Setting the Standard for Automation™

Mitigating Cybersecurity Risk to Life Science Manufacturing

Standards

Certification

Education & Training

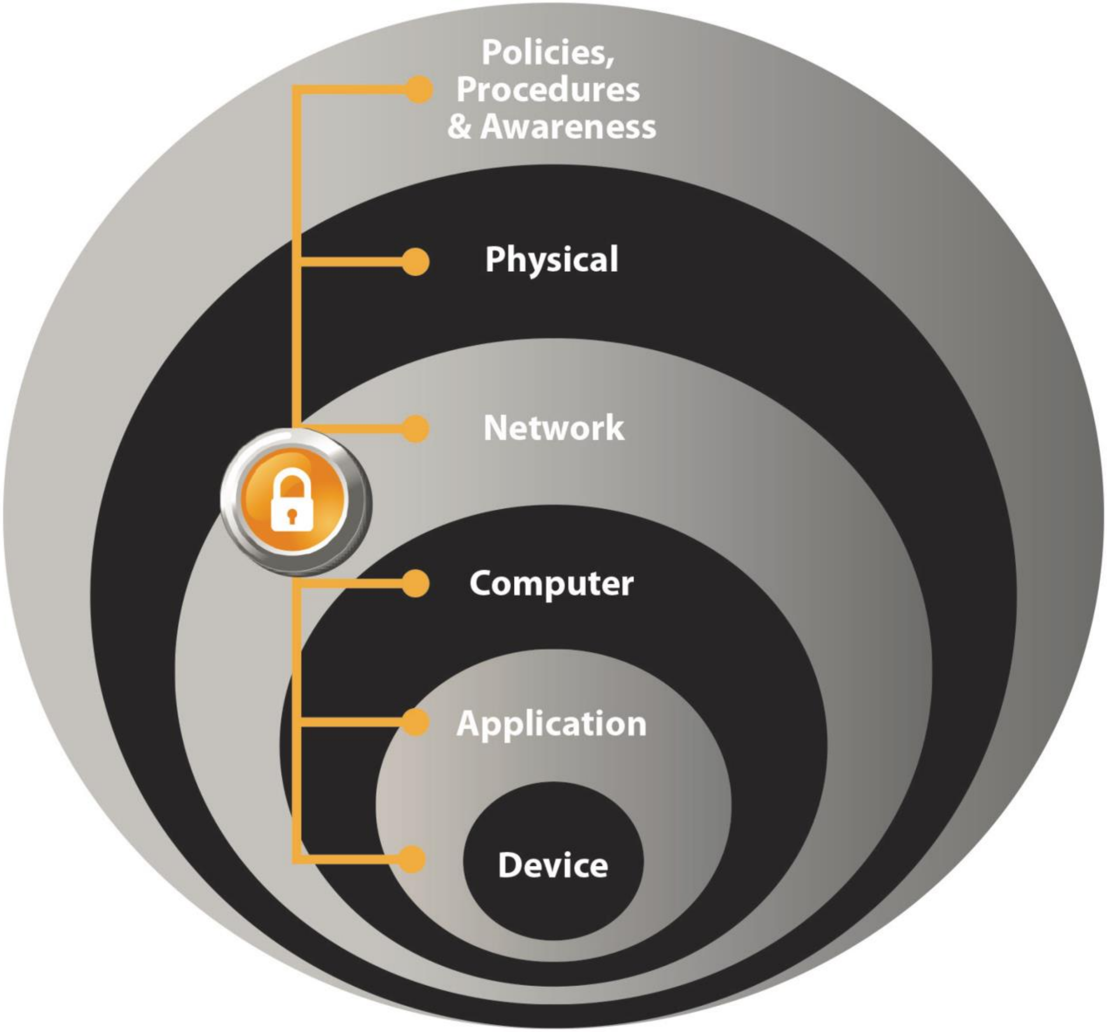
Publishing

Conferences & Exhibits

Presenter – Jim LaBonty

- 2007- Present : Pfizer Global Engineering - overseeing Process Automation and control system projects at Pfizer Biotech and Aseptic global manufacturing sites
- 2001-2007: Rockwell Automation - Life Science project team lead and Sr. System Architect (MES – Control Systems)
- Prior 20 years: Eastman Kodak - IT & Automation division head for Color Film Operations at Kodak Park.

Integrated Layers of Defense



Key Takeaway:

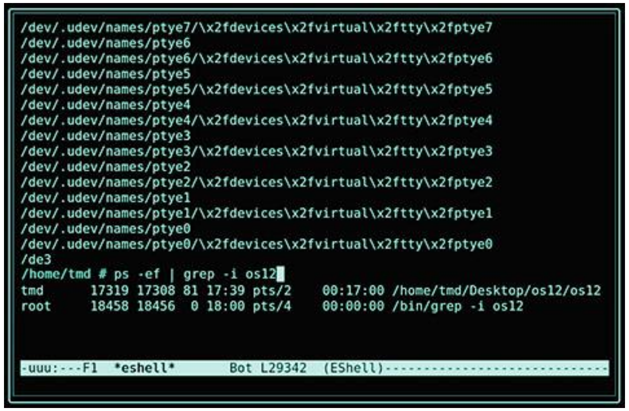
No Single product, methodology or technology can secure Control System Applications

Integrated Manufacturing Infrastructure Mitigating Security Risks

Security Risk: It is not a matter of When – it is much more a matter How one contains and limits the impact of Cyber-security risk!

Business Driver - Automation System Security

Even though Automation Technology (AT) has been the mythical target of many pop culture hacks and prior movie portrayals, until fairly recent the real world experience relative to automation systems security issues has been relatively few.



```
/dev/.udev/names/ptye7/\x2fdevices\x2fvirtual\x2ftty\x2fptye7
/dev/.udev/names/ptye6
/dev/.udev/names/ptye6/\x2fdevices\x2fvirtual\x2ftty\x2fptye6
/dev/.udev/names/ptye5
/dev/.udev/names/ptye5/\x2fdevices\x2fvirtual\x2ftty\x2fptye5
/dev/.udev/names/ptye4
/dev/.udev/names/ptye4/\x2fdevices\x2fvirtual\x2ftty\x2fptye4
/dev/.udev/names/ptye3
/dev/.udev/names/ptye3/\x2fdevices\x2fvirtual\x2ftty\x2fptye3
/dev/.udev/names/ptye2
/dev/.udev/names/ptye2/\x2fdevices\x2fvirtual\x2ftty\x2fptye2
/dev/.udev/names/ptye1
/dev/.udev/names/ptye1/\x2fdevices\x2fvirtual\x2ftty\x2fptye1
/dev/.udev/names/ptye0
/dev/.udev/names/ptye0/\x2fdevices\x2fvirtual\x2ftty\x2fptye0
/de3
/home/tmd # ps -ef | grep -i os12
tmd       17319 17308 81 17:39 pts/2    00:17:00 /home/tmd/Desktop/os12/os12
root      18458 18456  0 18:00 pts/4    00:00:00 /bin/grep -i os12


-uuu:---F1  *eshell*       Bot L29342  (EShell)---------------------------
```

The War on Automation Infrastructure Has Started

External Industry Examples…the last ten+ years

- In 2000, Vitek Boden, a 48-year-old man fired from his job at a sewage-treatment plant in Australia, remotely accessed his former workplace's computers and poured toxic sludge into parks and rivers; he had hoped the plant would re-hire him!
- In 2007, Scott Lunsford, a researcher for IBM's Internet Security Systems, offered to hack into a nuclear power station. "It turned out to be one of the easiest penetration tests I'd ever done," he says. "The 1st day, we had penetrated the network. Within a week, we were controlling a nuclear power plant. I thought, 'Gosh. This is a real big problem.'"
- Cyber Incident blamed for Nuclear Power Plant Shutdown. A nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours, after an automated software update was installed on a single computer.
- A Harrisburg, Pennsylvania, water treatment plant was accessed in early October, 2006, an employee's laptop computer was compromised via the Internet, and used as an entry point to install virus and spyware on the plant's computer system.
- January 8, 2008 –Teenage boy 'hacks' into the track control system of the Lodz city tram system, derailing four vehicles. Boy had adapted a television remote control so it could change track switches.
- In 2003, Slammer worm crashed Toledo Ohio nuke plant network .
- In 2000, Hackers cracked Gazprom security, controlled gas-flow switchboard, "We were very close to a major natural disaster."
- In 2007, an intruder installed unauthorized software and damaged the SCADA computer used to divert water from the Sacramento CA river.
- In 2008, CIA has information that cyber intrusions into Utilities (followed by extortion demands) have been used to disrupt power equipment in several world regions outside the United States.
- In 2011, Stuxnet virus infect Siemens control systems via 4 zero day vulnerabilities!
- In 2012, Duqu spyware reconnaissance….get ready for the next in coming tidal wave!
- In 2012, Shamoon virus hits Saudi Aramco –> 30, 000+ office PC computers disrupted.
- In 2013, Million+ attempted attacks each day hit USA critical supply chain (gas, oil, chemical, food, infrastructure)
- In 2014, Large BioPharma in EU loses all their IT file shares for the whole corporation!
- In 2014, Hackers struck an unnamed steel mill in Germany. They did so manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, resulting in "massive"—though unspecified—damage.

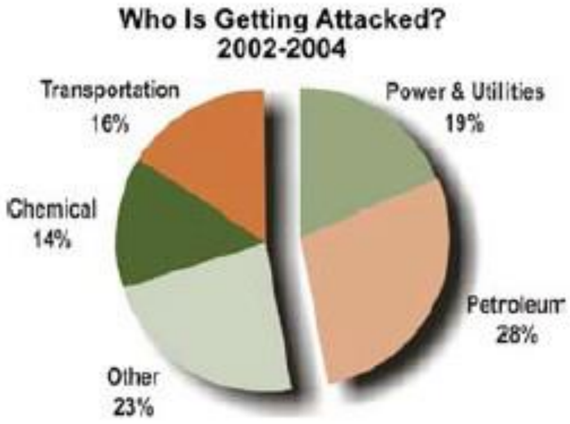
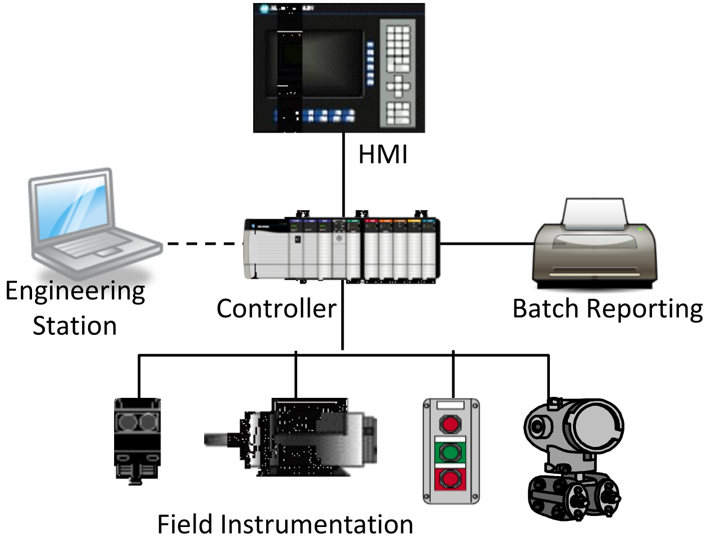


Exhibit 2.4 – Attacks on Industrial Control Systems

Source: Industrial Security Incident Database (Byres 2005)

Historical Security via Isolation & Obscurity



- Each piece of process equipment included its own isolated control system.
- No remote access of any kind – no possibility for remote hijacking systems.
- Engineering Station was only connected during troubleshooting or application change programming.
- All automation technology was very proprietary – no Ethernet, no Windows OS targets, etc.

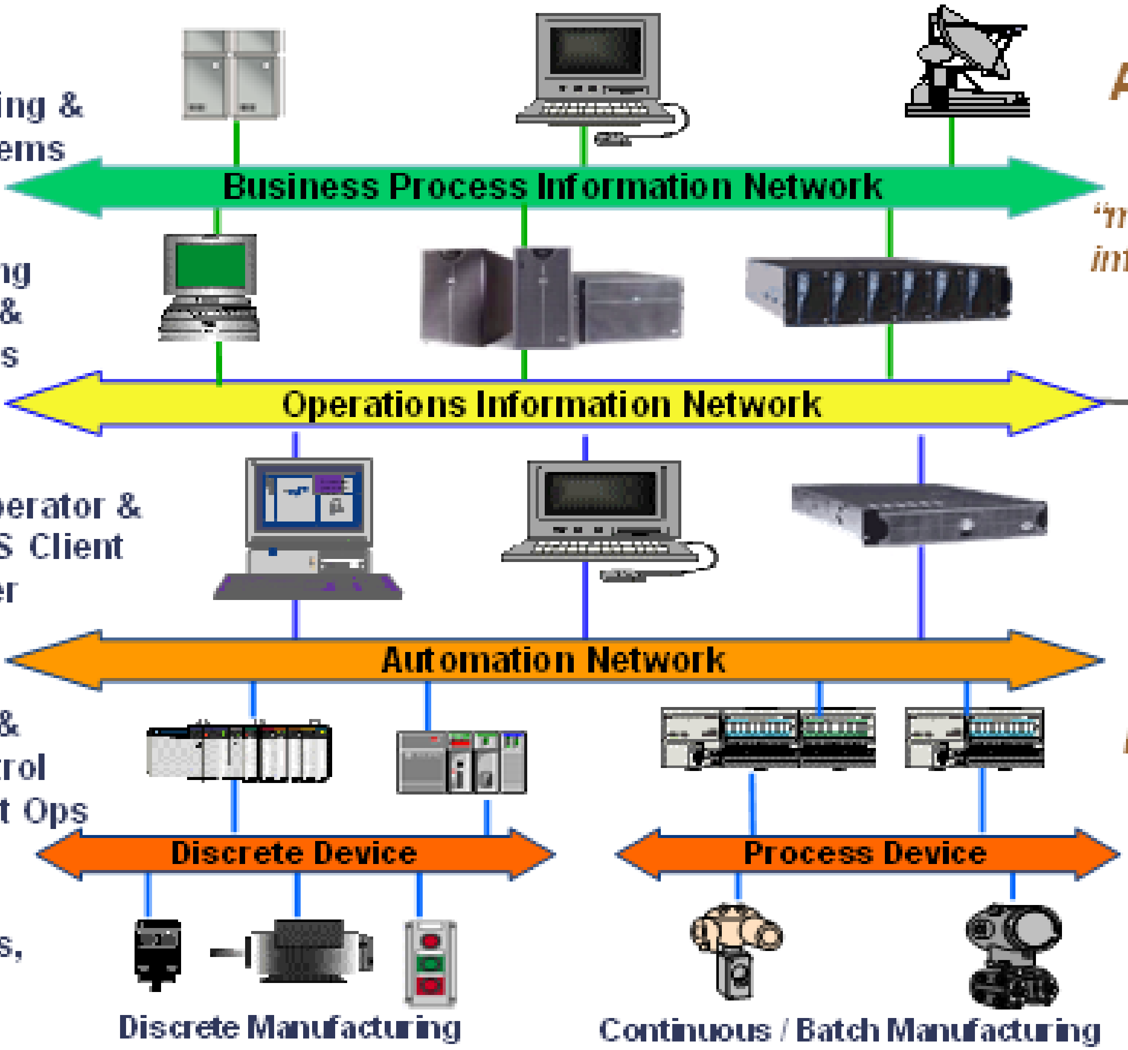
Historically, Automation Control Systems were quite secure via physical security isolation, but each “Automation Island” was information crippled.

The Manufacturing World today is quite Different (2001 vs. 2015) More than a Decade of Rapid Change …

- Automation Control Infrastructure is now becoming a hacker target
- Automation Connectivity- business needs are driving Integration
- Automation Technology (AT), definitely no longer proprietary
- Automation programming, no longer a niche engineering technology
- Automation Infrastructure, far too complex for a ‘hobbyist’ engineer
- Automation Technology and IT is absolutely *everywhere*!
- AT infrastructure is utilizing more and more IT infrastructure components and standard IT technologies
- Mfg. sites stop completely dead without Control Systems on-line!

Ever Increasing Manufacturing Business Risk year by year that needs to be managed properly …

System Architecture Model - Logical



LEVEL 4
Business Planning &
Logistics Systems

Business Process Information Network

LEVEL 3
Manufacturing
Operations &
Mgt Systems

Operations Information Network

LEVEL 2
Data Collection, Operator &
HMI Systems; DCS Client
Server Layer

Automation Network

LEVEL 1
Equipment &
Process Control
Systems for Unit Ops

Discrete Device

Process Device

LEVEL 0
I/O, Sensors,
Actuators

Discrete Manufacturing

Continuous / Batch Manufacturing

ASTM E2500

ASTM E2500:
"may also be applied to information (systems)"

Information
Systems

Process
Monitoring

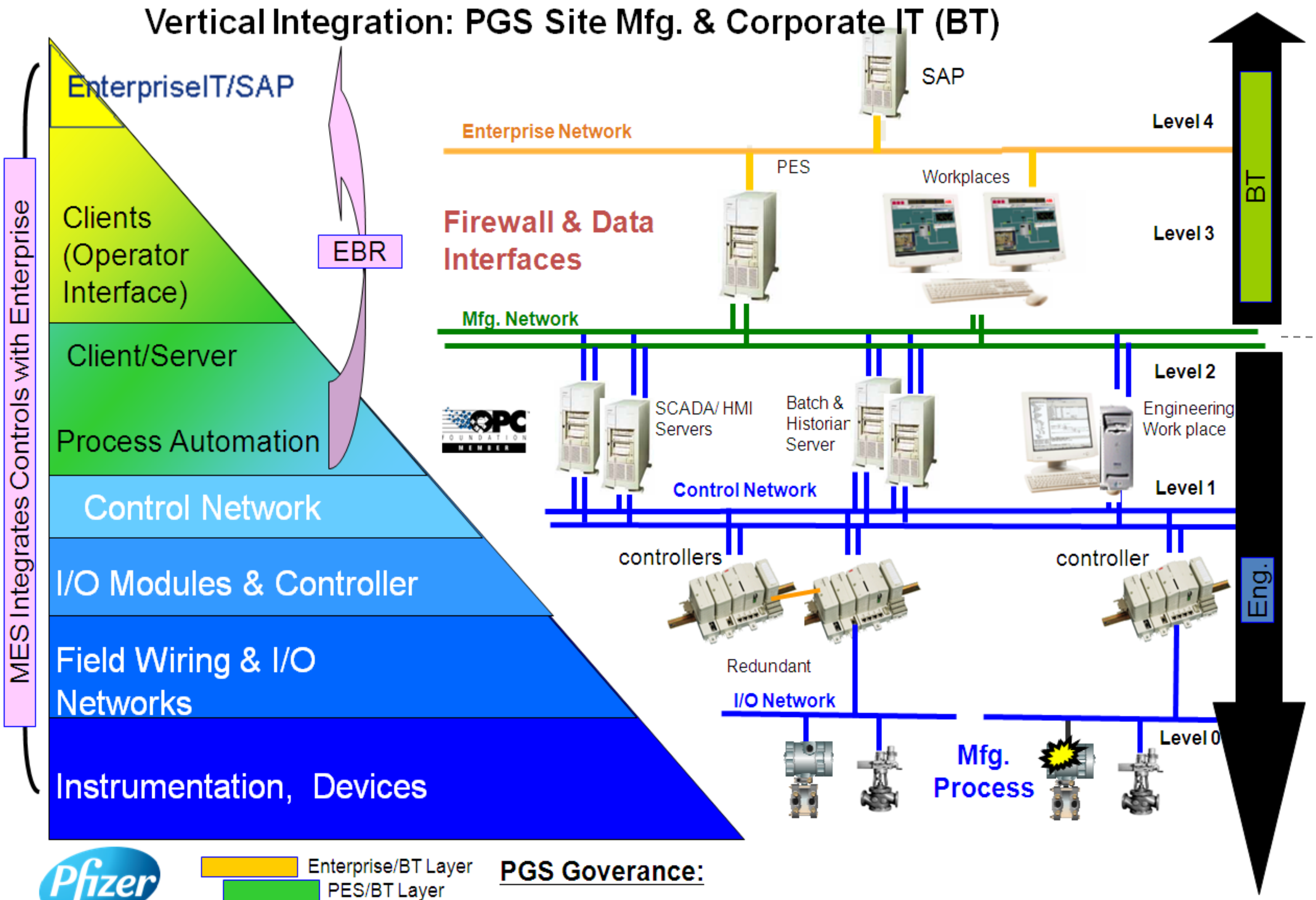
Control

Automation

ASTM E2500:

"is applicable to process monitoring and control systems and automation systems"

Integrated Manufacturing Systems



🟨 Enterprise/BT Layer

🟩 PES/BT Layer

PGS Goverance:

🟦 Process & Equipment Automation/ Site Engineering Layer

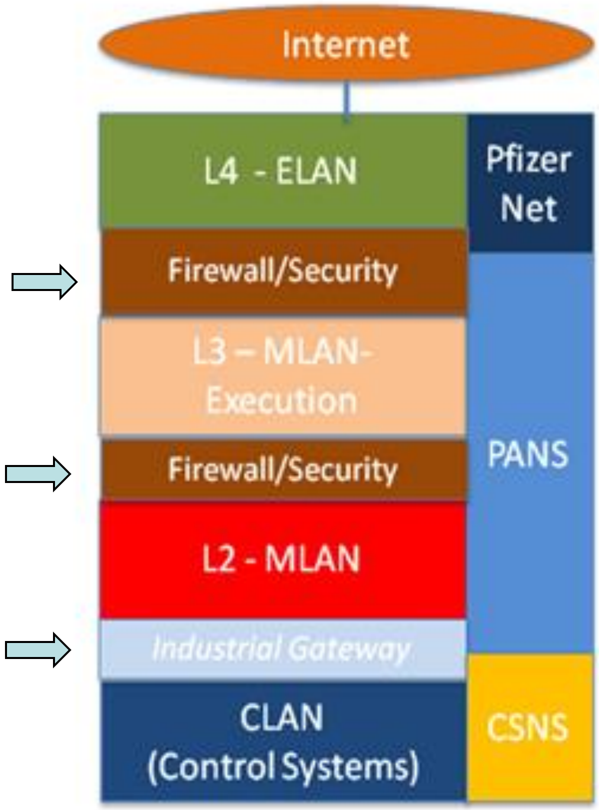
IT Systems

Follow an IT reinvestment strategy (typically 5-10 Years)

Control Systems

Follow each Mfg. site asset reinvestment strategy (typically 10-25 Years)

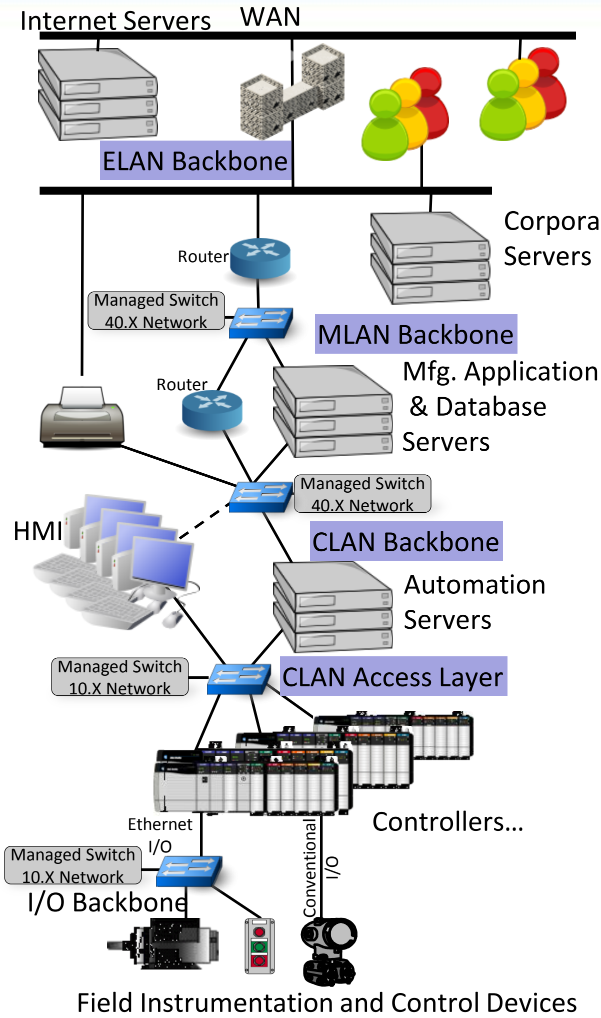
Layered Infrastructure - Defense-in-Depth



- Principle:
  - L4 ELAN : computer systems must have OS upgraded to supported OS.
  - L3 MLAN : OS patching / virus protection evaluated for business risk / protected by Firewall/ACL – more modern OS, support can lag
  - L2 MLAN: OS support / virus protection evaluated for business risk / protected by two Firewall/ACL, less modern OS, support lags over years
  - CLAN (control systems) evaluated for business risk. – generally unprotected PLCs and control systems due to legacy systems

Legend: ELAN = Enterprise LAN, MLAN = Manufacturing LAN, CLAN = Control System LANs

Automation Technology (AT): Security via Segregation by employing layered security methods

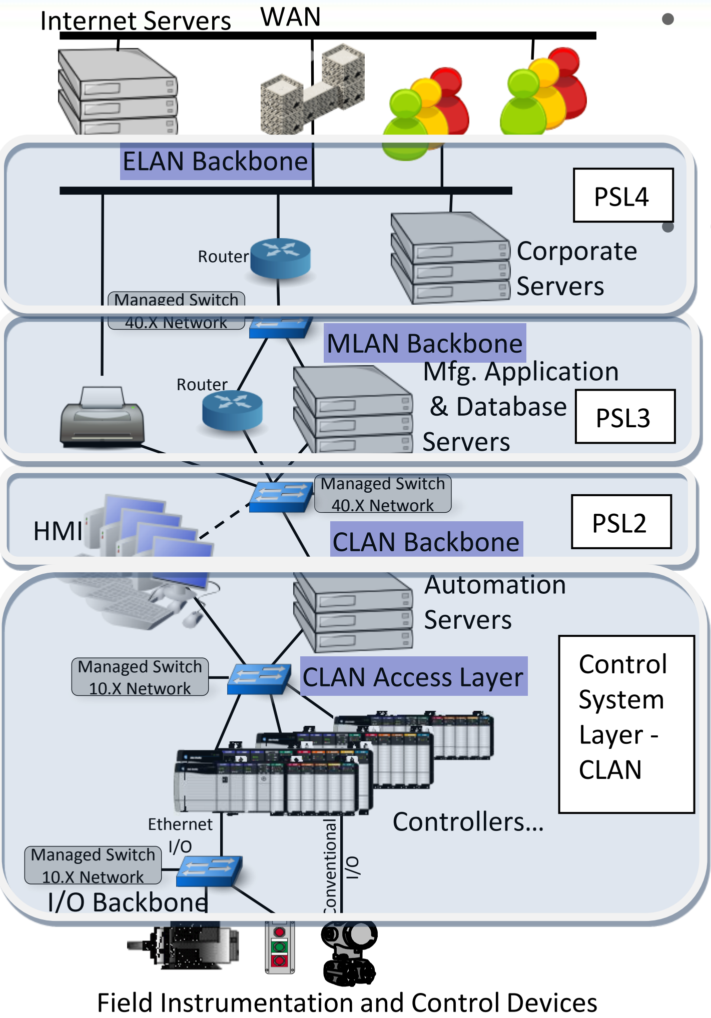


- Internet Servers:
  - Communications Servers (SMS)
  - Vendor Asset Management
  - Remote Access (VPN, etc)
- Corporate Servers:
  - Active Directory
  - ERP
  - MES System gateway
  - Citrix Servers
  - Analytics - global
  - LAN Drives
  - Backup/Recovery
  - CMMS
  - Time Servers
  - Domain Name Servers
  - Communications Servers (email)
  - SharePoint Portals
  - LIMS
  - Virtualized Servers (VMware)

- Mfg. Applications & Database Servers:
  - Continuous Data Historians
  - Batch Historians
  - Alarm Management Servers
  - OEE and Line Performance
  - PAT Analysis Systems
- Control System Servers:
  - Engineering Stations
  - App & Data Servers for
    - Process Historians and Data Collectors
    - HMI
    - Advanced Control (APC)
    - PAT Analysis
  - HMI Graphic Servers
  - Citrix Servers
  - Terminal Services Servers
  - Industrial Virtualization (VMware)
  - Industrial Virtualization (Hyper-V)
  - Other control systems…

Current AT architecture(s) facilitate dramatic increase in functionality: Mandatory for Manufacturing site objectives of Process Optimization, reduced Operating Costs, increased Utilization, increased Productivity and overall Safety.

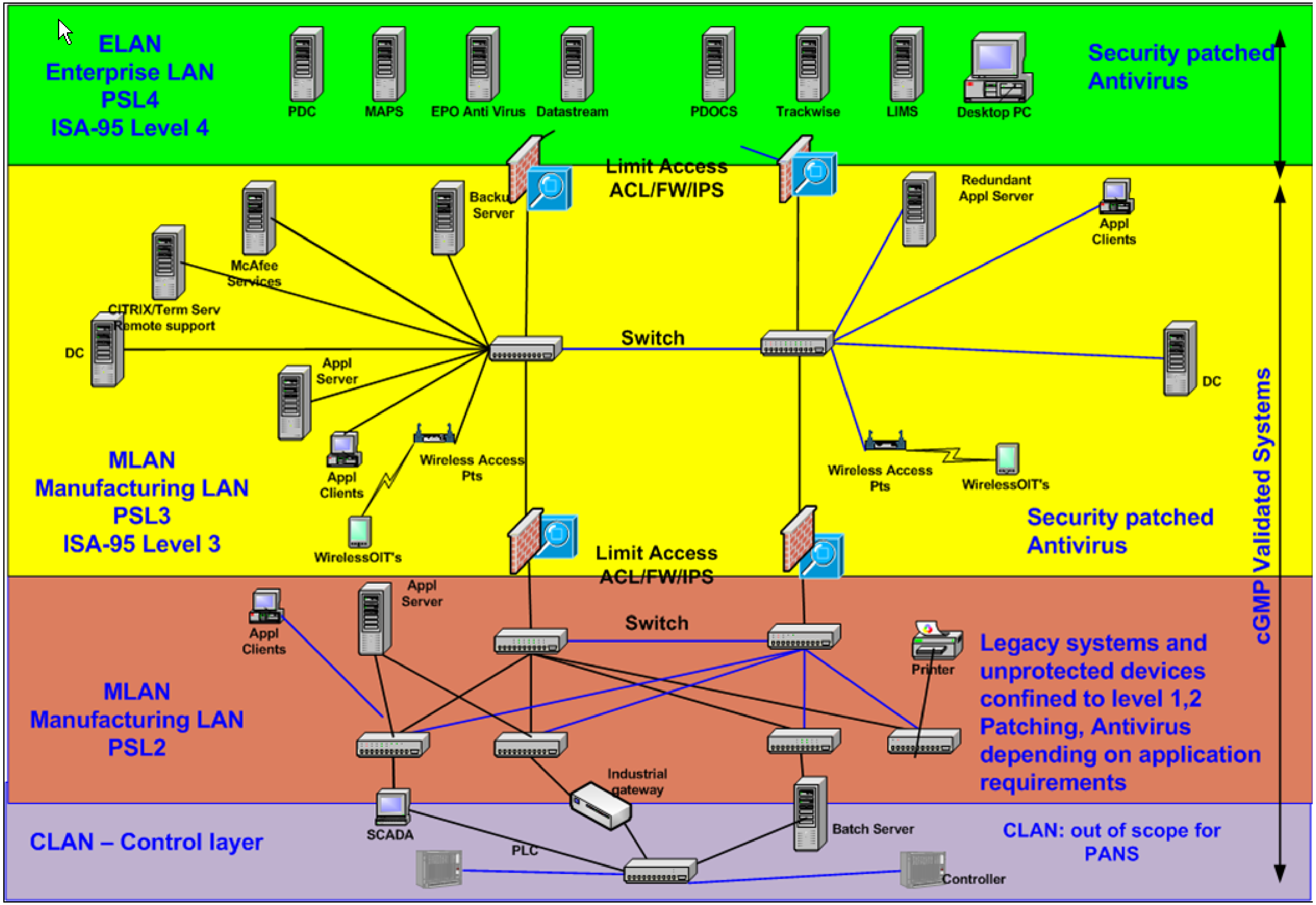
Automation Technology (AT): Security via Segregation by employing layered security methods



- Internet Servers:
  - Communications Servers (SMS)
  - Vendor Asset Management
  - Remote Access (VPN, etc)
- Corporate Servers:
  - Active Directory
  - ERP
  - MES Gateway
  - Citrix Servers
  - Catalyst
  - LAN Drives
  - Backup/Recovery
  - CMMS
  - Time Servers
  - Domain Name Servers
  - Communications Servers (email)
  - SharePoint Portals
  - LIMS
  - Virtual Servers (VMware)
- Mfg. App & Database Servers:
  - Continuous Data Historians
  - Batch Historians
  - Alarm Management Servers
  - OEE and Line Performance
  - PAT Analysis Systems
- Control System Servers:
  - Engineering Stations
  - App & Data Servers for
    - Process Historian and Data Collectors
    - HMI
    - Advanced Control (APC)
    - PAT Analysis
  - HMI Graphics Servers
  - Citrix Servers
  - Terminal Services Servers
  - Industrial Virtualization (VMware)
  - Industrial Virtualization (Hyper-V)
  - Other control systems…

Current AT architecture(s) facilitate dramatic increase in functionality: Mandatory for Manufacturing site objectives of Process Optimization, reduced Operating Costs, increased Utilization, increased Productivity and overall Safety.

Defense-in-Depth Network Architecture



ELAN
Enterprise LAN
PSL4
ISA-95 Level 4

Security patched
Antivirus

MLAN
Manufacturing LAN
PSL3
ISA-95 Level 3

Security patched
Antivirus

MLAN
Manufacturing LAN
PSL2

Legacy systems and unprotected devices confined to level 1,2
Patching, Antivirus depending on application requirements

CLAN – Control layer

CLAN: out of scope for PANS

ISA S95
Level 4

ISA S95
Level 3

ISA S95
Level 3/2

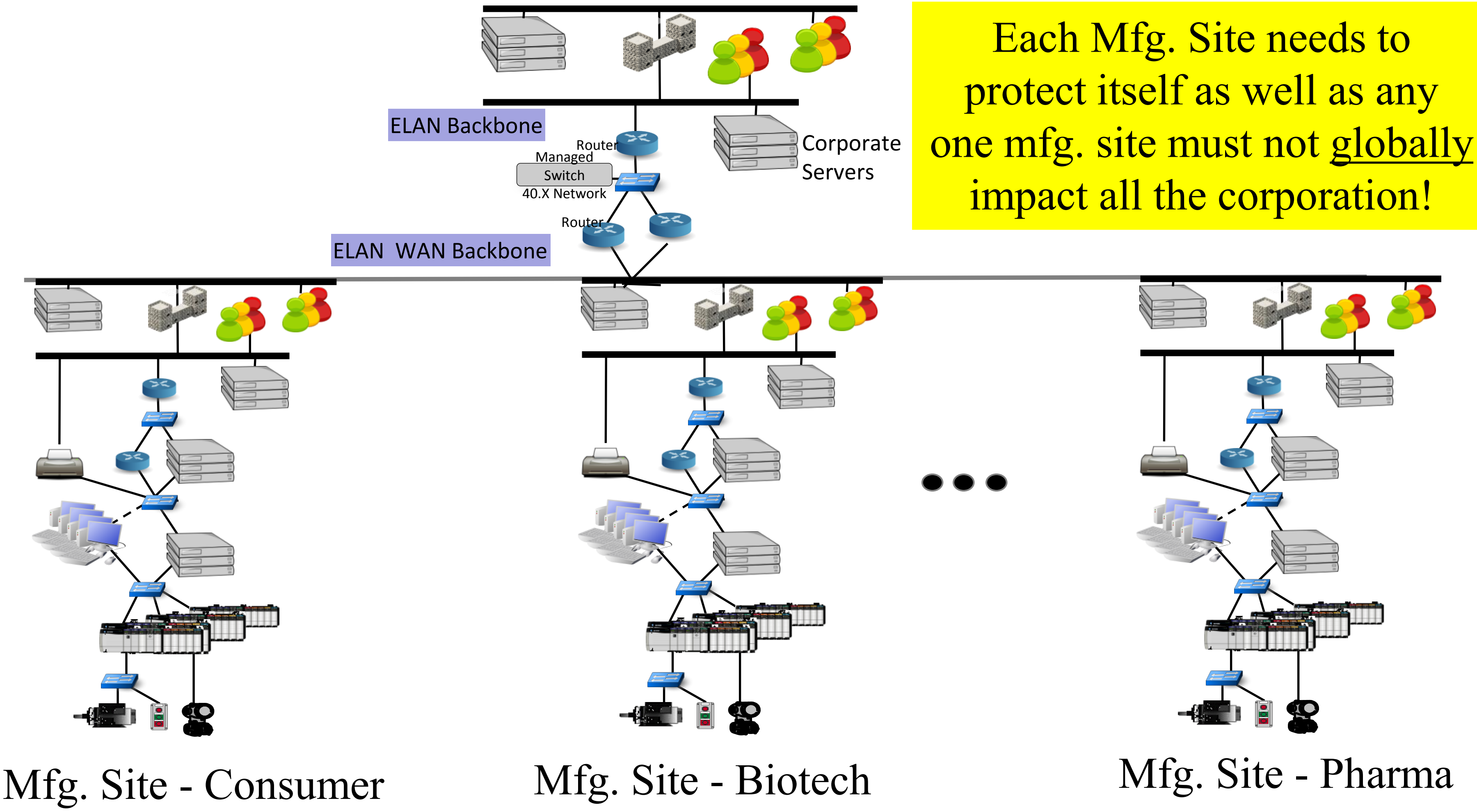
ISA S95
Level 2/1/0

Note: PSL stands for PANS Security Layer

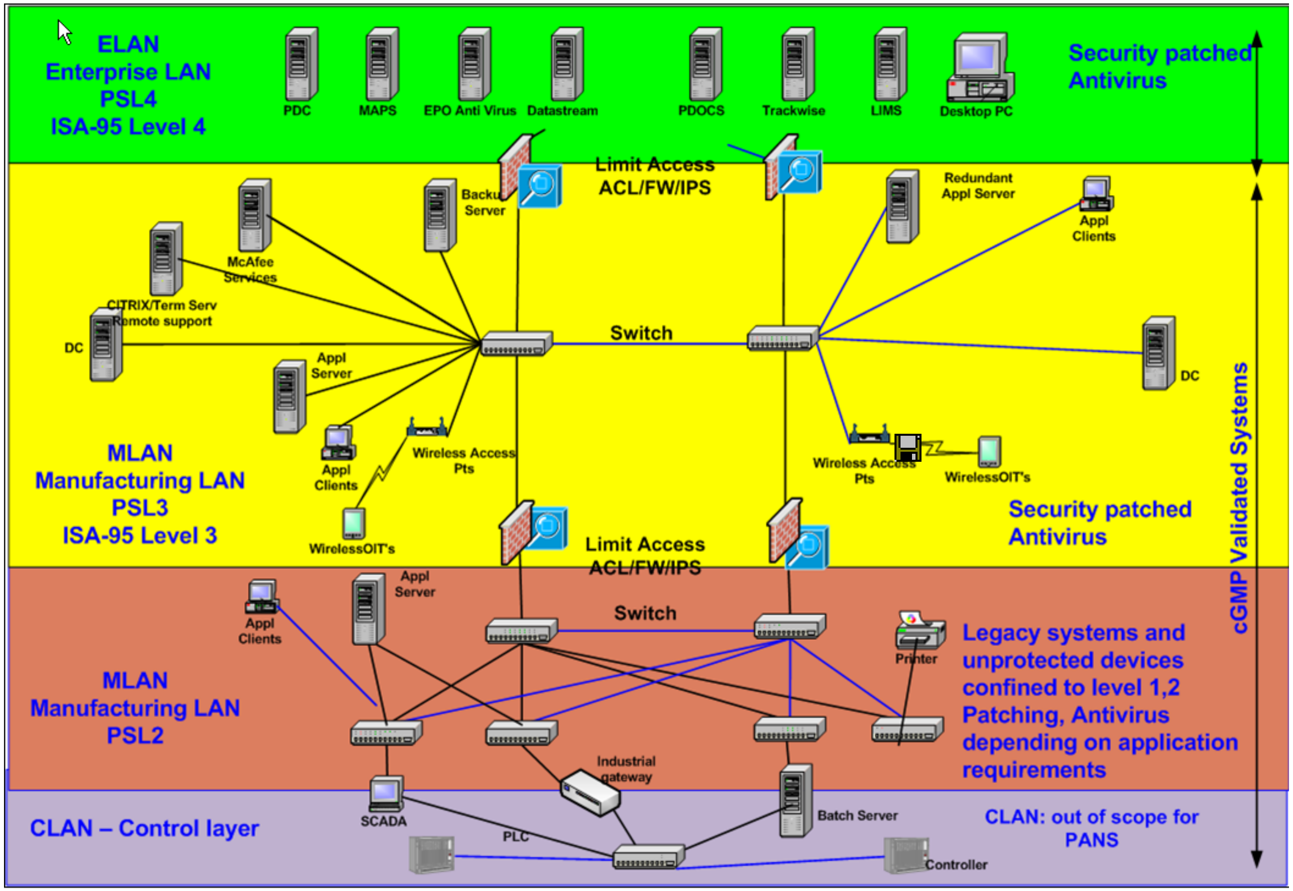
Global Enterprise : Security via Segregation

Employing layered security and defense-in-depth methods

Each Mfg. Site needs to protect itself as well as any one mfg. site must not globally impact all the corporation!



Network Infrastructure Architecture



Prior control network design philosophy was based on a ‘walled city’ paradigm – robust perimeter defense but weaker interior defense. An improved strategy for global site guidance is layered defense in depth security **plus** protected Cell/ Zone inner walls for control systems deployed based on business risk – an analogy sort of like ‘gated communities’.

Industrial Gateway – What is it?

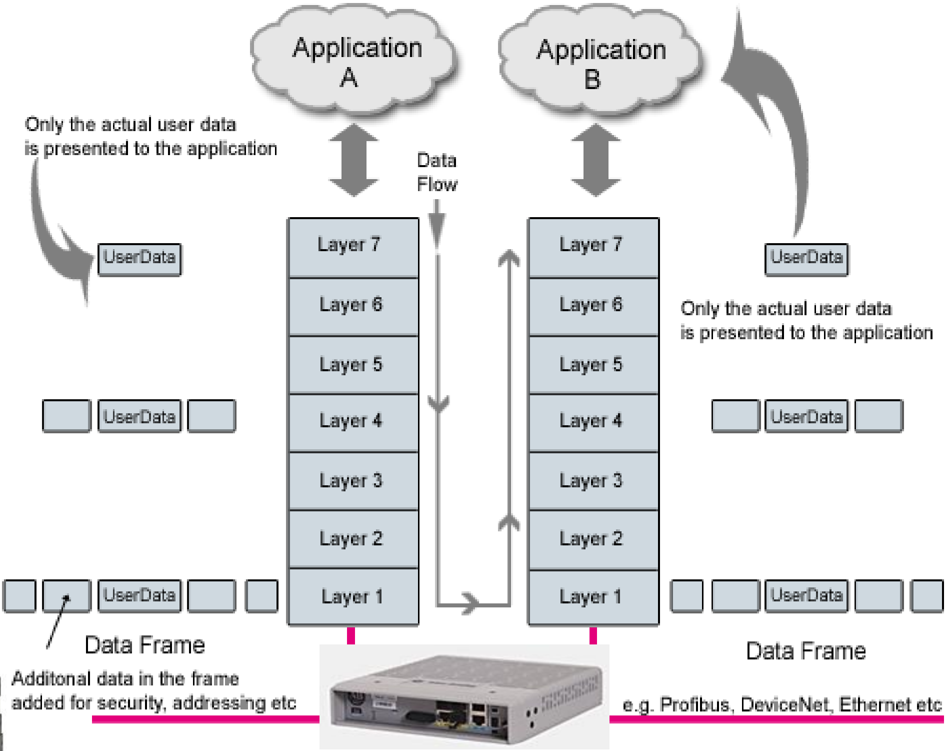
A basic *definition* of an industrial gateway is a network device capable of joining together two networks that use <u>different base protocols</u>.

Fully IPv6 compliant

MLAN

<u>Business IT protocols:</u>
TCP/IP
UDP

<u>Access Layer Switch (MLAN Layer 2)</u>



Application A
Application B
Only the actual user data is presented to the application
Data Flow
UserData
Layer 7
Layer 6
Layer 5
Layer 4
Layer 3
Layer 2
Layer 1
Only the actual user data is presented to the application
Data Frame
Additonal data in the frame added for security, addressing etc
Data Frame
e.g. Profibus, DeviceNet, Ethernet etc

<u>Industrial Gateway(s)</u>

Typically not IPv6 compliant

<u>Industrial IT protocols:</u>
TCP/IP
UDP
ProfiNet
CIP
EtherNet/ IP
Modbus IP
WirelessHart
EtherCAT
DeviceNet
Etc.

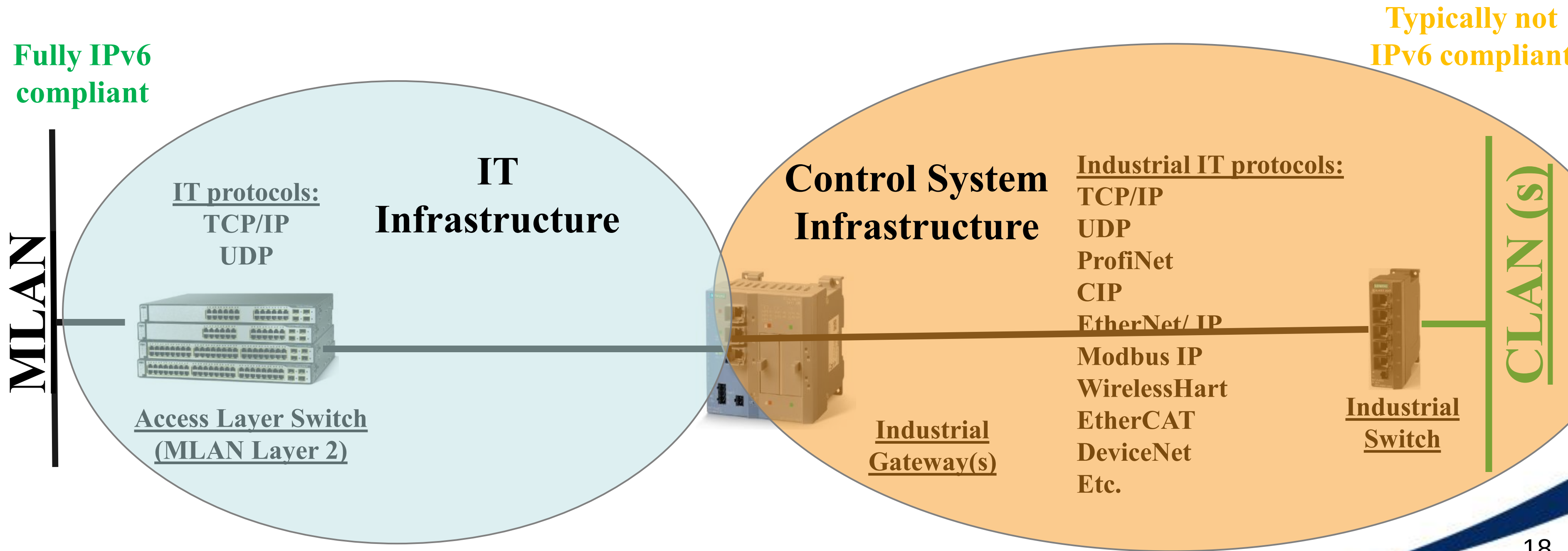
<u>Industrial Switch (CLAN)</u>

CLAN (s)

Industrial Gateway – Business Benefits?

Business Value of an Industrial Gateway Device to a Manufacturing site:

- **Enables Data and Information flow with Control System devices/ components**
- **Security built-in when connecting control system platform(s) with IT network infrastructure (enabling “Gated Communities”)**
- **Enables global support to access the control system platform, remotely**
- **Support, Configuration, Change and Management by local site Automation Engineering**
- **Enables encapsulation of well-aged control system technology and/or no longer supported Operating Systems (ex. Microsoft NT, W2000, XP, etc.)**



Questions ?

THANK YOU
FOR YOUR
ATTENTION
AND THANKS
FOR LISTENING!!!