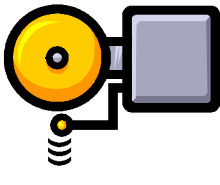
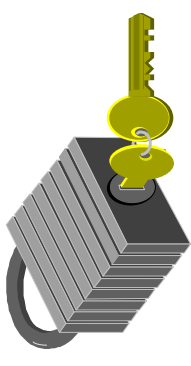




**Knowing the Available Technologies  
SCADA Security Workshop  
UTC Telecom 2004  
May 16-18, 2004**



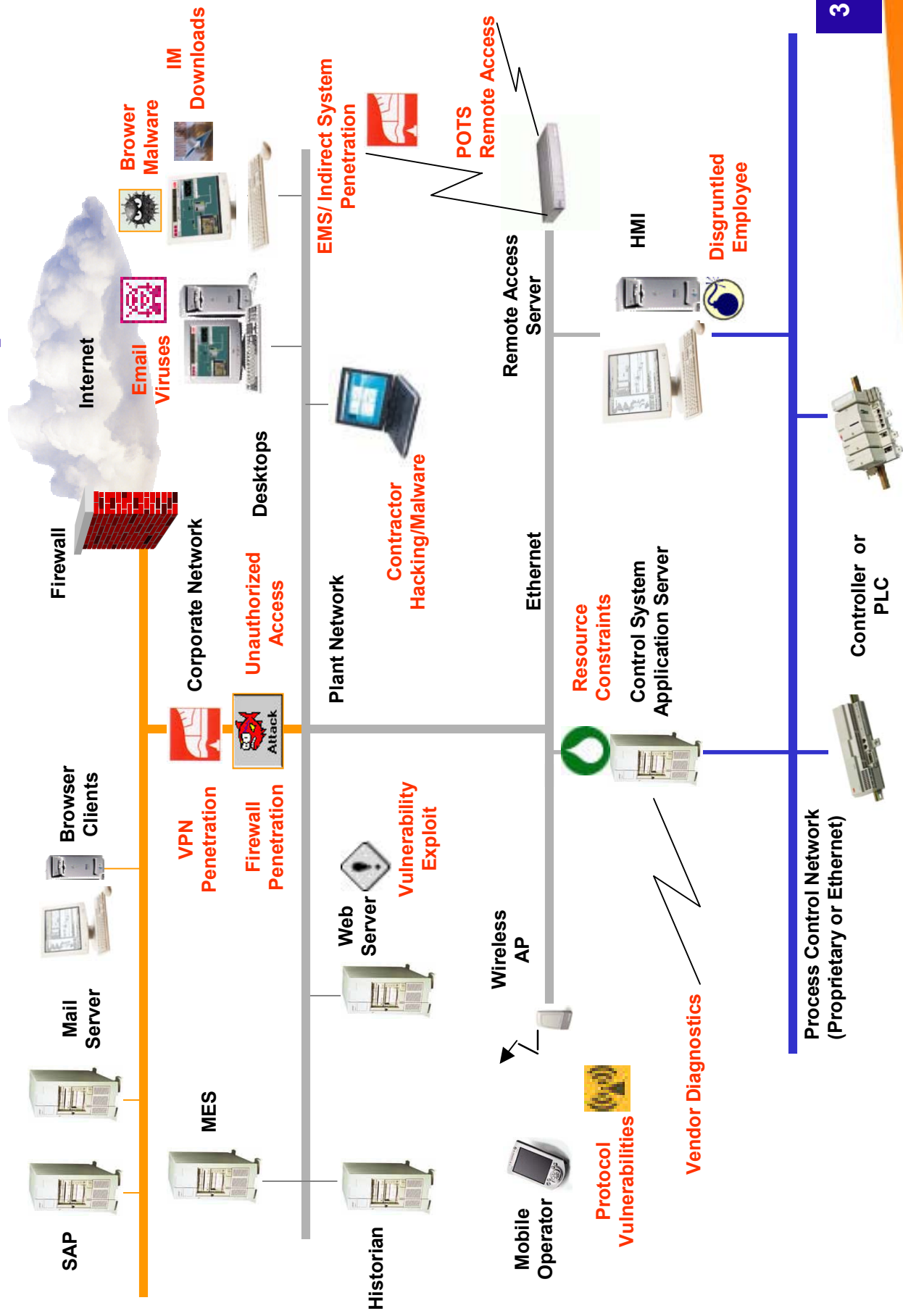
***Ron Derynck  
Director, Product Strategies  
rderynck@verano.com***

## What's Verano?

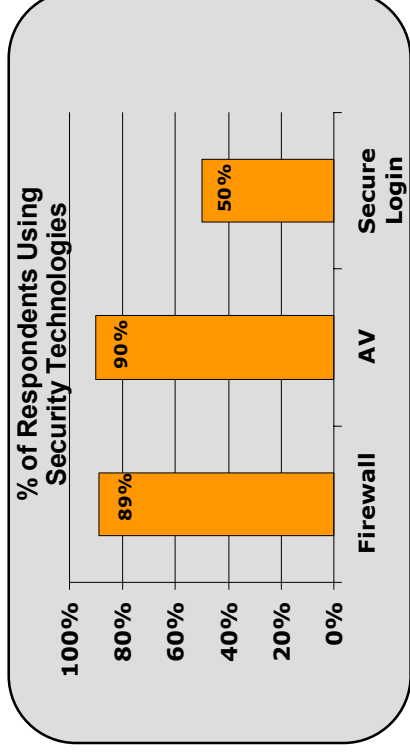
1. **The Spanish word for *summer***
2. **An industrial software company**
  - **Head Office near Boston, Mass**
  - **Software Development office in Calgary, Canada**
  - **2000 - acquired automation software business from HP**
  - **2002 - introduced Linux SCADA system**
  - **2003 - launches Industrial Defender product suite**



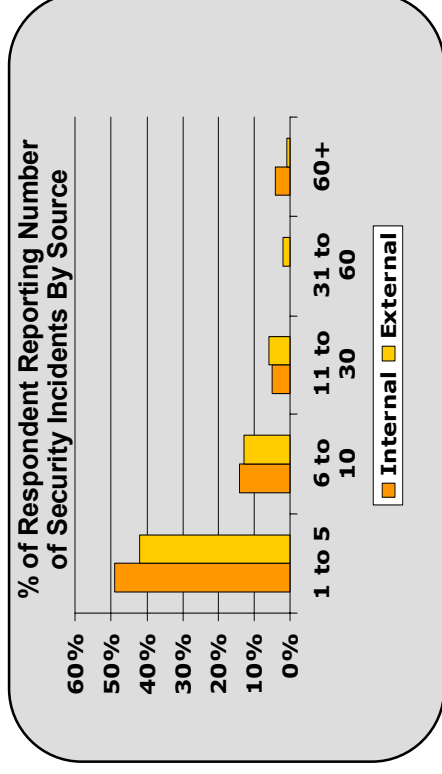
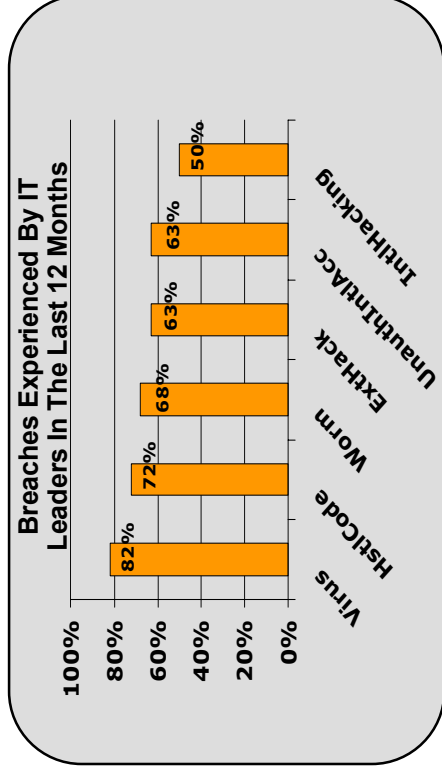
# Points of Potential Vulnerability



# Corporate Security Measures Are Not Sufficient



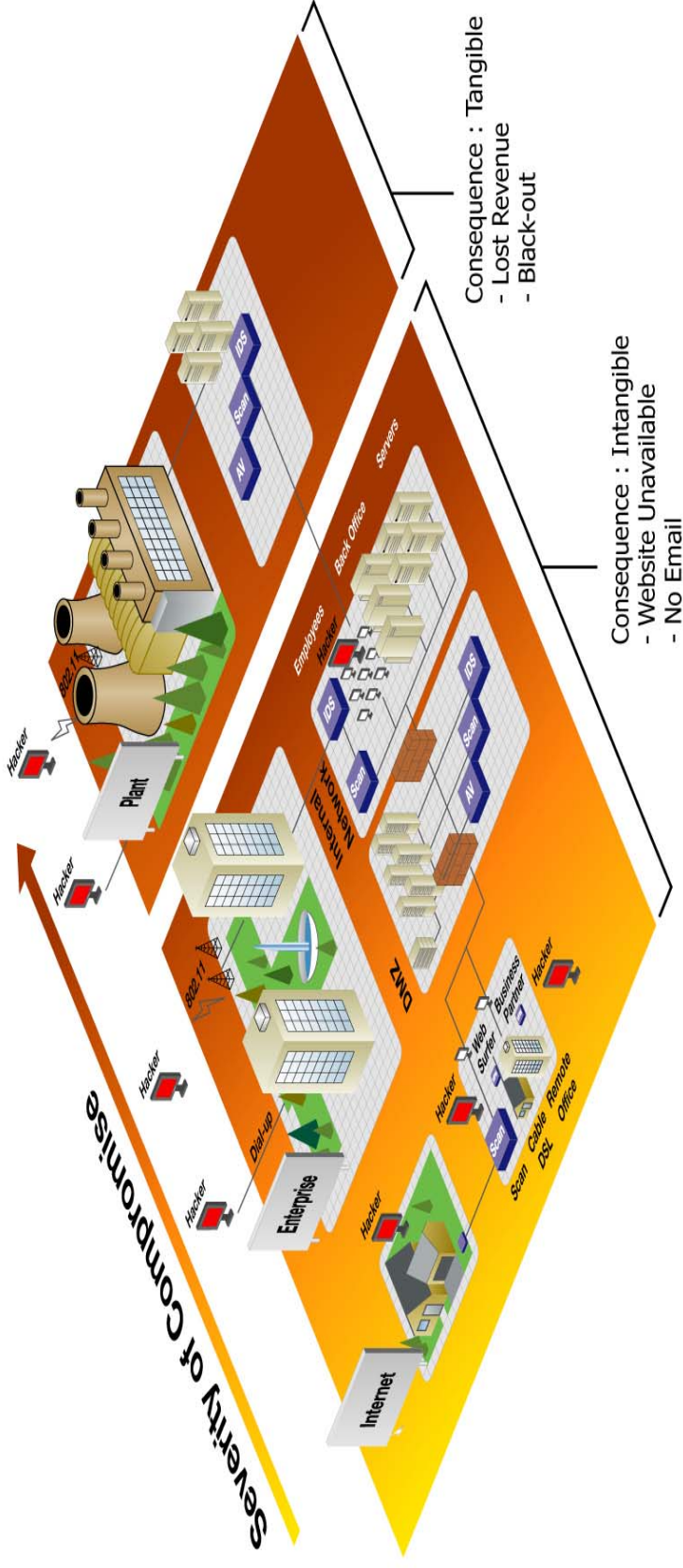
**External penetration still occurs...and no barrier to internal misuse exists**



Sources: 2002 FBI Survey, InfoTech Trends

# Control System Security Challenges

- Industry driven to open architectures over the last 10 years
- Control systems were not designed with security in mind
- Connecting IT and control networks created an access path for control network intrusion

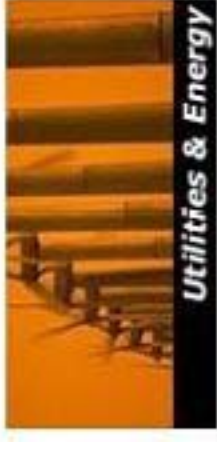


# Responding to the Challenge

- **Define and document your network perimeter**
- **Plan for "Defense in Depth"**
- **Protect against internal as well as external threats**
- **Segment your network**
- **Harden the control equipment**

# Special Considerations for Control Systems

- Differing risk management goals
- Differing architecture security focus
- Differing availability requirements
- Unintended consequences
- Time critical responses
- Differing response time requirements
- System software
- Resource constraints
- Information integrity
- Communications
- Software Updates



Source: ISA—TR99.00.02—2004 Integrating Electronic Security into the Manufacturing and Control Systems Environment



# Protecting the Control Network Perimeter



- **Firewall**
  - Ensures only authorized traffic enters the perimeter
- **Multi-port switches**
  - Segments traffic to maximize security
- **Network virus protection**
  - Detect and block incoming and outgoing viruses at the network perimeter
  - Control systems typically can/should not run AV
  - Best practices dictate you should have AV on the desktop and at the perimeter
- **In-line intrusion prevention**
  - Detect and block 1000+ types of intrusions
- **Content filtering**
  - Deep packet inspection to detect and remove threats and inappropriate content
- **VPN**
  - secures remote links
- **High availability**
  - load sharing and fail-over

## Multi-function security appliance

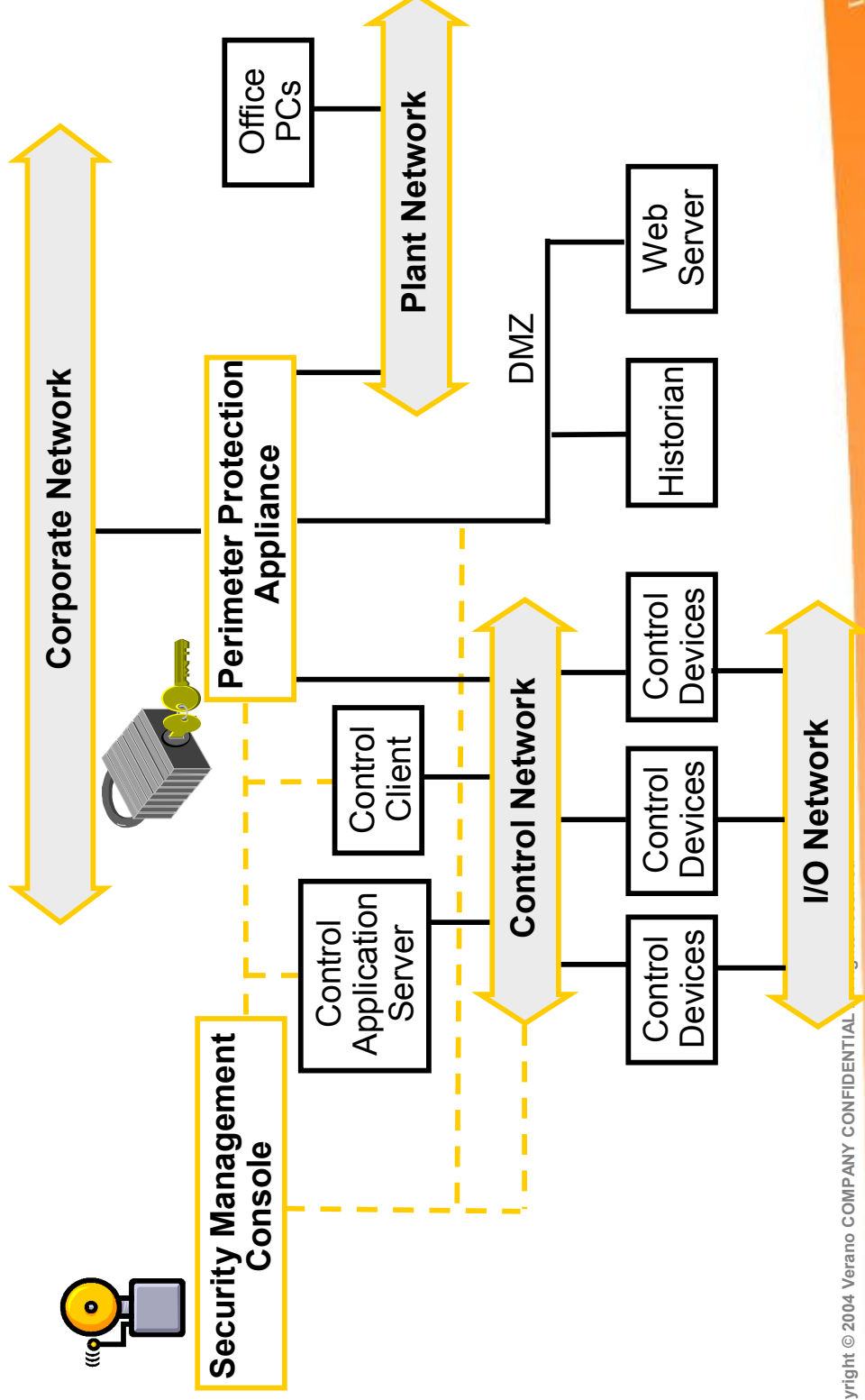




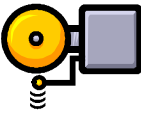


# Perimeter defense is a good start, but...

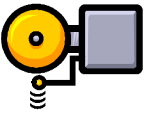
- Doesn't protect against internal threats
- Doesn't tell you when the perimeter has been penetrated
- Doesn't tell you when you have resource issues
- Doesn't tell you when devices are added to the control network



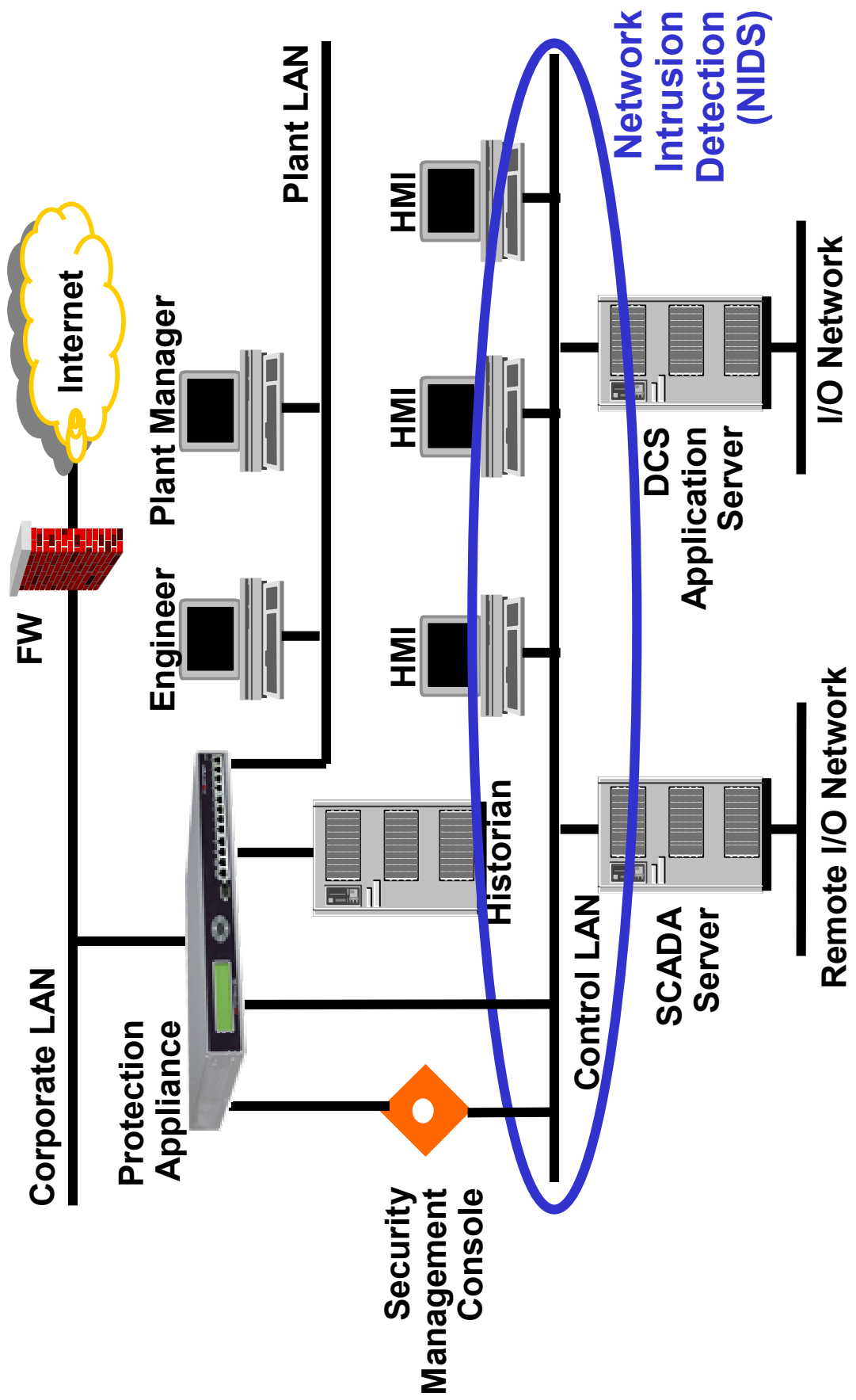
# Intrusion Detection Systems



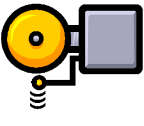
- **Network Intrusion Detection Systems (NIDS) - Systems that monitor network traffic and identify patterns that are deemed suspicious. NIDS uses passive packet sniffing to compare network traffic against a set of rules that determine whether the traffic indicates an attack.**
- **Host Intrusion Detection Systems (HIDS) - Software that monitors a system or application log files. These systems respond with an alarm or countermeasure when a user attempts to gain access to unauthorized data, files, or services.**



# Control Network IDS



# Intrusion Alert Example



Industrial Defender - Mozilla

File Edit View Go Bookmarks Tools Window Help

**INDUSTRIAL DEFENDER®** Refresh

Monitor Incidents Reports Metric Setup Admin Logout

Metric: watch Network IDS eth0 Priority 2  
Current Value: 0.0 msgs/10sec

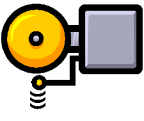
### Priority 2 vs. Time

log history:

Apr 7, 2004 11:55:46PM GMT+07:00

04/07-23:55:355.7976477 [\*\*] [1:20003:2] MS-SQL Worm propagation attempt [\*\*] {Classification: Misc Attack} [Priority 2] {UDP} 192.168.120.205:2196 -> 192.168.222.132:143

- Industrial Defender
- IT
- Guard
- HMI Stn 1
- HMI Stn 2
- HMI Stn 3
- SCADA Primary
- SCADA Backup
- Plant Web Server
- DCS Server 1
- DCS Server 2
- DCS Server 3
- Agent status
- DCS Agent
- Informational
- Network Traffic
- Resource usage
- Windows event logs
- Historian



# Beyond IDS

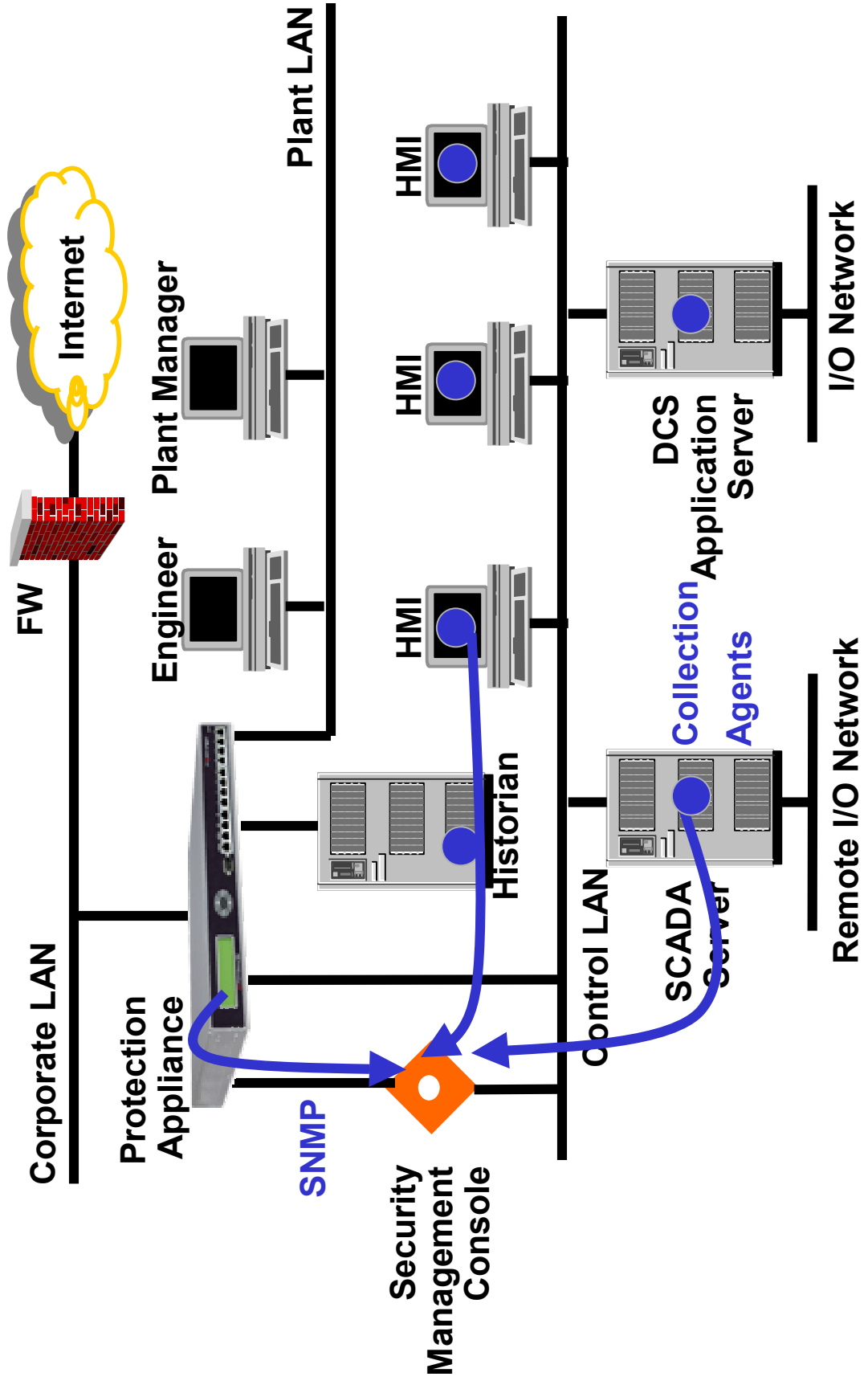
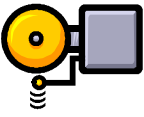
## Security

- ❑ **Control network intrusion detection**
  - control protocol signatures
  - control network anomalies
  - control network rules
- ❑ **Control network integrity**
  - Device addition
  - Device masquerading
  - Device continuity
  - Network equipment status
- ❑ **Host access monitoring**
  - Failed log-in attempts
  - Failed password change attempts
  - Password age status
  - Root user count
  - Total user count
- ❑ **Critical file monitoring**
  - File deletion, modification
  - File permission changes
  - File checksum mismatch

## Performance & Integrity

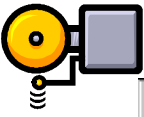
- ❑ **Host performance**
  - Resource Usage (CPU, disk space swap space)
  - Network traffic counts
  - Hardware status (CPU temperature, fan speed)
  - System Uptime
  - Identification (name, OS version, hardware type, IP address)
  - Event log status
- ❑ **Control application Integrity**
  - Installed software
  - Open listen sockets
  - Abnormal program exits
  - Control Application shutdown
  - Process terminations
  - Watchdog status
  - Message queue status

# Security and Performance Agents





# Performance Metric Example



Industrial Defender - Mozilla

File Edit View Go Bookmarks Tools Window Help

**INDUSTRIAL DEFENDER** Refresh Monitor Incidents Reports Admin Metric Setup Logout

- Industrial Defender
- IT
- Guard
- HMI Stn 1
- HMI Stn 2
- HMI Stn 3
- SCADA Primary
- SCADA Backup
- Plant Web Server
- DCS Server 1
- DCS Server 2
- DCS Server 3
- Agent status
- DCS Agent
- Informational
- Network Traffic
- Resource usage
- Windows event logs
- Historian

**Metric: DCS Server 3** Informational Configuration

OS version: DCS Server 3 x86 Windows 2000 Build 2195 (Service Pack 4)  
IP addresses: 192.168.1.110

**Metric: DCS Server 3** Informational Uptime  
value: up 5 days, 03:40

**Metric: DCS Server 3** Resource usage CPU usage  
Current Value: 3.4 percent

**CPU usage vs. Time**

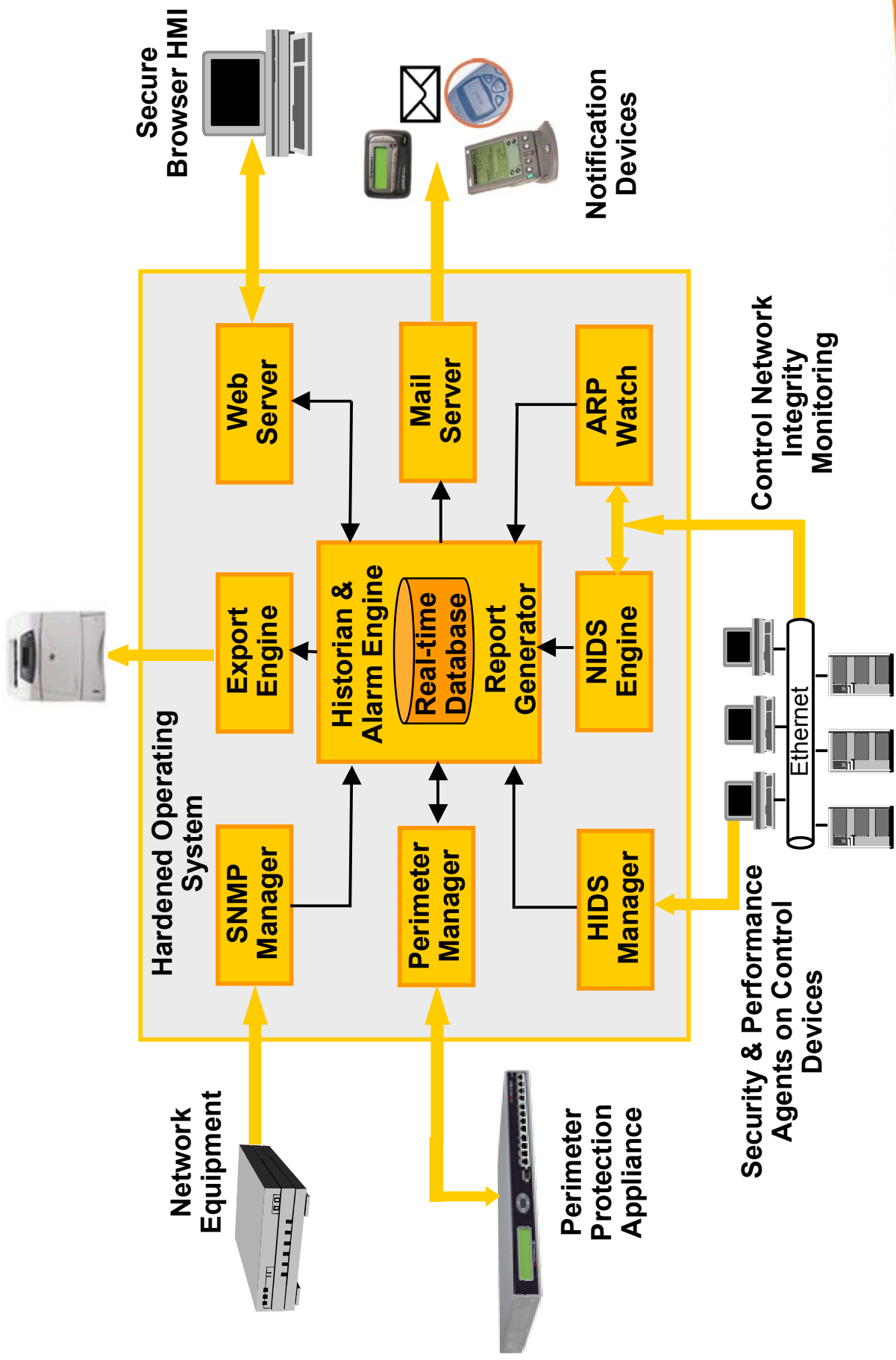
Consolidate

CPU usage (percent)

100  
90  
80  
70  
60  
50  
40  
30  
20  
10  
0

07:00 07:30 08:00 08:30 09:00 09:30 10:00 10:30 11:00

# Control Network Security Management System



# Conclusions



- **The increasing sophistication of cyber threats demands a multi-layered approach to protecting the security and integrity of mission critical systems.**
- **Threats are internal as well as external.**
- **Security Event Management systems designed specifically for control networks are now available.**



© Copyright 2004 Verano Inc. owns copyright content of this document and all attachments unless otherwise indicated. All rights reserved. Users of Verano Inc. software and tools associated with the software such as sales & marketing collateral, presentations, user manuals, training documentation etc. may not republish nor reproduce in whole or in part the information, in any form or by any means, in any manner whatsoever without the prior written permission of Verano Inc., and any such unauthorized use constitutes copyright infringement. An acknowledgement of the source must be included whenever Verano Inc. material is copied or published. If you require further information on a permitted use or license to reproduce or republish any material, address your inquiry to Verano Inc. Suite 120, 575 West Street, Mansfield, Massachusetts, 02048-1164. Any infringement of Verano Inc. rights will result in appropriate legal action. Verano Inc. disclaims any and all liability for any consequences which may result from any unauthorized reproduction or use of this Work whatsoever.