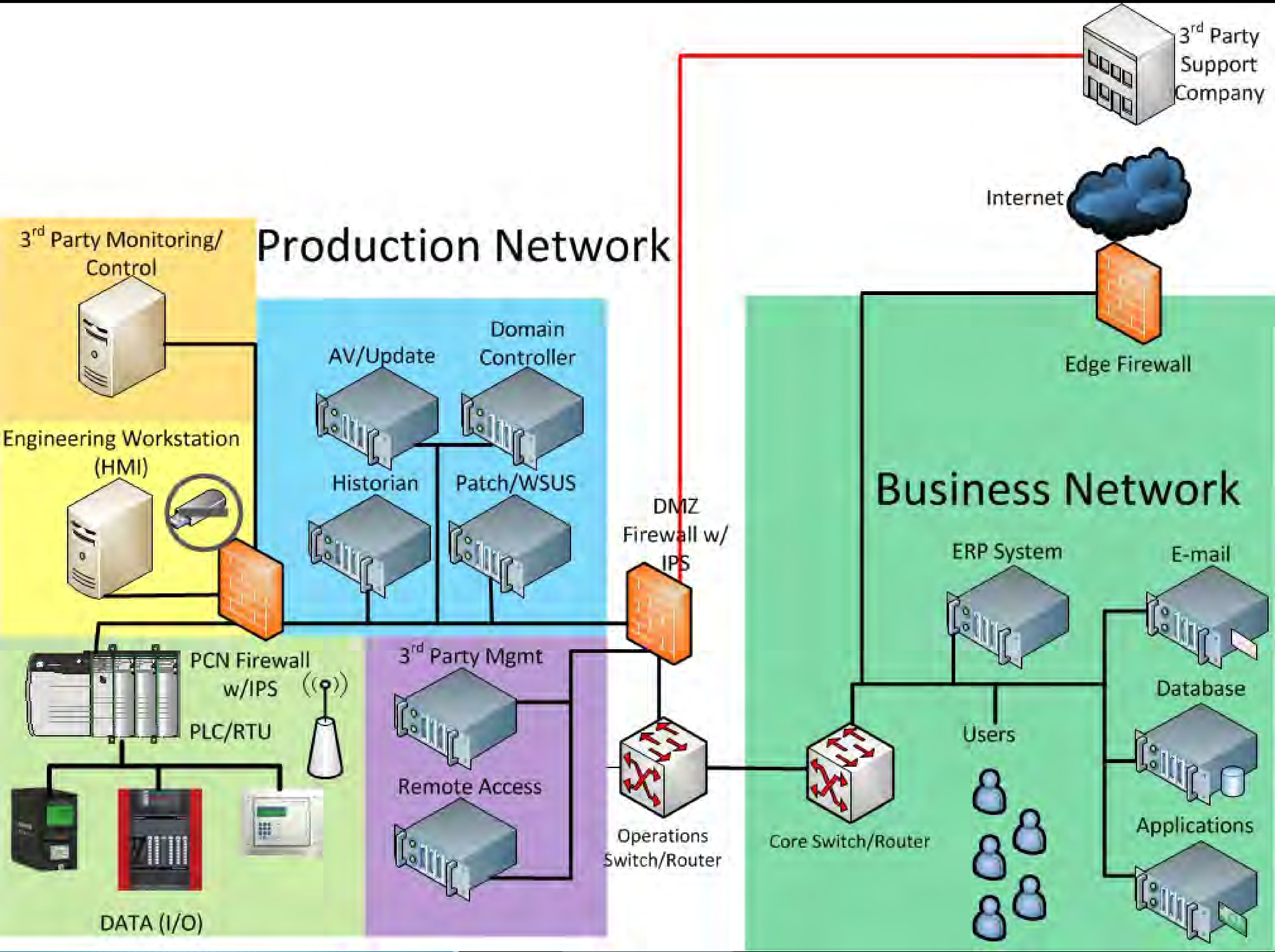
Host-based security

- 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!


3rd Party Support Company
Internet
3rd Party Monitoring/ Control
Production Network
Domain Controller
AV/Update
Edge Firewall
Engineering Workstation (HMI)
Historian
Patch/WSUS
Business Network
DMZ Firewall w/ IPS
ERP System
E-mail
PCN Firewall w/IPS
PLC/RTU
Database
Users
Applications
Operations Switch/Router
Core Switch/Router
DATA (I/O)

3rd 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!


3rd Party Support Company
Internet
Production Network
3rd Party Monitoring/ Control
Domain Controller
AV/Update
Edge Firewall
Engineering Workstation (HMI)
Historian
Patch/WSUS
Business Network
DMZ Firewall w/ IPS
ERP System
E-mail
PCN Firewall w/IPS
3rd Party Mgmt
Database
PLC/RTU
Users
Remote Access
Applications
Operations Switch/Router
Core Switch/Router
DATA (I/O)

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)
- 3rd 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-Forner-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
- @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/
- 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/