RtPM

Cyber Security Tools

By Jim White
WiredCity, Div. of OSIsoft

OSISOFT USERS CONFERENCE 2004

DISCOVER YOUR PORTAL TO PERFORMANCE

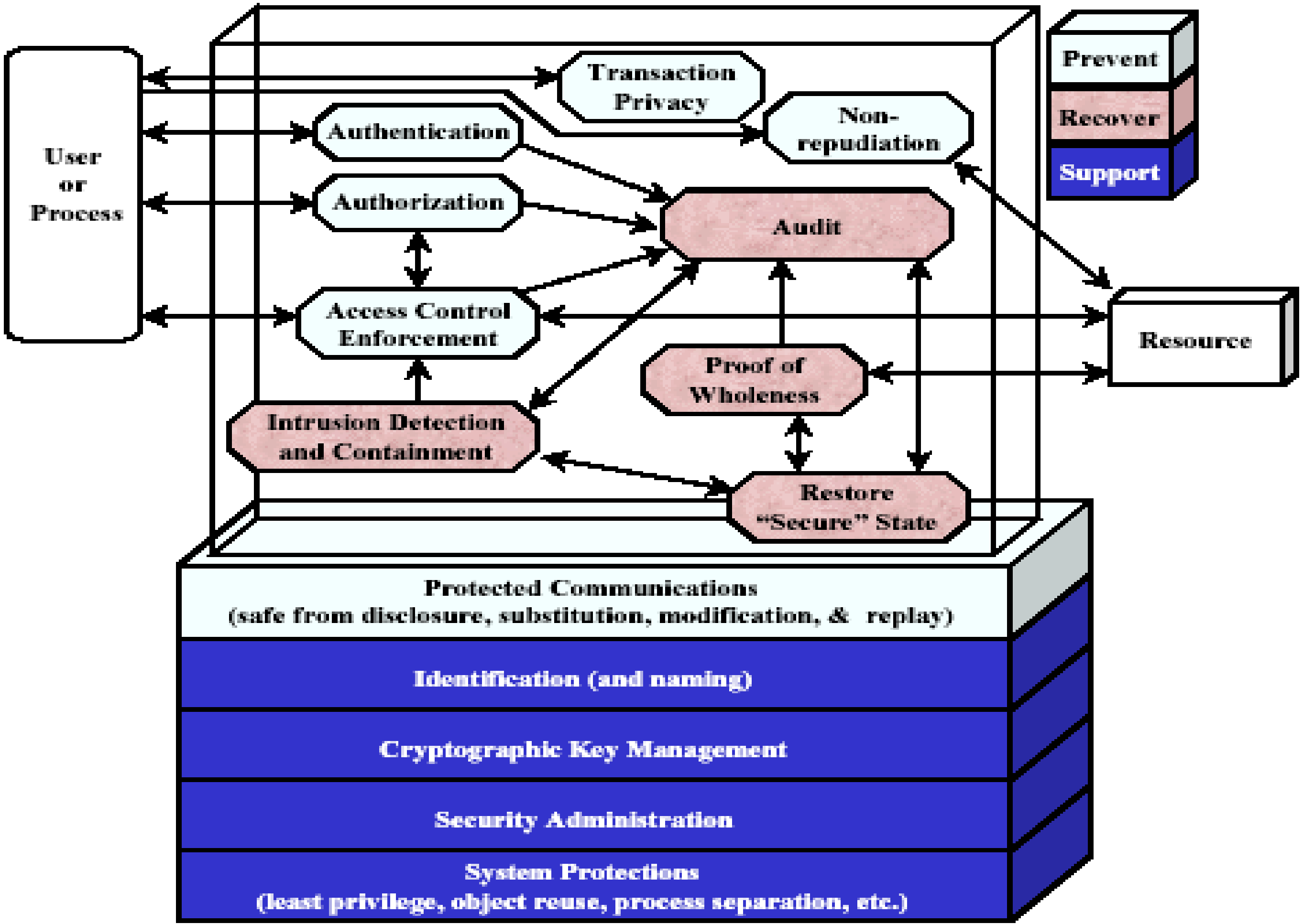
Security Tools

- The term “Tools”
  - – Not a replacement for experienced professionals (intelligence behind the wheel not under the hood)
  - – Not a substitute for good security policies and procedures
  - – Goals: Detect-Prevent-Delay-Mitigate

Security Tools

- Proliferating with increase in attacks
- Many claim to be “ the holy grail”
- Some marketing as “ the security solution”
- How do they fit into a security strategy

Security Service Model


Prevent
Recover
Support
User or Process
Transaction Privacy
Non-repudiation
Authentication
Authorization
Audit
Access Control Enforcement
Resource
Proof of Wholeness
Intrusion Detection and Containment
Restore "Secure" State
Protected Communications (safe from disclosure, substitution, modification, & replay)
Identification (and naming)
Cryptographic Key Management
Security Administration
System Protections (least privilege, object reuse, process separation, etc.)

Courtesy of NIST pub.800-33

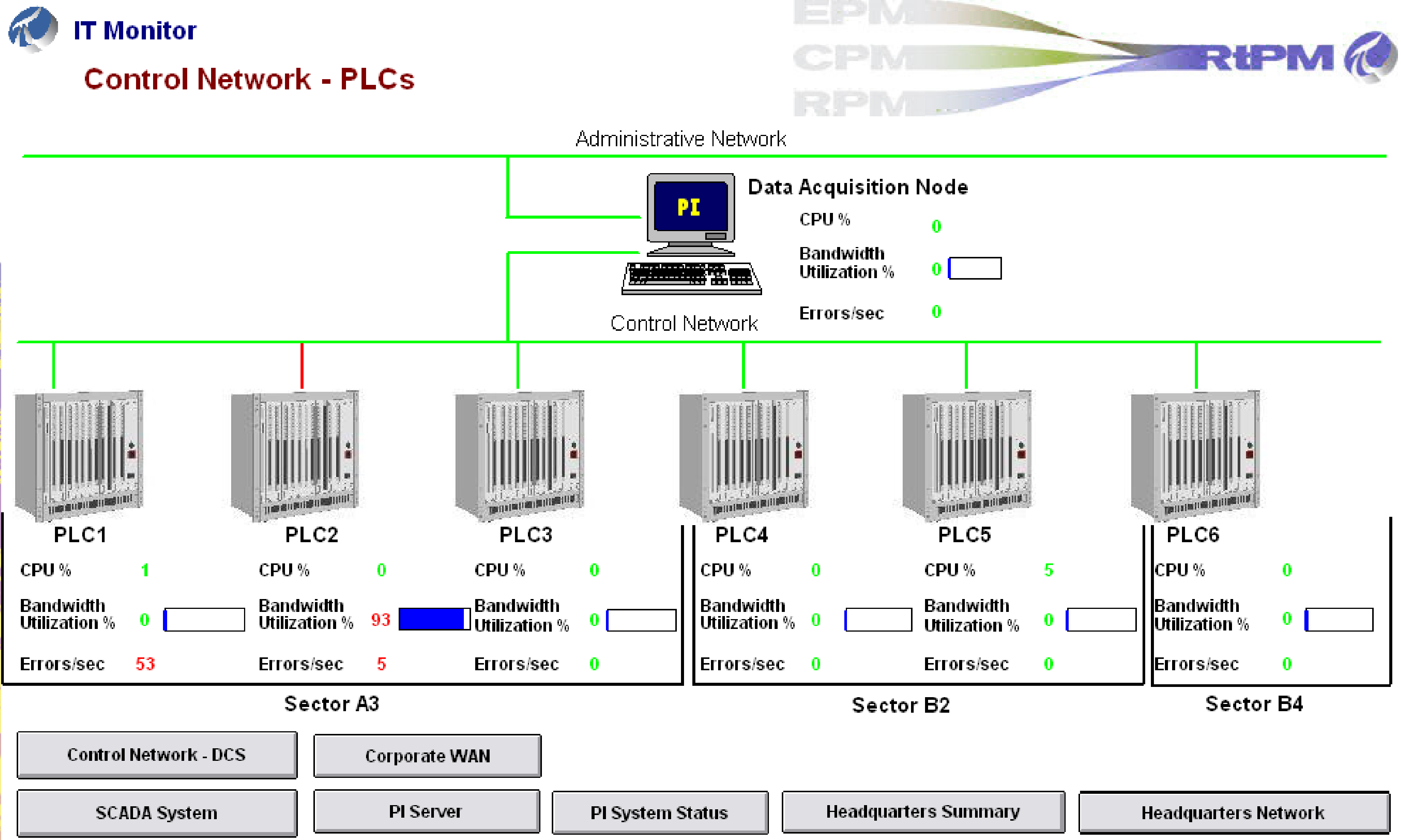
Security Tools

- Firewalls
- Host/Network based Intrusion Detection
- Intrusion Prevention Systems
- Network Scanners
- Security Event Management Systems
- File Integrity Systems
- Vulnerability Analyzers

Intrusion Detection Systems (IDS)

- Most IDS look for signature based suspicious activity
  - Known published attack signatures (i.e. viruses)
- New IDS models based on anomaly detection
  - Statistical
    - Baseline operations
    - Develop behavior profile
    - Look for statistical differences
    - Look for abnormal behavior
  - Packet signature or protocol anomalies

Intrusion Detection



IT Monitor

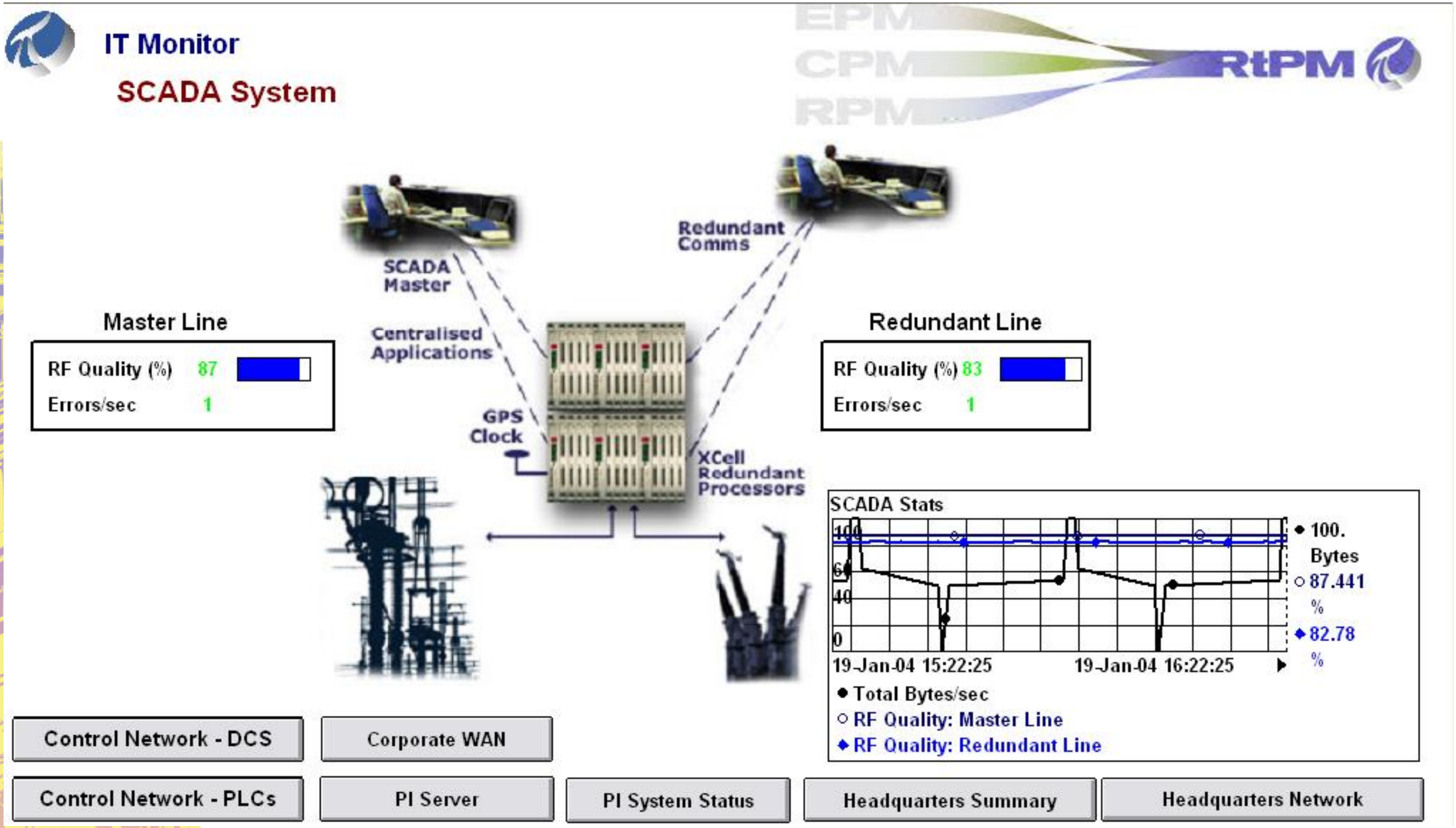
Control Network - PLCs

Data Acquisition Node

CPU %	0
Bandwidth Utilization %	0
Errors/sec	0

	PLC1	PLC2	PLC3	PLC4	PLC5	PLC6
CPU %	1	0	0	0	5	0
Bandwidth Utilization %	0	93	0	0	0	0
Errors/sec	53	5	0	0	0	0

Intrusion Detection



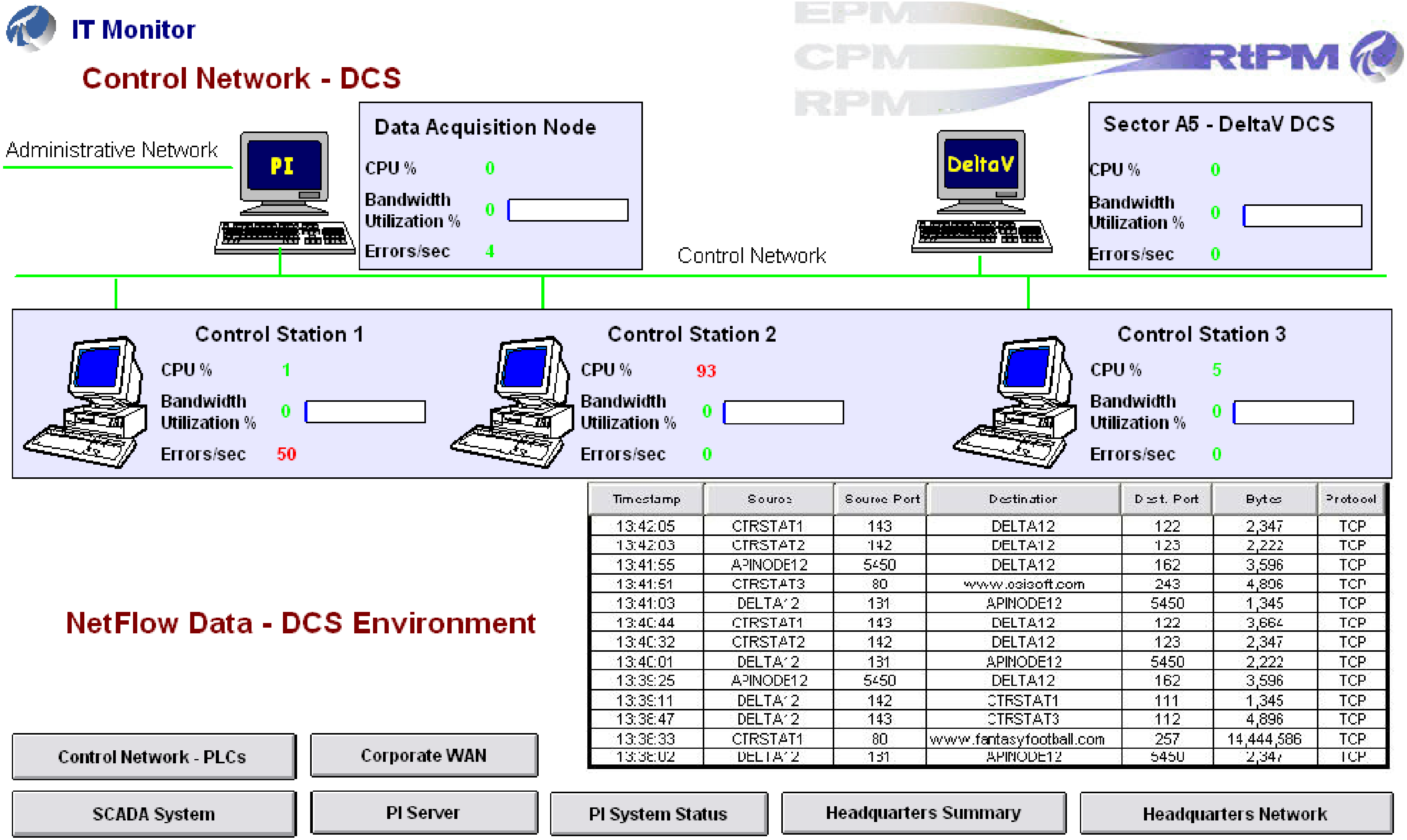
Master Line

RF Quality (%)	87
Errors/sec	1

Redundant Line

RF Quality (%)	83
Errors/sec	1

Intrusion Detection



IT Monitor

Control Network - DCS

Administrative Network

Control Network

PI

Data Acquisition Node

CPU % 0

Bandwidth Utilization % 0

Errors/sec 4

DeltaV

Sector A5 - DeltaV DCS

CPU % 0

Bandwidth Utilization % 0

Errors/sec 0

Control Station 1

CPU % 1

Bandwidth Utilization % 0

Errors/sec 50

Control Station 2

CPU % 93

Bandwidth Utilization % 0

Errors/sec 0

Control Station 3

CPU % 5

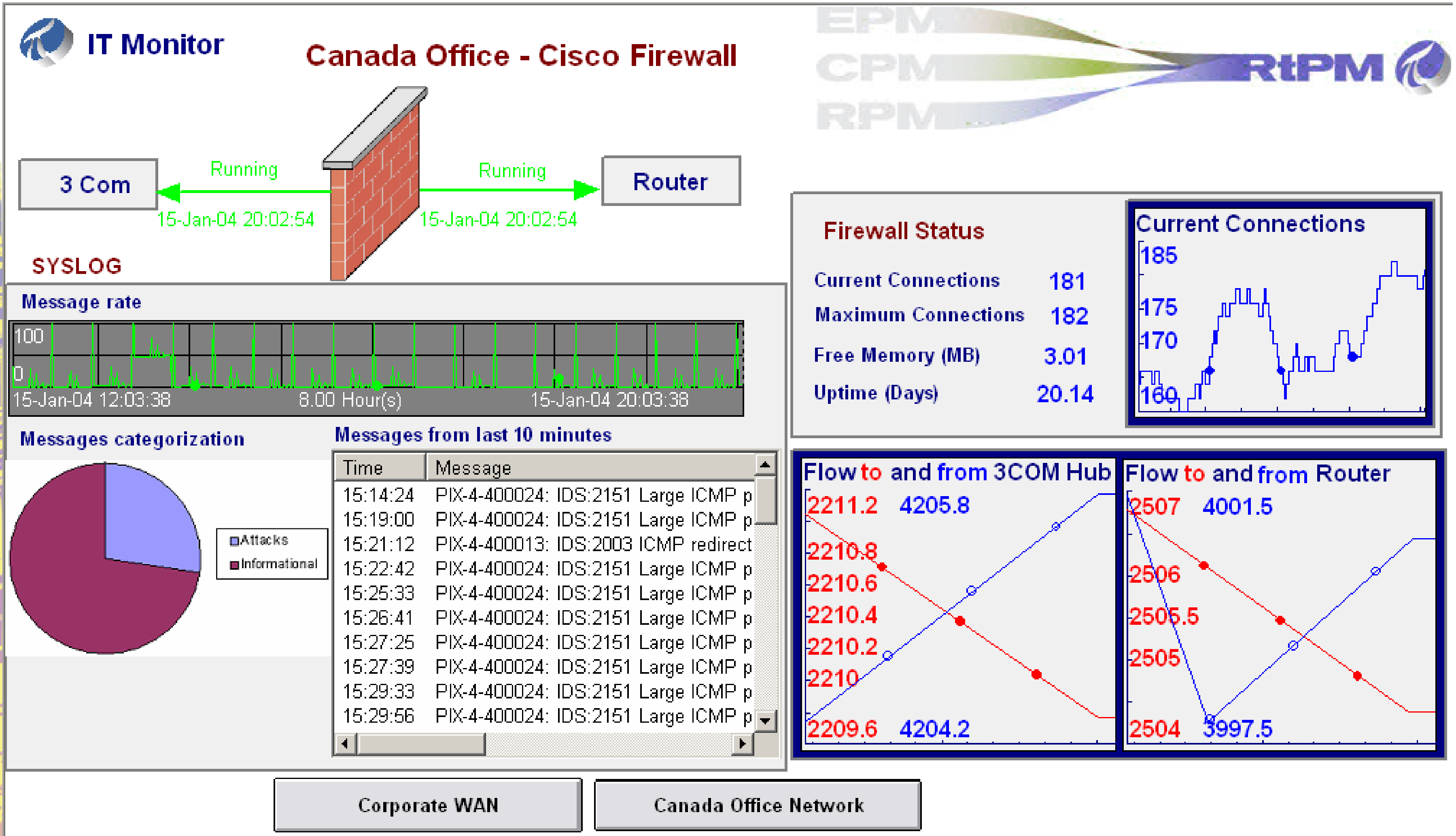
Bandwidth Utilization % 0

Errors/sec 0

NetFlow Data - DCS Environment

Timestamp	Source	Source Port	Destination	Dest. Port	Bytes	Protocol
13:42:05	CTRSTAT1	143	DELTA12	122	2,347	TCP
13:42:03	CTRSTAT2	142	DELTA12	123	2,222	TCP
13:41:55	APINODE12	5450	DELTA12	162	3,596	TCP
13:41:51	CTRSTAT3	80	www.osisoft.com	243	4,896	TCP
13:41:03	DELTA12	131	APINODE12	5450	1,345	TCP
13:40:44	CTRSTAT1	143	DELTA12	122	3,664	TCP
13:40:32	CTRSTAT2	142	DELTA12	123	2,347	TCP
13:40:01	DELTA12	131	APINODE12	5450	2,222	TCP
13:39:25	APINODE12	5450	DELTA12	162	3,596	TCP
13:39:11	DELTA12	142	CTRSTAT1	111	1,345	TCP
13:38:47	DELTA12	143	CTRSTAT3	112	4,896	TCP
13:38:33	CTRSTAT1	80	www.fantasyfootball.com	257	14,444,586	TCP
13:38:02	DELTA12	131	APINODE12	5450	2,347	TCP

Intrusion Detection



Firewall Status

Current Connections	181
Maximum Connections	182
Free Memory (MB)	3.01
Uptime (Days)	20.14

Messages from last 10 minutes

```
Time      Message
15:14:24  PIX-4-400024: IDS:2151 Large ICMP p
15:19:00  PIX-4-400024: IDS:2151 Large ICMP p
15:21:12  PIX-4-400013: IDS:2003 ICMP redirect
15:22:42  PIX-4-400024: IDS:2151 Large ICMP p
15:25:33  PIX-4-400024: IDS:2151 Large ICMP p
15:26:41  PIX-4-400024: IDS:2151 Large ICMP p
15:27:25  PIX-4-400024: IDS:2151 Large ICMP p
15:27:39  PIX-4-400024: IDS:2151 Large ICMP p
15:29:33  PIX-4-400024: IDS:2151 Large ICMP p
15:29:56  PIX-4-400024: IDS:2151 Large ICMP p
```

Intrusion Prevention System (IPS)

- Inline NIDS that acts like a bridge
  - Basically a NIDS with blocking capability of a firewall
  - Sits between systems needing protection
  - Unlike bridge, does packet content analysis for signatures
- Layer Seven switches
  - Looks at layer 7 info (DNS,HTTP,SMTP) and makes routing decisions
  - Good to protect against DOS attacks (known signatures)

Intrusion Prevention System (IPS)

- Application Firewall /IDS
  - Typically loaded on host to be protected
    - Comes with overhead that could be a management headache
  - Customizable to look for application behavior
    - Memory management
    - API calls
    - Interaction between application and operating system
    - Prevents by blocking unknown behavior
      - Can be dangerous for control systems

Vulnerability Scanners/Analyzers

- Passive fingerprinters
  - identifies host and devices on network
  - some will report services running
- Network vulnerability scanner
  - Views the network from a hacker’s perspective
  - Extremely noisy and prone to false positives
  - Dangerous
    - Crashes target in many cases

IT Security Tools

- No Tool is “ The answer”
- Always use a layered approach
  - “Security–in-depth”
- Implement good policies and procedures before tools