PROCESS CONTROL SYSTEMS FORUM

Secure Network Architectures for Control Systems

March 7, 2007
Andrew Wright
andwrigh@cisco.com
Critical Infrastructure Assurance Group
CISCO

Agenda

- **Control Systems Security**
  - control systems
  - technology trends
  - new security threats
  - differences from enterprise networks
- **Cisco Secure Architectures for Control**
  - logical view
  - DMZ design
  - control zone designs
  - status & future

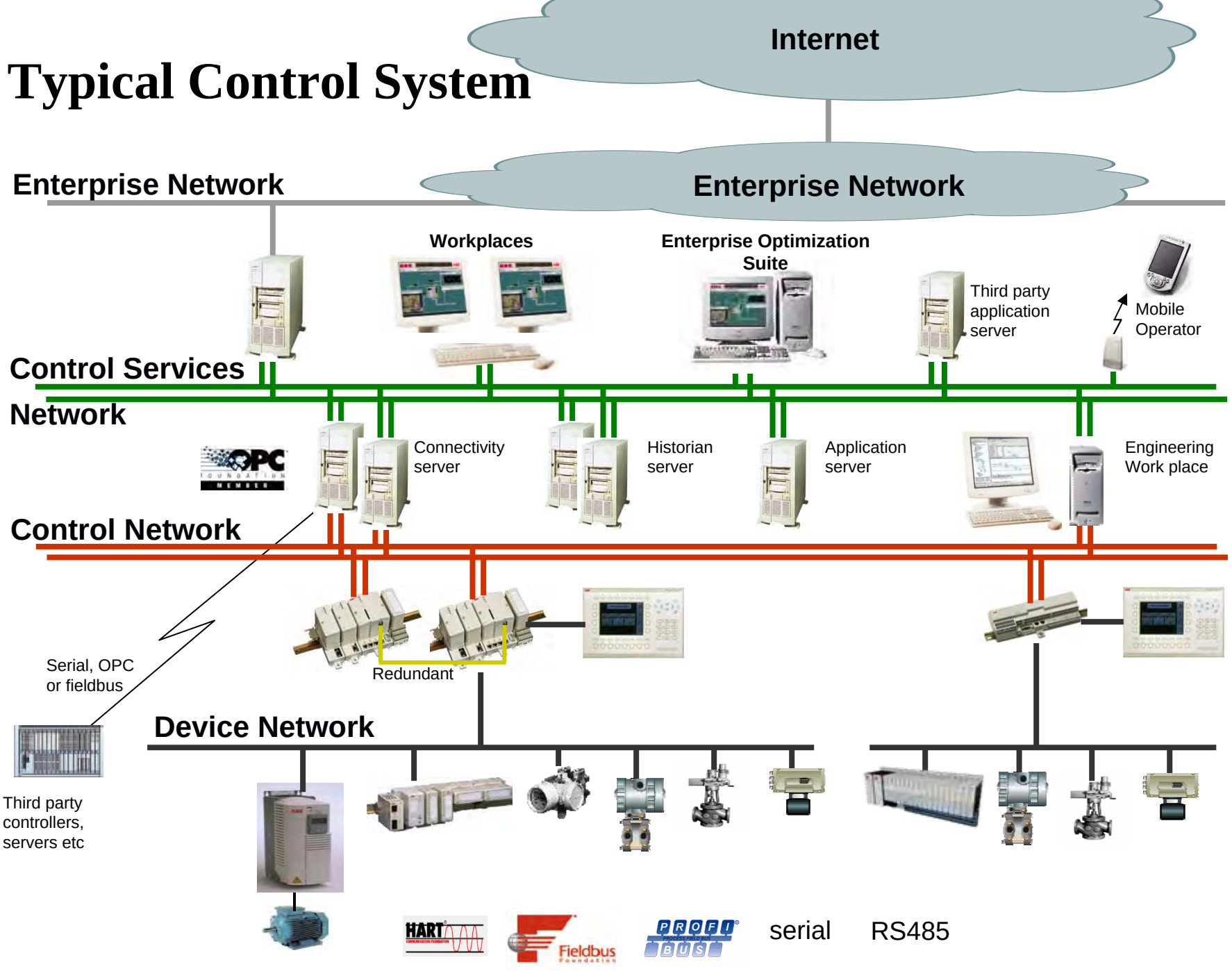
Control Systems

- **Control system - collection of computer systems and devices that monitors and controls physical processes and machines**
  - manufacturing
  - oil & gas
  - water, wastewater
  - chemical plants
  - electric power generation, transmission, distribution
  - transportation
  - …

Types of Control Systems

- **Supervisory Control and Data Acquisition (SCADA)**
  - large geographic distances
  - supervisory control (non-real-time, minutes)
- **Process Control Systems (PCS)**
  - closed loop, central control, near real-time (seconds)
- **Distributed Control Systems (DCS)**
  - similar to Process Control, but not centralized
- **Automation aka Discrete Control**
  - similar to DCS, real-time (milliseconds)

Typical Control System



Technology Trends in Control Systems

- **Adoption of COTS (Commercial-Off-The-Shelf) technologies**
  - MS Windows, WinCE, various embedded RTOSes
  - apps - databases, web servers, web browsers, …
  - IT protocols - HTTP, SMTP, FTP, DCOM, XML, …
- **Connectivity of control system to enterprise LAN**
  - improved business visibility and efficiency
  - remote access to control center and field devices
- **Adoption of IP Networking**
  - common in Control Svcs, gaining in Control, starting in Device
  - most new industrial devices have Ethernet ports
  - many legacy protocols being embedded in TCP or UDP
    - e.g. Modbus/TCP, DNP3

New IP-based Control Systems

- ODVA EtherNet/IP
- Profinet
- Foundation Fieldbus HSE
- Telvent
- ...
- Honeywell Experion
- Emerson Ovation
- Yokogawa VNET/IP
- Invensys Infusion

- IP to the Control Network or even Device Network
- Not all are fully compatible

New Security Threats

- COTS + IP + connectivity = new security threats
- All of those of Enterprise networks and more

- But security issues differ!

Untargeted Threats

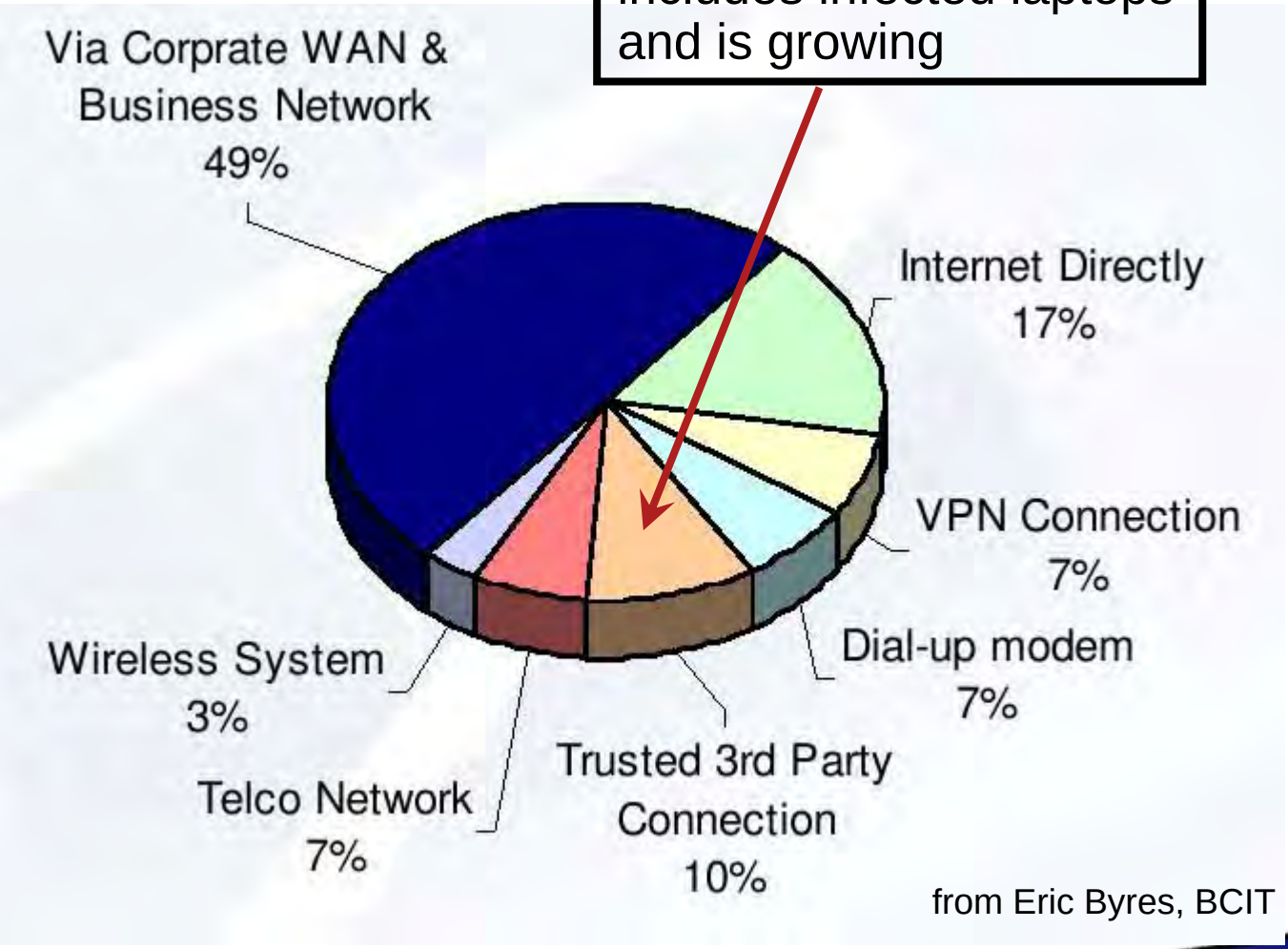
- Worm/Virus Du Jour
- DOS causing loss of availability
- Unauthorized/Unknown access to control system devices
- Unpatched systems
- Improper use of control systems workstations
- Unauthorized applications on the control network
- Network scans by IT staff
- Accidental misconfigurations
- Insecure wireless connections
- Insecure wired connections outside physical control (eg. WAN)

Targeted Threats

- **Organized crime**
  - increasing use of botnets for DDOS and extortion
  - thriving market for day-zero vulnerabilities
- **Terrorists and nation states**
  - potential damage of a blended attack is far greater than physical alone
  - many nations (including US) have cyber attack capabilities for warfare
    - other nations known to be mapping US infrastructure for 10 years
  - documents on SCADA found on Al-Queda computers in Afghanistan
  - renewed calls from Al-Queda for attacks to reduce oil flow to US
- **Competitive espionage**
  - manipulation of spot markets
  - DoS preventing response to market conditions
- **Disgruntled insiders**
  - fired or on strike and know all the passwords

Attack Vectors

includes infected laptops and is growing



from Eric Byres, BCIT

How Big are the Risks?

- **Little information sharing about actual attacks**
  - BCIT incident database has about 30 incidents per year
  - financials estimate that 2% of incidents occurring are reported
  - concern for damage of corporate reputation and stock price
- **But potential consequences can be huge**
  - 2003 NE blackout was not a cyber attack, but could have been
  - big auto has lost many $M to worms/viruses
- **Risk = vulnerability X threat X consequence**

vulnerability:	large
threat:	**insufficient data** (in public)
consequence:	large
conclusion:	??

Differences from Enterprise Networks

- **Availability, Integrity, Confidentiality in that order**
- **Some devices must operate in extreme environments**
- **Physical topologies may be unusual**
- **Many special purpose limited function systems / devices**
- **Network configurations are fairly static**
- **Long service lifetimes**
- **Much legacy equipment**
- **Fragile implementations**
- **Unpatched systems**
- **Managed by control systems dept. who are not IT experts**

Standard Enterprise Architectures are not appropriate!

PROCESS CONTROL SYSTEMS FORUM

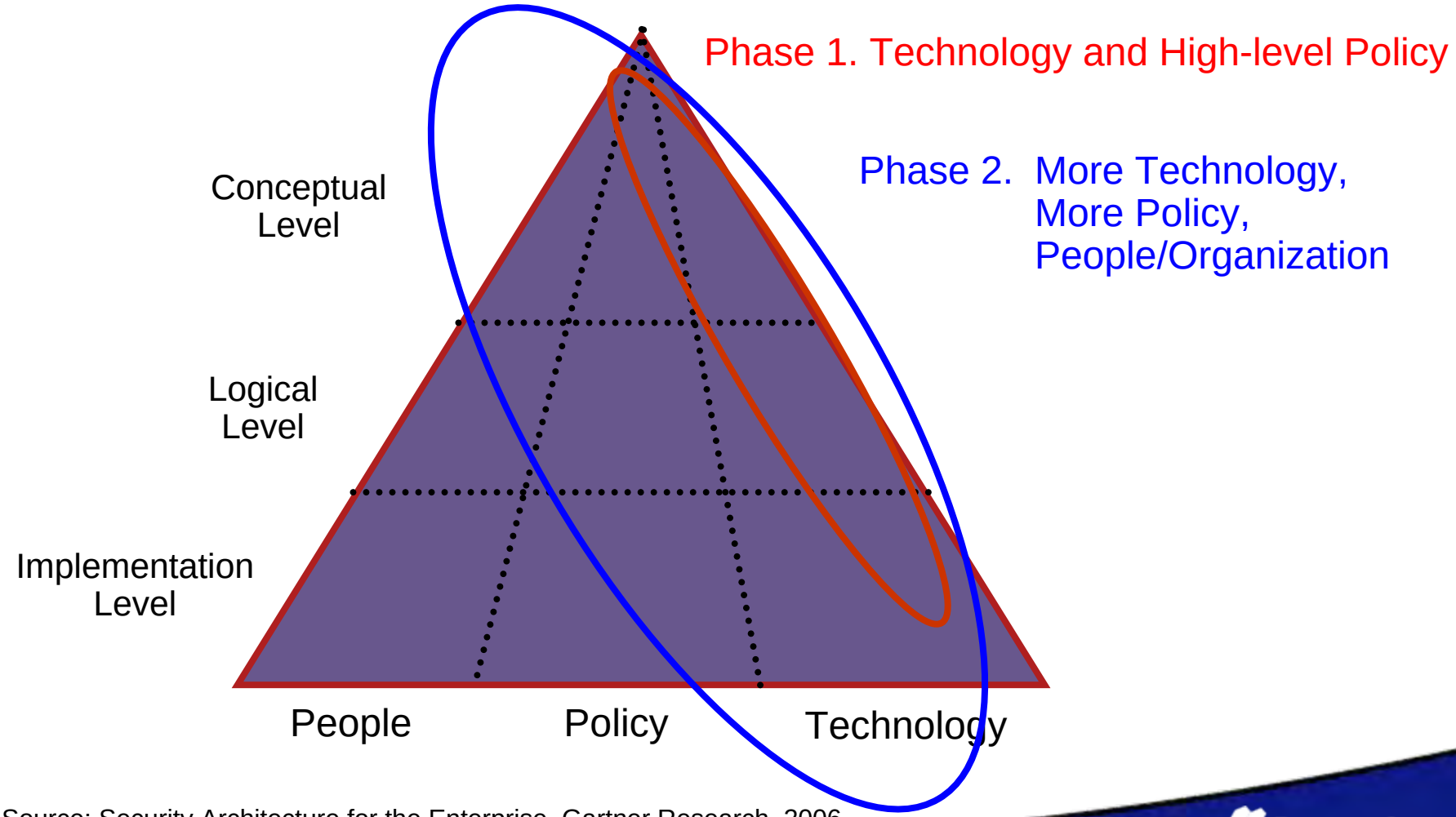
Secure Network Architectures for Control Systems

Collaborating to Advance Control System Security

Secure Network Architectures for Control

- **Based on IP**
  - higher performance, lower total cost of ownership, future proof
- **Flexible**
  - technologies, topologies, transmission media, performance levels
- **Scalable**
  - from small to very large control systems
- **Secure**
  - against both today's and tomorrow's threats

Cisco Secure Architectures for Control

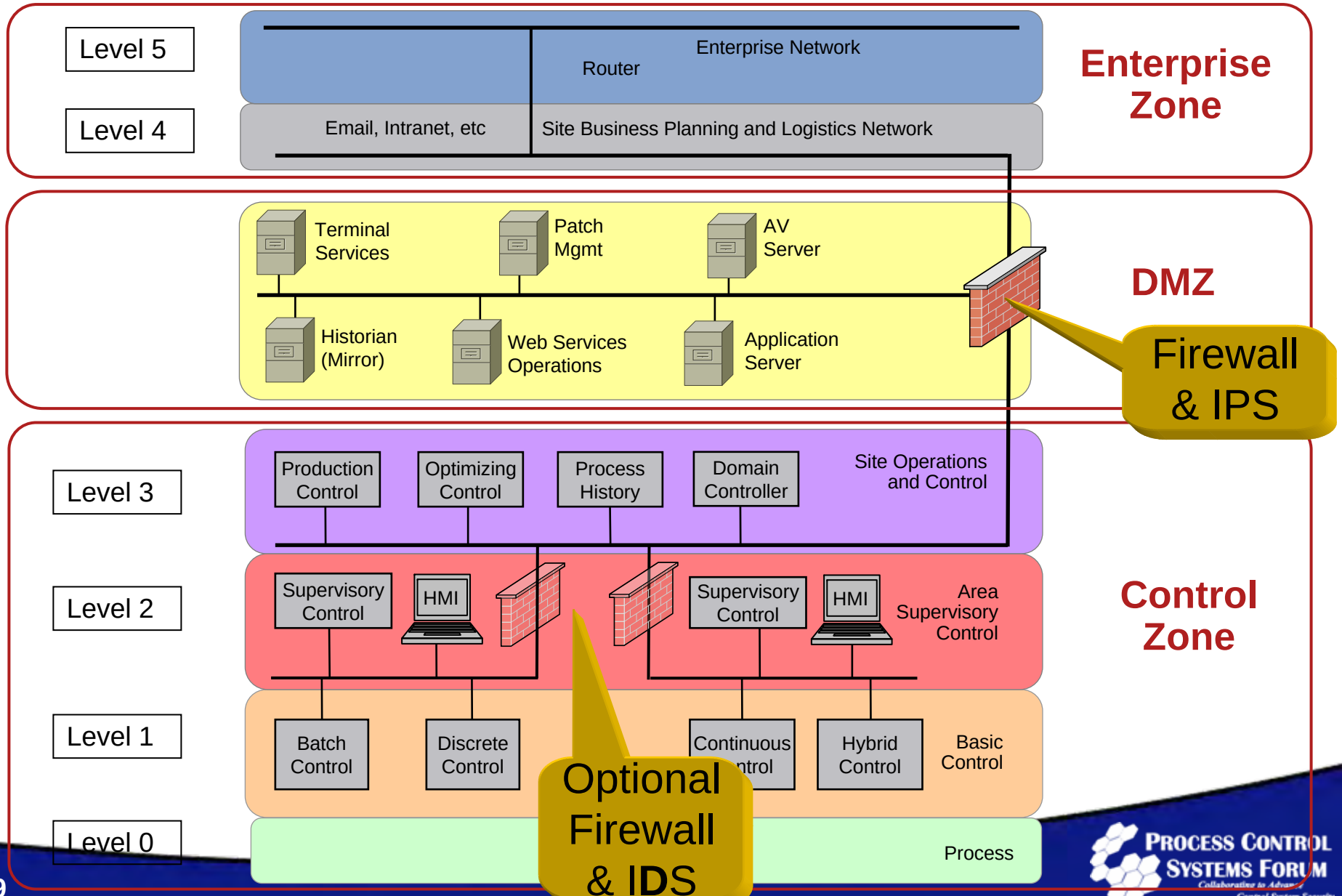


Source: Security Architecture for the Enterprise, Gartner Research, 2006

Cisco Secure Architectures for Control

- **Architectural guidelines for secure process control, distributed control, automation, and SCADA**
  - product, deployment, and configuration guidance to address unique considerations of control systems environments
  - leverage enterprise solutions where applicable (core, distribution, access, firewall, vpn)
  - modules for specific functionality (SCADA, remote access, etc.)
  - validated performance for small to medium size systems
  - clear and concise guidance!
- **Developing in partnership with control system vendors**
  - OSISoft, Rockwell, and others

Logical Overlay on SP99 / Purdue Model of Control

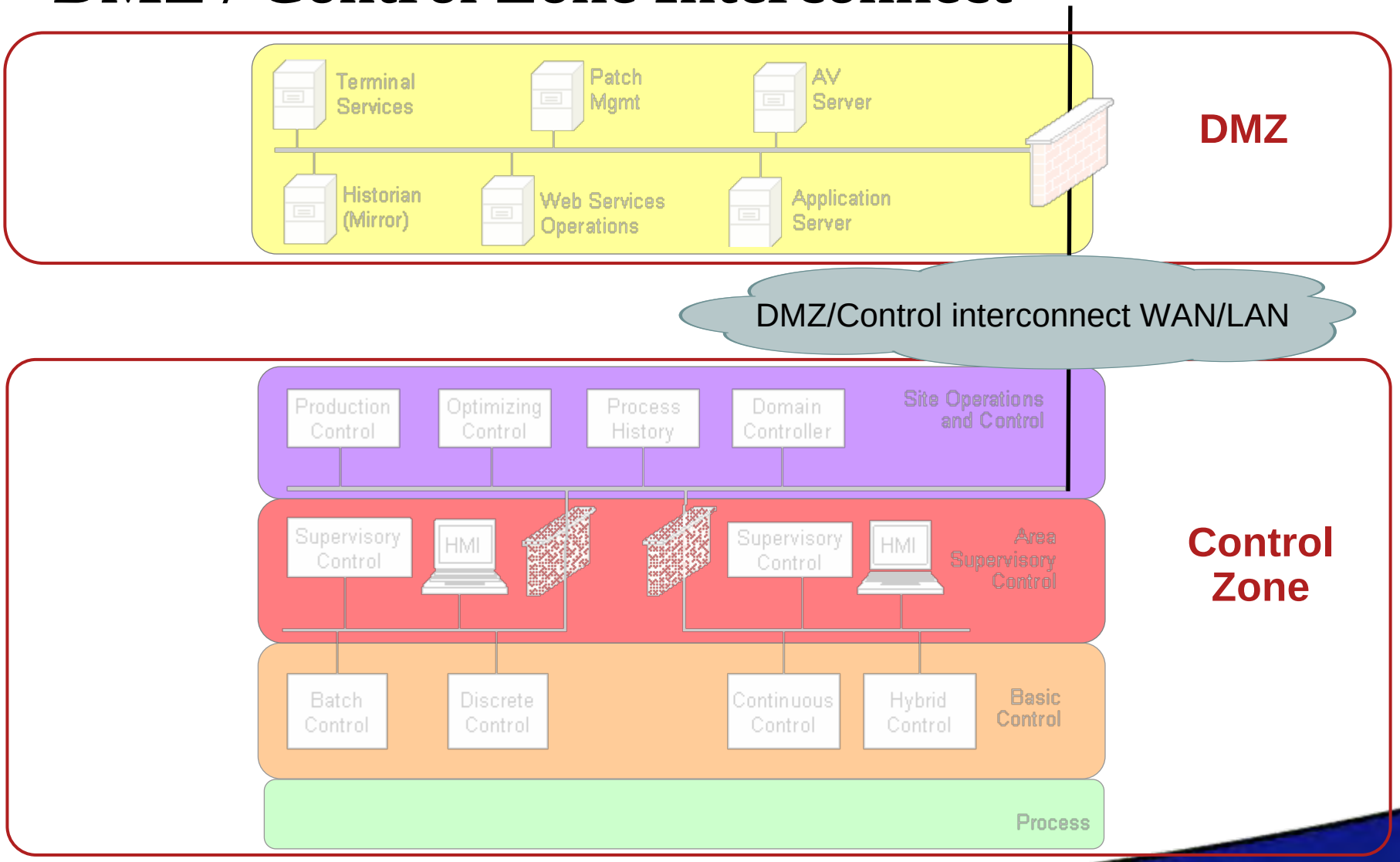


Process Control Systems Forum
Collaborative to Advance Control System Security

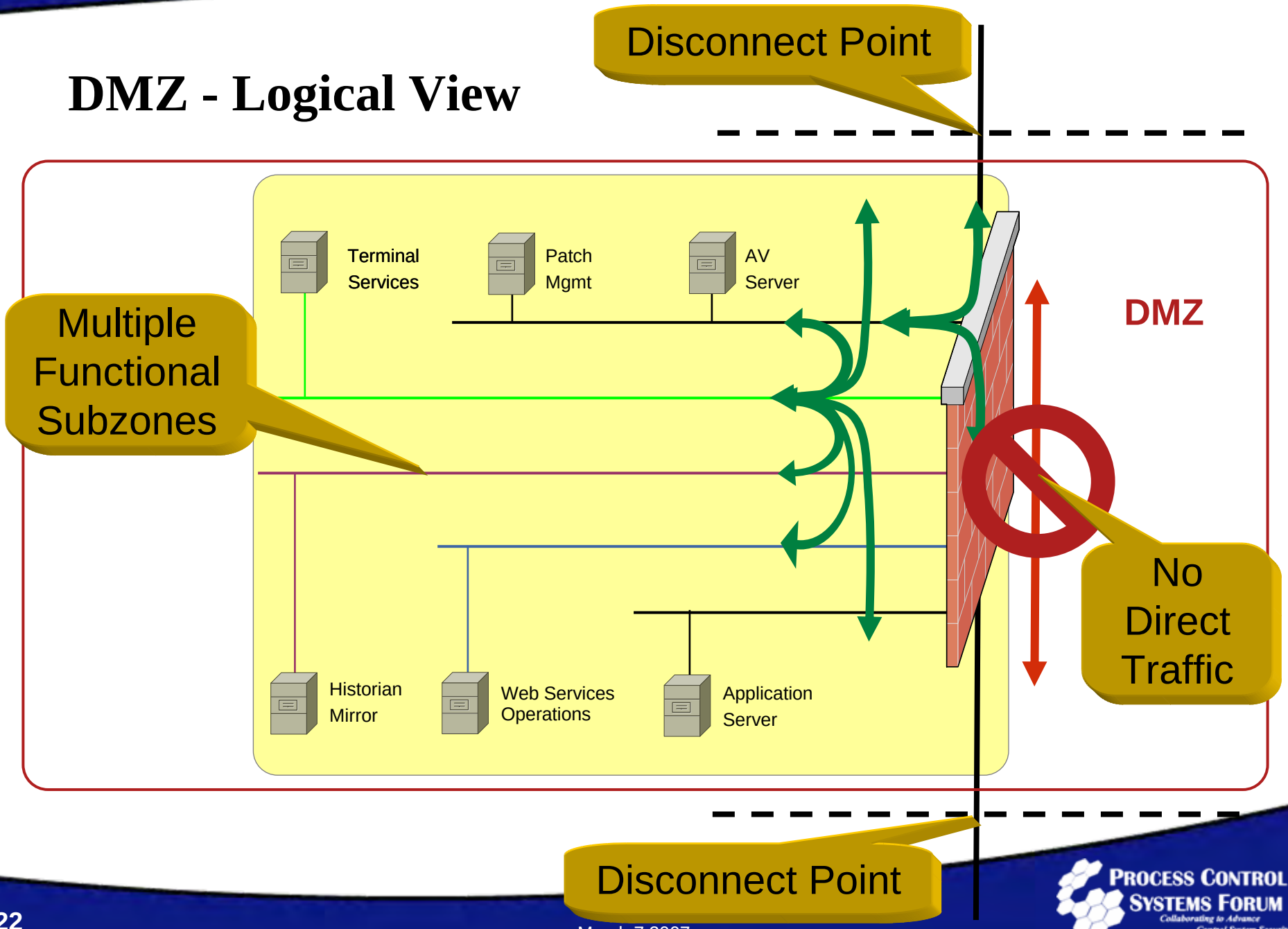
Logical Architecture

- **Enterprise Zone contains typical business systems**
  - email, web, office apps, etc.
- **DMZ provides business connectivity**
  - contains only non-critical systems that need access to both Control and Enterprise Zones
  - enforces separation between Enterprise and Control Zones
  - consists of multiple functional sub-zones
    - separated by firewall and IPS
- **Control Zone demarcates critical control systems**
  - consists of multiple functional sub-zones
    - (optionally with firewall and IDS)

DMZ / Control Zone Interconnect



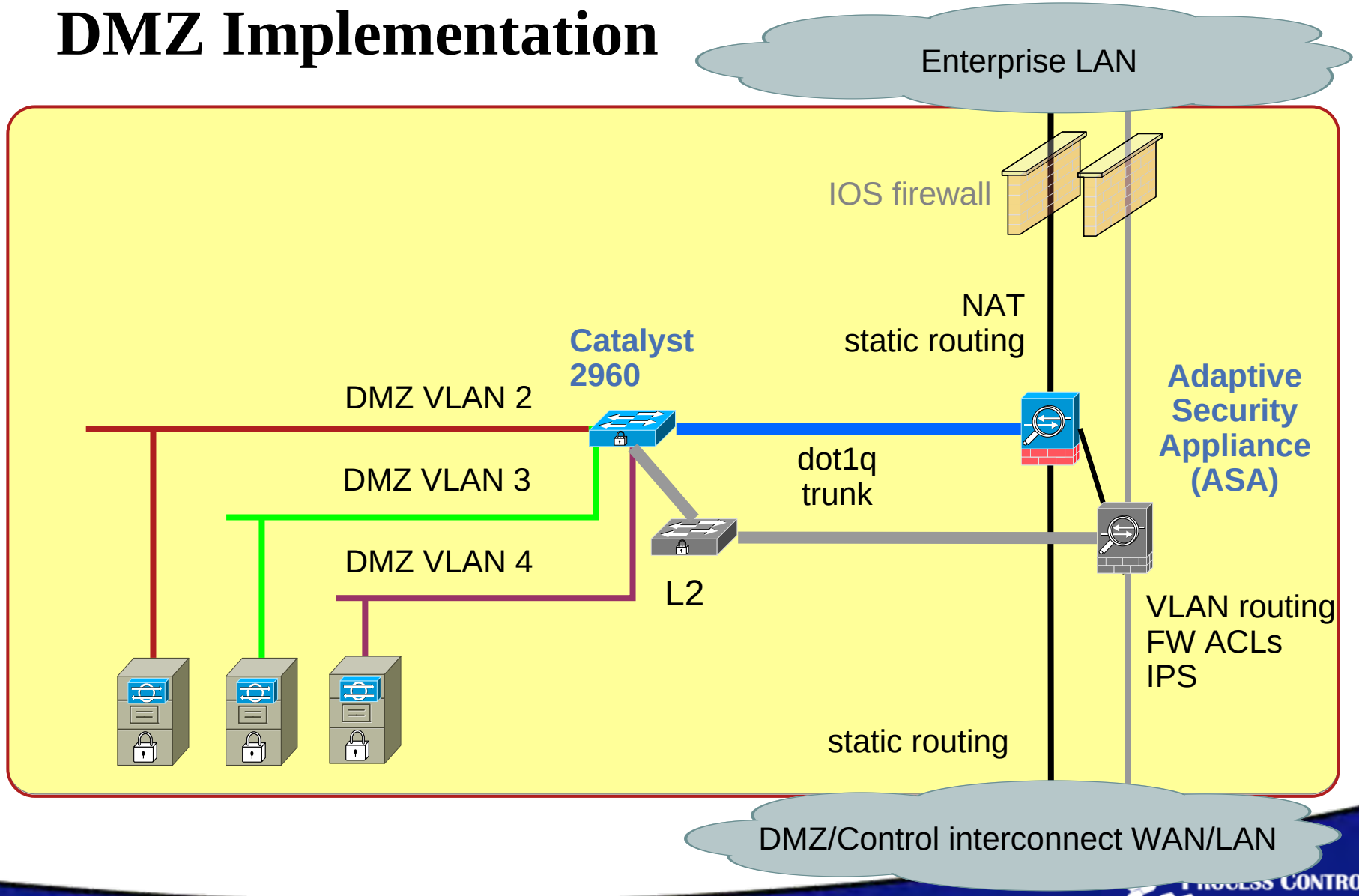
DMZ - Logical View



DMZ Design Principles

- **DMZ has multiple functional sub-zones**
- **Limited communication between sub-zones**
- **DMZ provides only path in/out of Control Zone**
- **No direct traffic across DMZ**
- **No common ports between upper and lower firewalls**
- **No control traffic across upper firewall**
- **Firewalls are potential disconnection points**
  - Control Zone must be independent to allow continued operation
  - DMZ must be independent to allow remediation

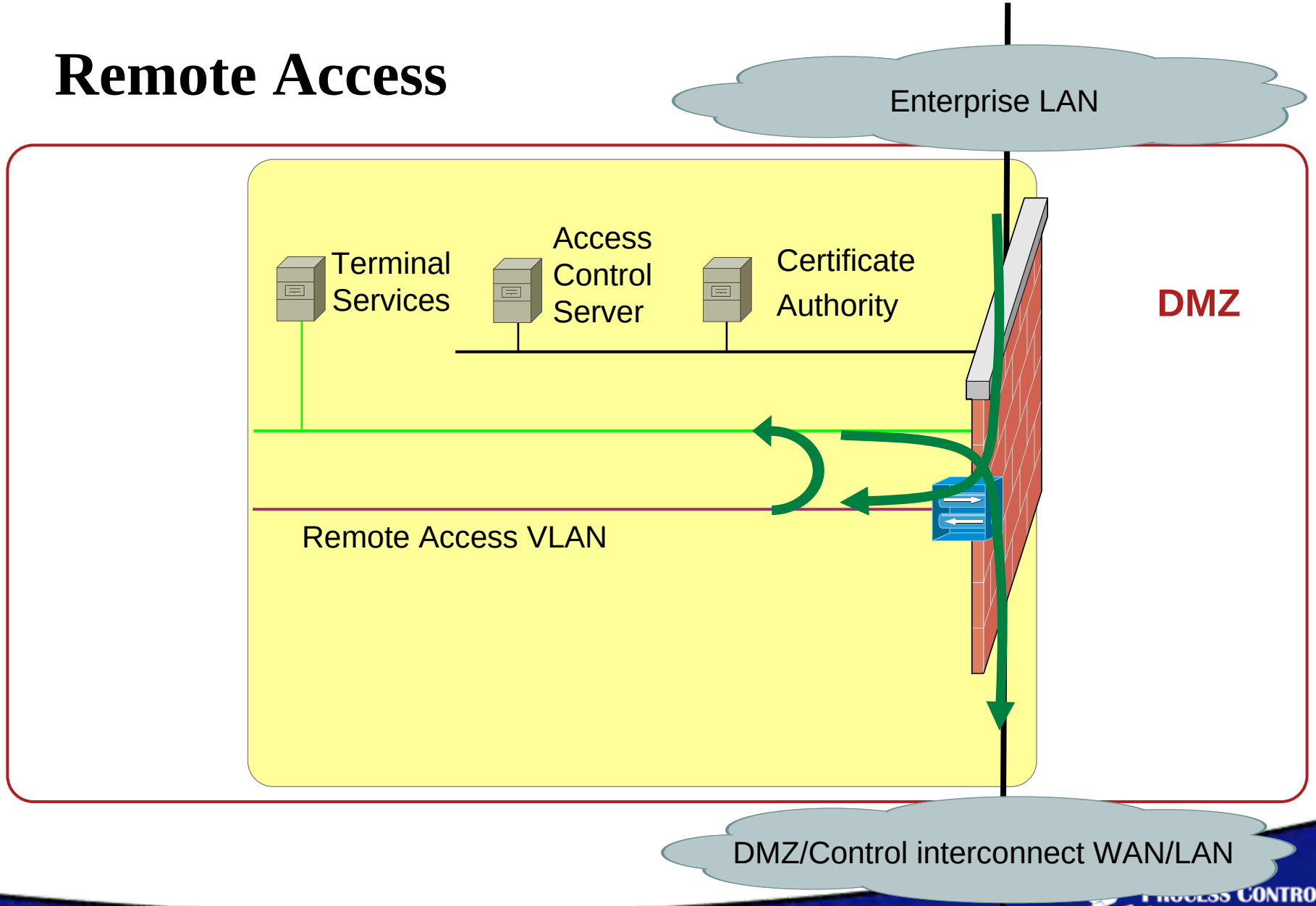
DMZ Implementation



DMZ Implementation

- **Cisco ASA with Advanced Inspection Module (IPS)**
  - signatures for DNP3, Modbus
- **Sub-zones implemented by VLANs**
  - all inter-VLAN routing done by ASA
  - L2 switch must be Cisco switch to prevent VLAN hopping
- **Static routing and ACLs implement policy between**
  - DMZ VLANs, Enterprise Zone, Control Zone
- **Optional active-standby redundancy**
  - Servers can use teaming drivers
- **Optional separate hardware firewall**
  - defends against ASA compromise or misconfiguration

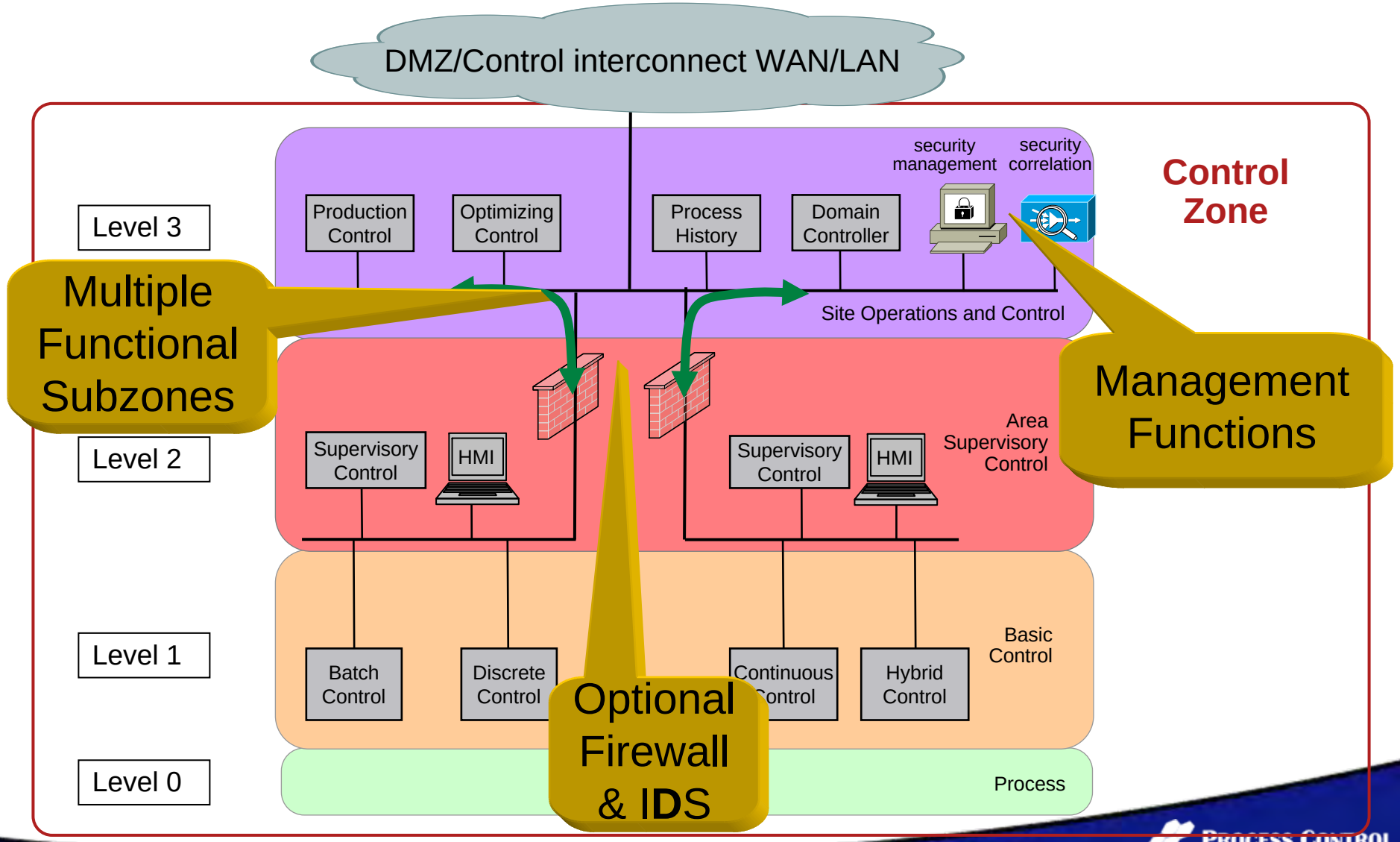
Remote Access



Remote Access

- **ASA terminates VPNs into a remote access VLAN**
  - client or client-less VPN
- **Authentication via:**
  - AAA server, LDAP, Active Directory, ...
  - multi-factor hardware token
- **Clients use Remote Desktop to connect to Terminal Svcs**
  - applications installed on Terminal Svcs machine
  - or hop to another machine via Remote Desktop
- **Network can provide coarse Role-Based Access Control**
  - ASA dynamically creates ACLs based on user or group

Control Zone - Logical View

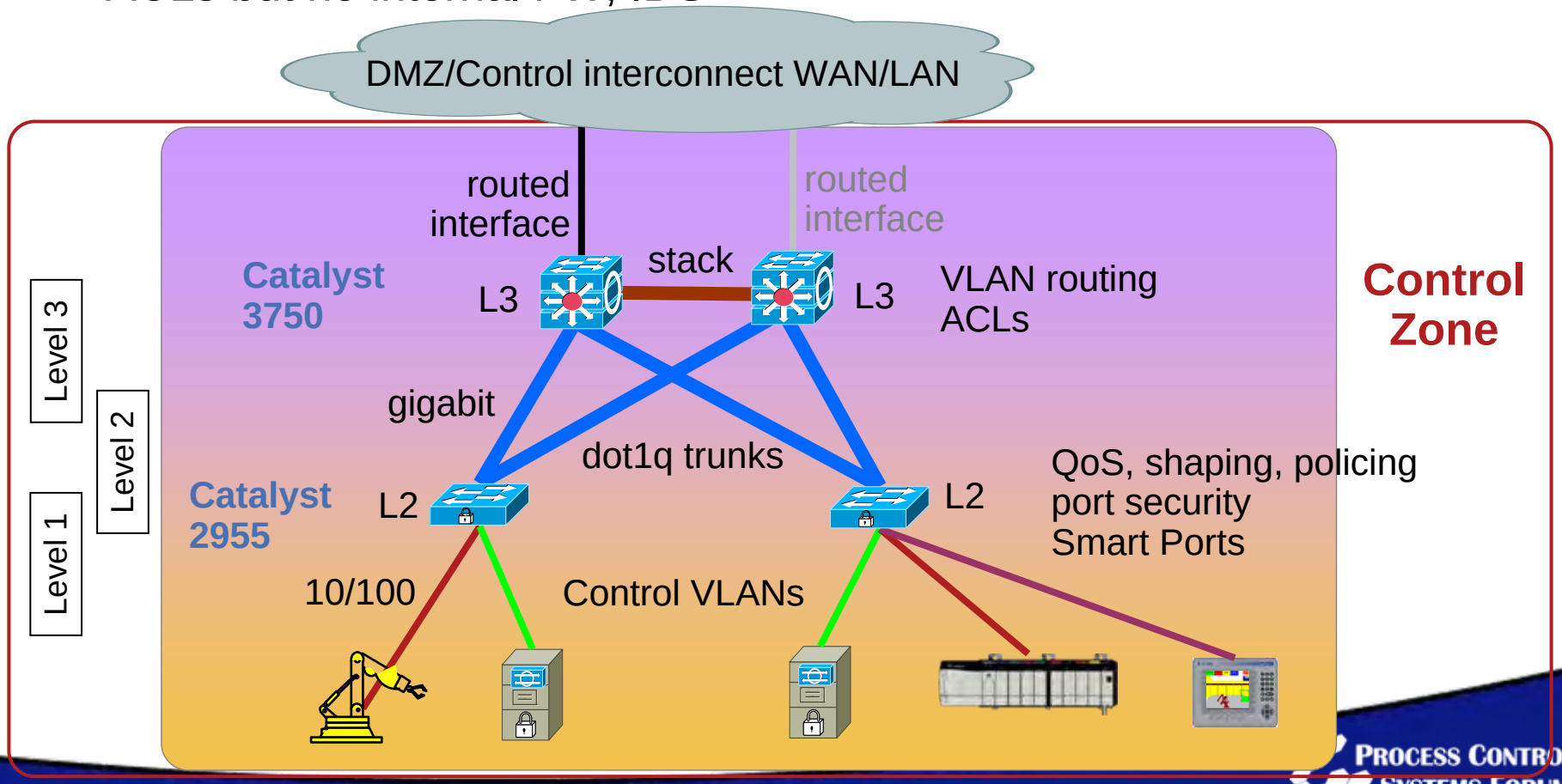


Control Zone Design Principles

- **Independent of DMZ and Enterprise Zones**
  - allows for disconnection
- **Minimal number of connections to DMZ**
- **Limited communication between sub-zones**
- **Management only from inside**
- **Protection inside and throughout control zone**
  - port security
  - QoS, traffic shaping, traffic policing
  - Smart Ports macros for easy port configuration
  - optional IDS, firewall between sub-zones
  - Cisco Clean Access (802.1x NAC in future)

Control Zone Implementation - Small

- Fast routing between VLANs via L3 switch
- ACLs but no internal FW, IDS



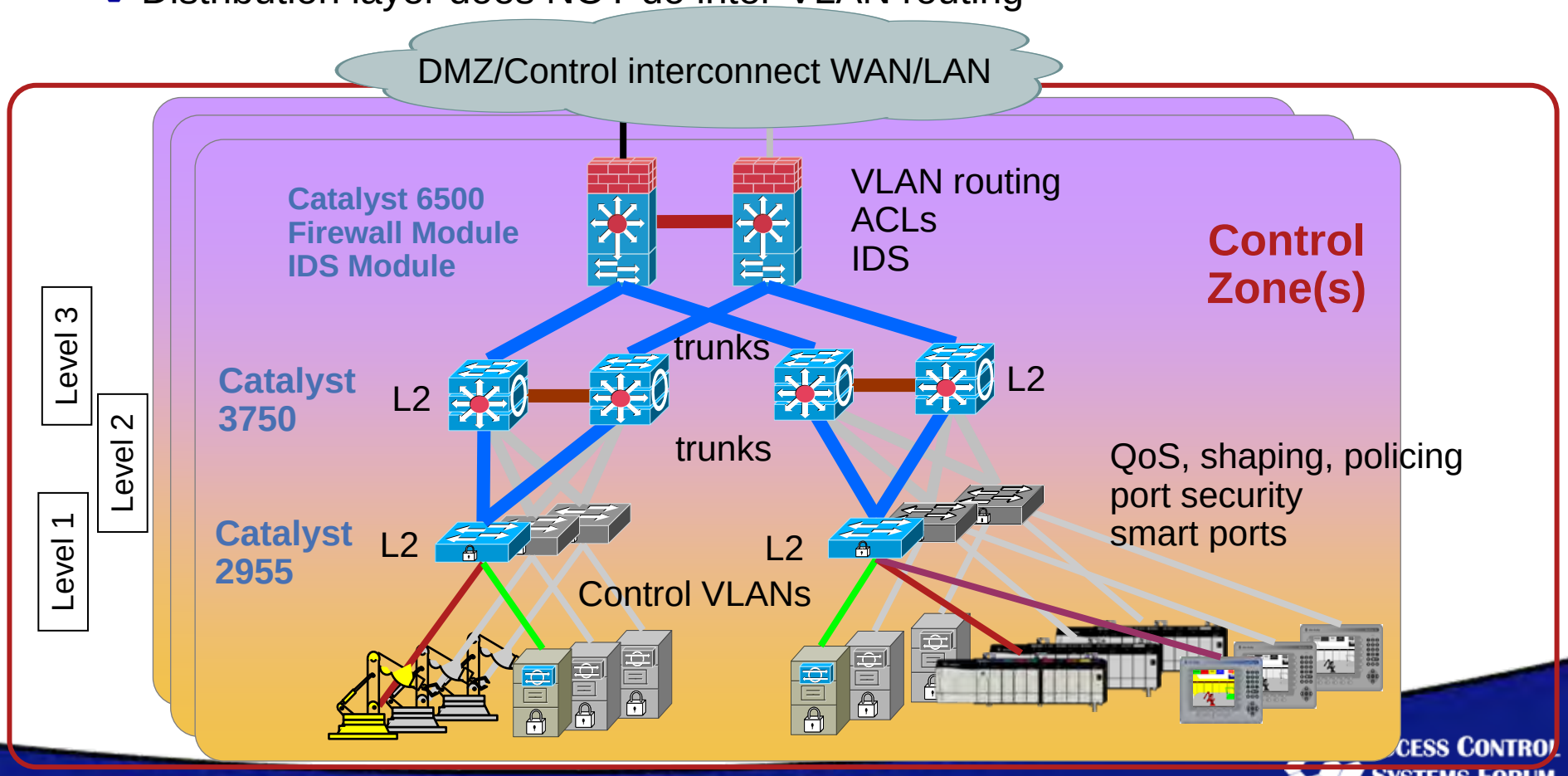
PROCESS CONTROL SYSTEMS FORUM
Collaborating to Advance Control System Security

Control Zone Implementation - Small

- **Sub-zones implemented by VLANs**
  - communication policy enforced by ACLs
- **3750 stackable L3 switches for core layer**
  - fast routing between control VLANs
  - fast failover
- **Rapid PVST+ for fast star network convergence**
- **Optional distribution layer**
- **2955 industrial switches for access layer**
  - dual gigabit uplinks
- **Servers can use teaming drivers for network resiliency**

Control Zone Implementation - Large

- High performance, high availability
- FW, IDS between Control VLANs
- Distribution layer does NOT do inter-VLAN routing



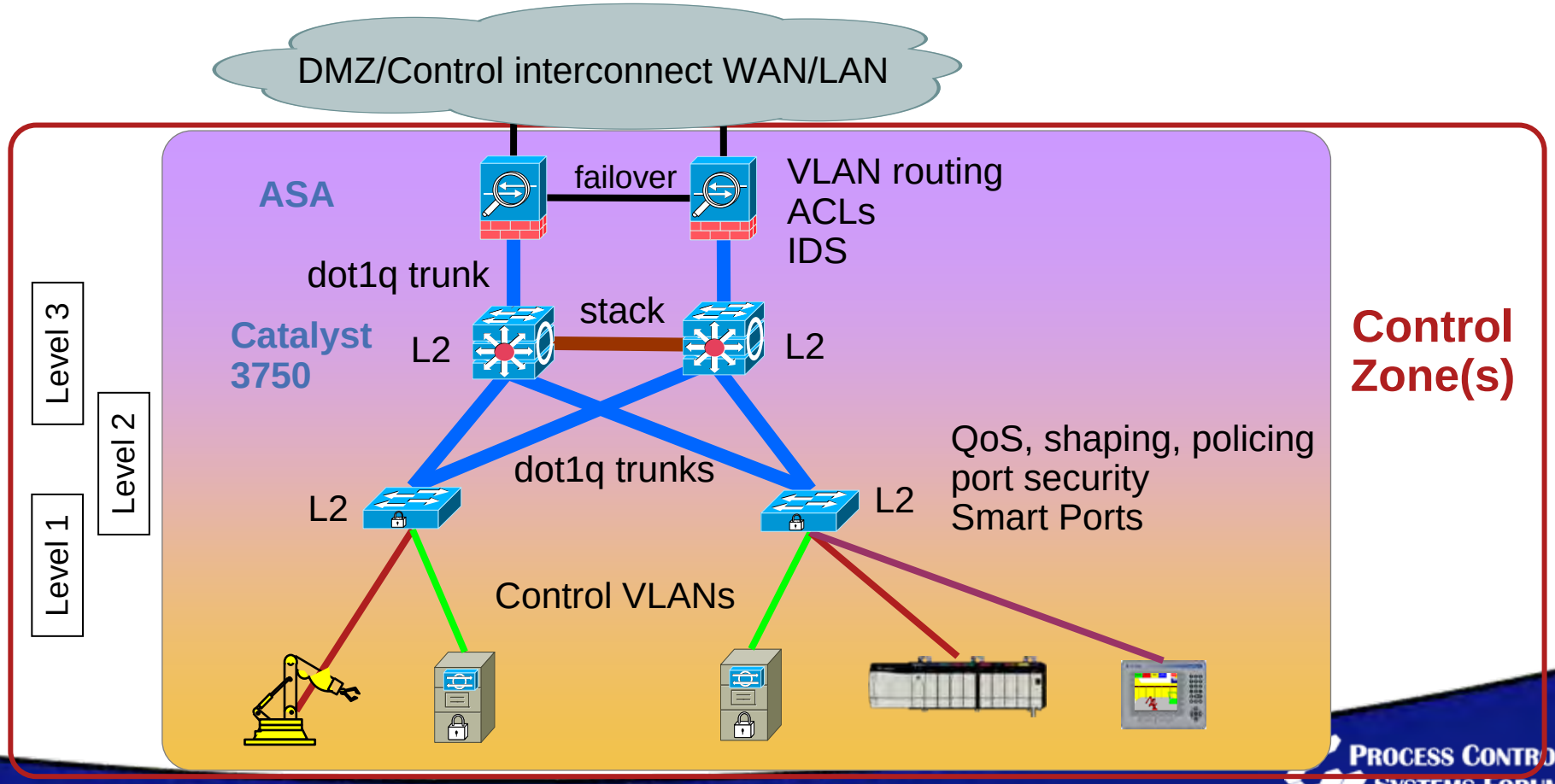
CESS CONTROL
SYSTEMS FORUM
Collaborating to Advance
Control System Security

Control Zone Implementation - Large

- **Sub-zones implemented by VLANs**
- **All traffic between VLANs passes thru firewall and IDS**
  - IDS ensures no interference with control due to false positives
  - helps limit spread of infection within Control Zone
  - helps impede scanning of Control Zone
- **6500 core provides high availability**
- **3750 stackable switches for distribution layer**
  - do not do inter-VLAN routing

Control Zone Implementation - Medium

- FW, IDS between VLANs with lower cost/performance than 6500s
- Inter-VLAN routing done by ASA



Control Zone Implementation - Medium

- **Similar in function to Large implementation**
- **ASA does firewall and IDS between DMZ, control zones, and between control VLANs**
  - iintra-VLAN traffic bypasses firewall via distribution switch stack
  - intra-VLAN traffic not impacted by ASA speed

Cisco MARS

- **MARS – Monitoring, Analysis, and Response System**
  - monitors switches, routers, firewalls via SNMP
  - detects network attacks
  - allows single-click response
- **reduces false positives by providing an end-to-end view**
- **can generate audit compliance reports**
- **can accept control system events from OSISoft**

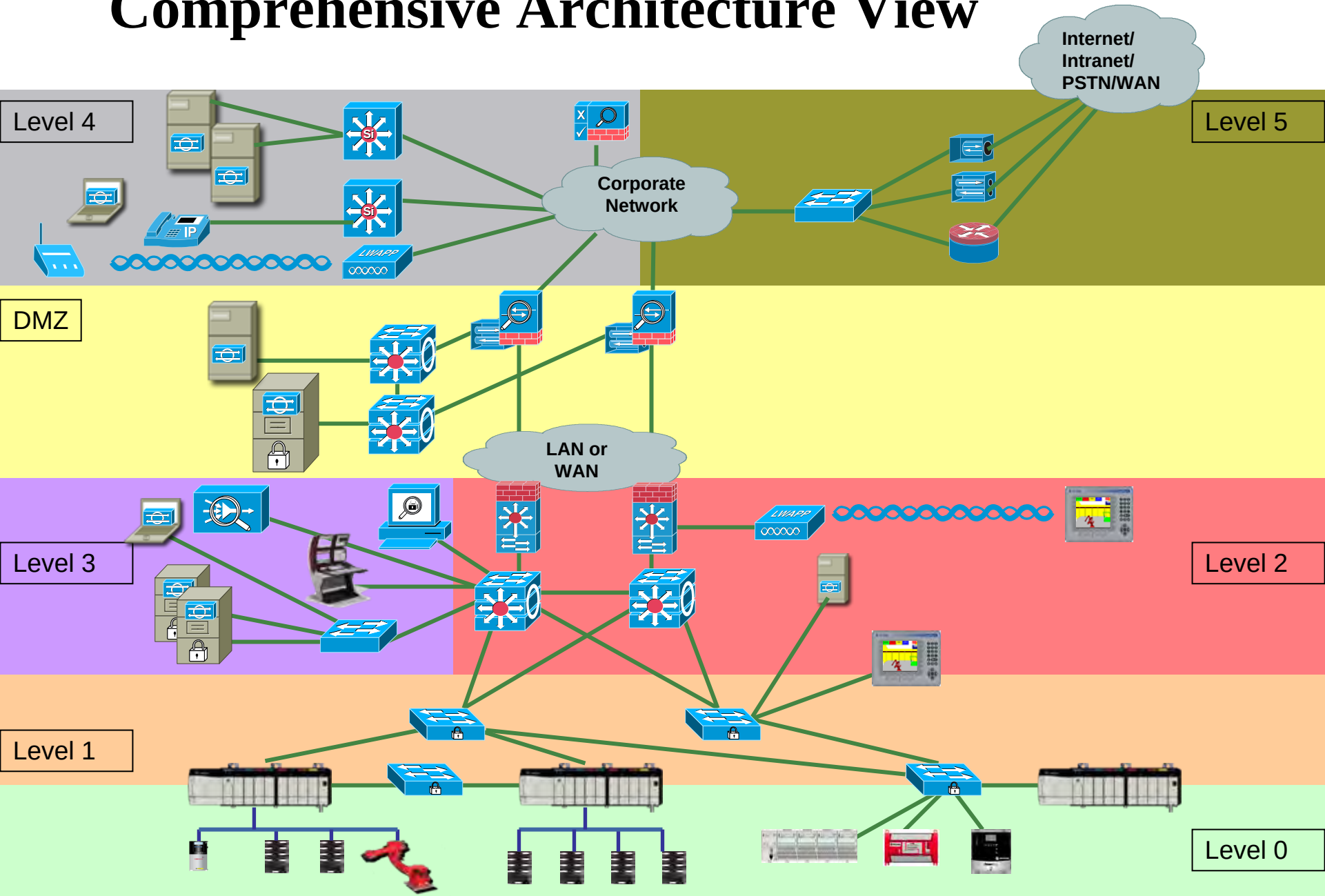
Cisco Clean Access

- Network Admission Control, but more mature than 802.1x
- Mediates access to network from wired or wireless
- Authenticates client before allowing network access
- Can check client is running a trusted anti-virus product
- Can help prevent infection of control system by infected laptops
- Appropriate for both DMZ and Control Zone

Cisco Security Agent

- Signatureless Host-based IPS for Windows, Linux
- Requires development of a policy for specific applications
- Can prevent “day zero” exploits
- Reduces need to patch
- Cisco will work with vendors to develop profiles for control systems servers

Comprehensive Architecture View



Status

- **CIAG investigating general architectures**
  - constructing a lab in Austin TX
- **Several groups in Cisco looking at specific verticals**
  - automation
  - oil & gas
  - pipeline
- **Design guides in development**
- **Seeking feedback from vendors and operators**
- **Seeking additional vendors interested in cooperative R&D**

Future Plans

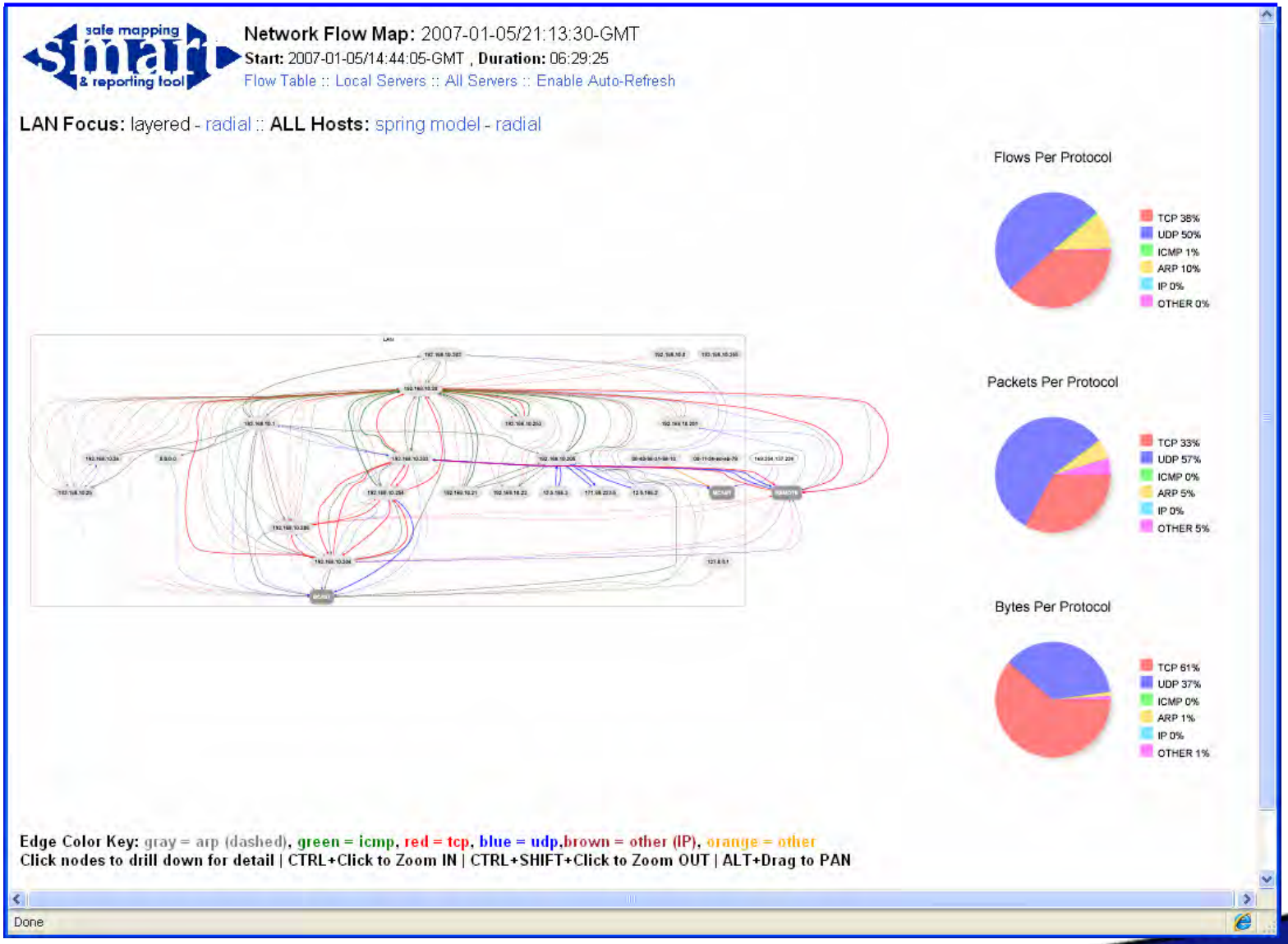
- SCADA over IP
- Better ring redundancy
- Layer 3 access
- Integrated physical security
- Wireless remote access
- Wireless device access

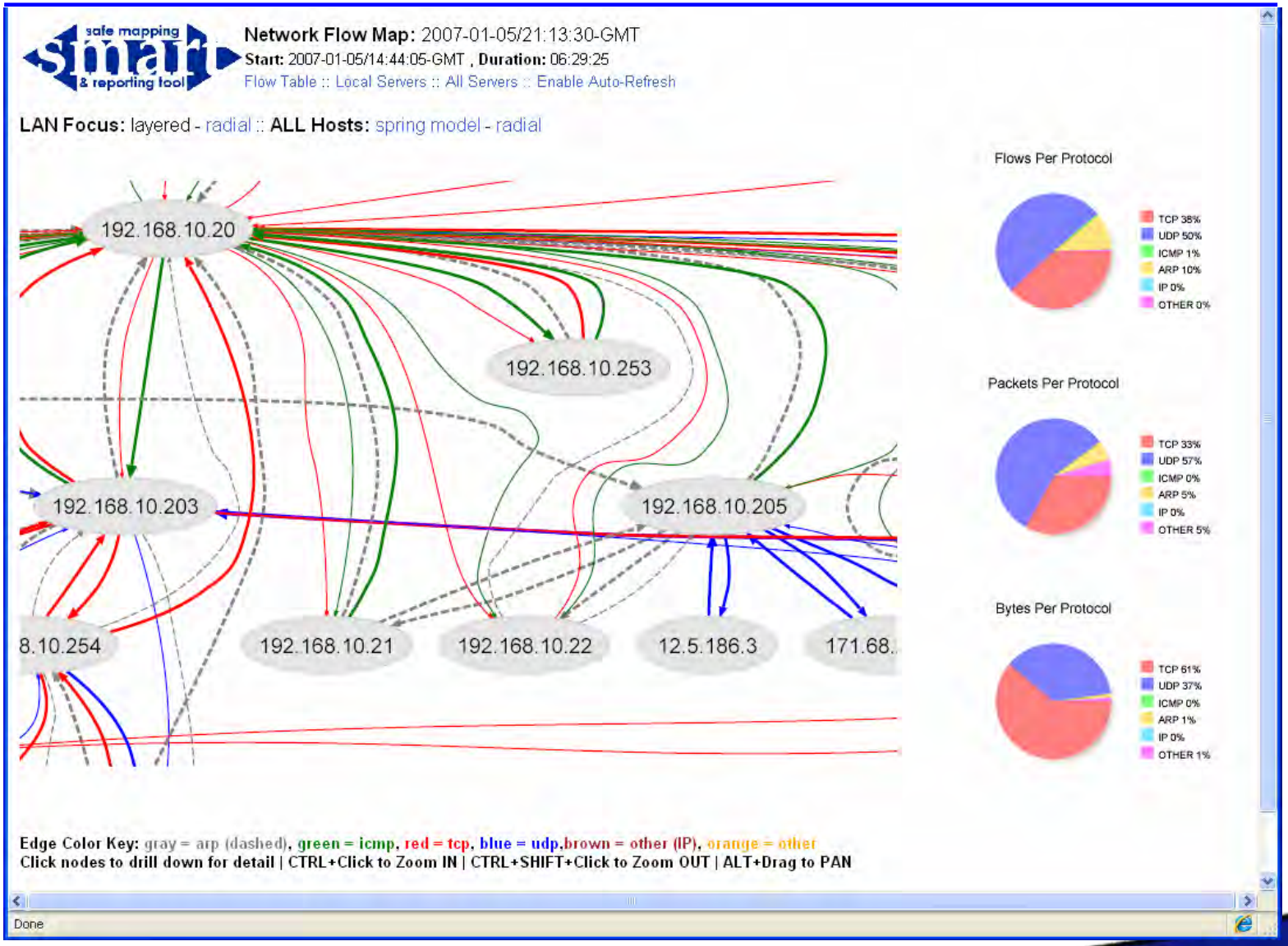
- And someday ... Convergence!

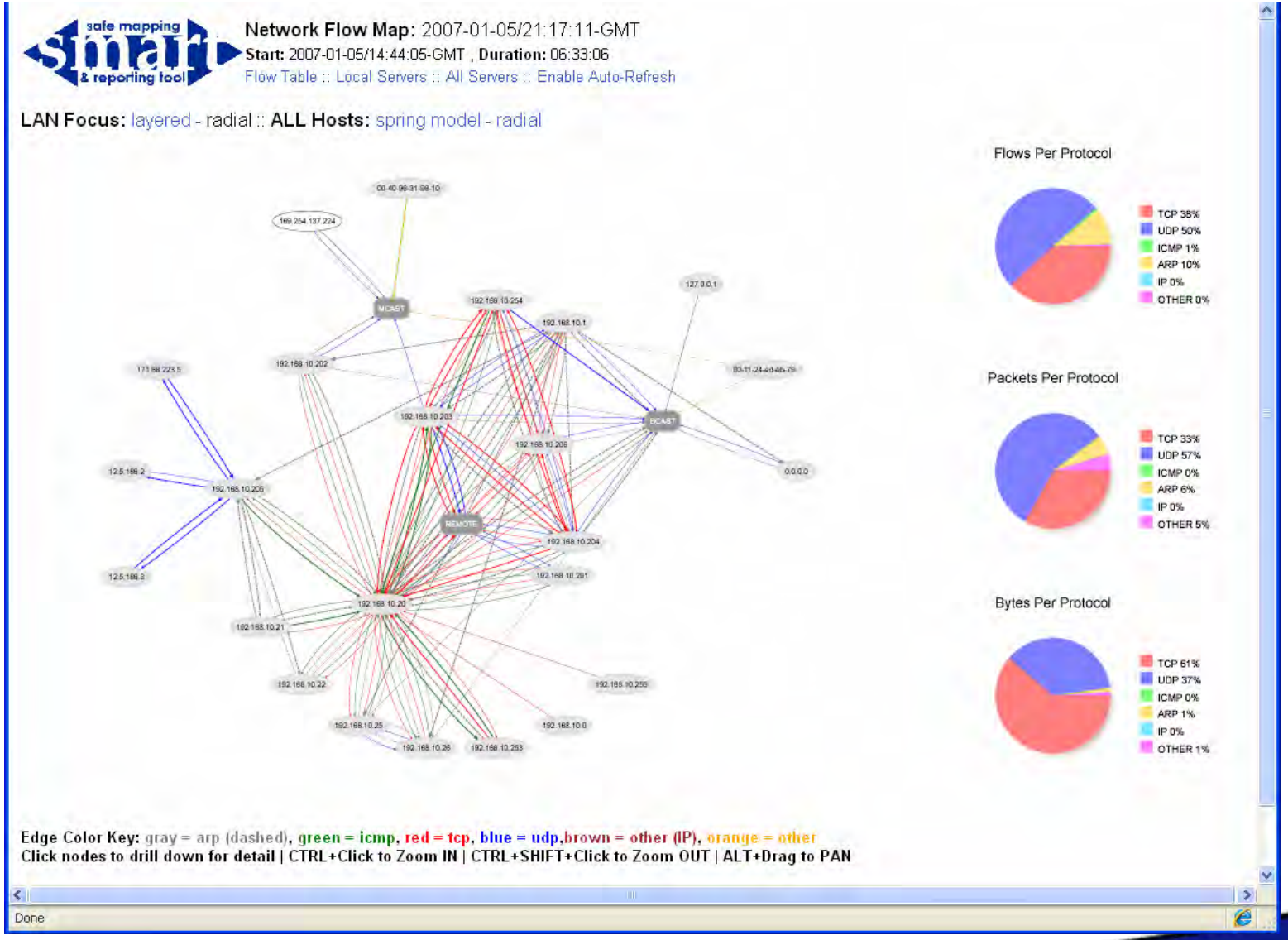
andwrigh@cisco.com

SMART Overview

- **Safe Mapping And Reporting Tool**
  - safe network mapping for control systems networks
- **Broad applicability to any LAN**
- **Completely passive discovery**
- **Visualize flows rather than topology**
- **Network forensics**
- **Data collection/sharing for better informed CIP research**
- **Implemented using Perl, Graphviz, SVG (open source)**
- **Cross platform**
  - Linux (and probably *nix) or Windows (via Cygwin)
- **Open source (soon)**


safe mapping
smart
& reporting tool
Network Flow Map: 2007-01-05/21:13:30-GMT
Start: 2007-01-05/14:44:05-GMT , Duration: 06:29:25
Flow Table :: Local Servers :: All Servers :: Enable Auto-Refresh
LAN Focus: layered - radial :: ALL Hosts: spring model - radial
Flows Per Protocol
TCP 38%
UDP 50%
ICMP 1%
ARP 10%
IP 0%
OTHER 0%
Packets Per Protocol
TCP 33%
UDP 57%
ICMP 0%
ARP 5%
IP 0%
OTHER 5%
Bytes Per Protocol
TCP 61%
UDP 37%
ICMP 0%
ARP 1%
IP 0%
OTHER 1%
Edge Color Key: gray = arp (dashed), green = icmp, red = tcp, blue = udp,brown = other (IP), orange = other
Click nodes to drill down for detail | CTRL+Click to Zoom IN | CTRL+SHIFT+Click to Zoom OUT | ALT+Drag to PAN
Done


safe mapping
smart
& reporting tool
Network Flow Map: 2007-01-05/21:13:30-GMT
Start: 2007-01-05/14:44:05-GMT , Duration: 06:29:25
Flow Table :: Local Servers :: All Servers :: Enable Auto-Refresh
LAN Focus: layered - radial :: ALL Hosts: spring model - radial
192.168.10.20
192.168.10.253
192.168.10.203
192.168.10.205
8.10.254
192.168.10.21
192.168.10.22
12.5.186.3
171.68.
Flows Per Protocol
TCP 38%
UDP 50%
ICMP 1%
ARP 10%
IP 0%
OTHER 0%
Packets Per Protocol
TCP 33%
UDP 57%
ICMP 0%
ARP 5%
IP 0%
OTHER 5%
Bytes Per Protocol
TCP 61%
UDP 37%
ICMP 0%
ARP 1%
IP 0%
OTHER 1%
Edge Color Key: gray = arp (dashed), green = icmp, red = tcp, blue = udp,brown = other (IP), orange = other
Click nodes to drill down for detail | CTRL+Click to Zoom IN | CTRL+SHIFT+Click to Zoom OUT | ALT+Drag to PAN
Done


safe mapping
smart
& reporting tool
Network Flow Map: 2007-01-05/21:17:11-GMT
Start: 2007-01-05/14:44:05-GMT , Duration: 06:33:06
Flow Table :: Local Servers :: All Servers :: Enable Auto-Refresh
LAN Focus: layered - radial :: ALL Hosts: spring model - radial
Flows Per Protocol
TCP 38%
UDP 50%
ICMP 1%
ARP 10%
IP 0%
OTHER 0%
Packets Per Protocol
TCP 33%
UDP 57%
ICMP 0%
ARP 6%
IP 0%
OTHER 5%
Bytes Per Protocol
TCP 61%
UDP 37%
ICMP 0%
ARP 1%
IP 0%
OTHER 1%
Edge Color Key: gray = arp (dashed), green = icmp, red = tcp, blue = udp,brown = other (IP), orange = other
Click nodes to drill down for detail | CTRL+Click to Zoom IN | CTRL+SHIFT+Click to Zoom OUT | ALT+Drag to PAN
Done

SMART: All Servers (Local Servers)

srcIP	name	srcMAC	srcPORT	proto	description
64.112.229.132	www.giac.org	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
63.99.250.236	3.www.chemistry.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.202.197	signin.ebay.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
198.133.219.25	www.cisco.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
192.168.10.205		00-14-69-87-f7-7e	4500	udp	
204.2.208.40	a1654.g.akamai.net	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.192.115	pages.ebayrealestate.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
140.98.193.141	ieee.org	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.192.87	pages.ebay.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
192.150.18.118	www-mm.wip3.adobe.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.204.56	cgi5.ebay.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.211.160.134	search.ebay.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.202.181	scgi.ebay.com	00-0f-66-1f-ee-b9	443	tcp	https 443/tcp # MCom
64.236.38.184	a1486.g.akamai.net	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
204.120.182.142	www2.foxnews.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
204.2.208.46	a120.g.akamai.net	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
209.249.142.97	js.lb-revsci.net	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
143.252.148.161		00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
206.114.207.70	realtytrac.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
216.75.16.194	www.realclearpolitics.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
199.181.252.161	comstock-interactivedata.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.202.135	my.ebay.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
204.2.208.57	a1919.g.akamai.net	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
72.5.124.95	java.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.192.126	hp-core-other.ebay.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
195.47.237.48	www.hemscottdata.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
204.2.208.71	a1486.g.akamai.net	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
63.240.4.179	www.forbes.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
72.21.206.5	D.www.amazon.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
198.133.219.119	newsroom.cisco.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
64.50.82.58	mycavuto.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
209.234.235.149	www.lipperweb.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
216.73.87.101	us.ebayobjects.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
207.242.93.81	www.accuweather.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
204.2.208.81	a127.g.akamai.net	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.211.180	www.ebaystores.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
208.65.168.3		00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.135.215.37	www.express.ebay.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
209.62.176.52	ad.3ad.doubleclick.net	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
66.211.160.251	offer.ebay.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
198.133.219.83	ng-prod1.cisco.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP
205.234.192.144	www.zacks.com	00-0f-66-1f-ee-b9	80	tcp	http 80/tcp www www-http # WorldWideWeb HTTP

Done

(Test Lab) SMART Network Flow Map | (Test Lab) SMART Host Detail: 192....

Host Detail: 192.168.10.20

MAC Address	00-e0-81-24-d5-f1
MAC OUI	TYAN COMPUTER CORP.
Operating System	Linux 2.4/2.6 -= 2.6.7 (up: 11409 hrs)

Sent:		arp		tcp		udp		icmp	
Total Flows	641	Flows	257	Flows	367	Flows	2	Flows	15
Total Packets	10029	Packets	829	Packets	9035	Packets	145	Packets	20
Total Bytes	8057182	Bytes	49740	Bytes	7994474	Bytes	11540	Bytes	1428

Received:		arp		tcp		udp		icmp	
Total Flows	397	Flows	13	Flows	367	Flows	2	Flows	15
Total Packets	8382	Packets	808	Packets	7412	Packets	139	Packets	23
Total Bytes	2478355	Bytes	48480	Bytes	2391207	Bytes	37256	Bytes	1412

Top tcp source ports

Port(flows)	33022(175)	38505(13)	22033(7)	38502(2)	41866(1)	41833(1)	41846(1)	41835(1)	41743(1)	41803(1)
Port(pkts)	33022(5874)	22033(1276)	41753(133)	41760(60)	41763(59)	41778(53)	41782(45)	41834(41)	41779(36)	41726(33)
Port(bytes)										

Top udp source ports

Port(flows)	123(1)	33345(1)
Port(pkts)	33345(122)	123(23)
Port(bytes)	33345(9470)	123(2070)

Flow source 192.168.10.20

srcIP	srcMAC	srcPORT	dstIP	dstMAC	dstPORT	proto	pkts	bytes	duration	first pkt	last pkt
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.203	00-05-4e-41-ef-14	0(code)	icmp	1	60	0.0000	2007-01-05 20:15:59.4113-GMT	2007-01-05 20:15:59.4113-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	198.133.219.25	00-0f-66-1f-ee-b9	0(code)	icmp	6	588	5.0121	2007-01-05 17:54:09.441775-GMT	2007-01-05 17:54:14.453830-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.253	00-0f-66-19-2a-bd	0(code)	icmp	1	60	0.0000	2007-01-05 20:16:00.546929-GMT	2007-01-05 20:16:00.546929-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.255	BCAST	0(code)	icmp	1	60	0.0000	2007-01-05 20:16:00.538020-GMT	2007-01-05 20:16:00.538020-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.205	00-14-69-87-f7-7e	0(code)	icmp	1	60	0.0000	2007-01-05 20:15:58.987953-GMT	2007-01-05 20:15:58.987953-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.202	00-11-24-ed-eb-79	0(code)	icmp	1	60	0.0000	2007-01-05 20:15:59.3100-GMT	2007-01-05 20:15:59.3100-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.22	00-e0-81-26-88-83	0(code)	icmp	1	60	0.0000	2007-01-05 20:15:52.602188-GMT	2007-01-05 20:15:52.602188-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.254	00-07-40-fb-d2-85	0(code)	icmp	1	60	0.0000	2007-01-05 20:16:00.538126-GMT	2007-01-05 20:16:00.538126-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.21	00-e0-81-26-8a-05	0(code)	icmp	1	60	0.0000	2007-01-05 20:15:52.602144-GMT	2007-01-05 20:15:52.602144-GMT
192.168.10.20	00-e0-81-24-d5-f1	8(type)	192.168.10.25	00-10-7f-04-d0-9e	0(code)	icmp	1	60	0.0000	2007-01-05	2007-01-05

http://66.68.146.77:33022/smart/www/192.168.10.20.html#

Network Architecture: andwrigh@cisco.com
SMART: swaddell@cisco.com