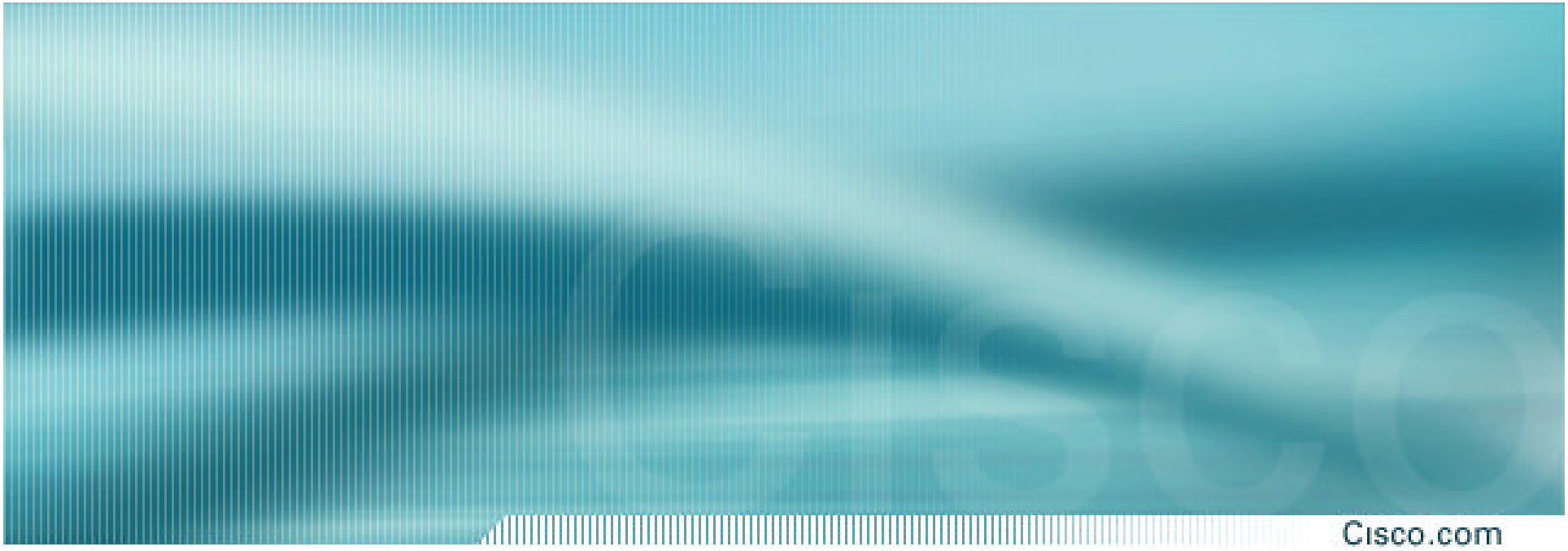


Integrating IT and Control System Security

A Vendor-Researcher Perspective

Matthew Franz (mfranz@cisco.com)

Critical Infrastructure Assurance Group (CIAG)

http://www.cisco.com/go/ciag/

Objectives

- Map out common ground between IT and control system security
- Refine control system vulnerability space and encourage more systematic analysis and testing
- Stimulate the development of technical requirements to enhance security products
- Identify mid to long-term research areas
- Get a sanity-check from folks in the trenches

Up Front Caveats

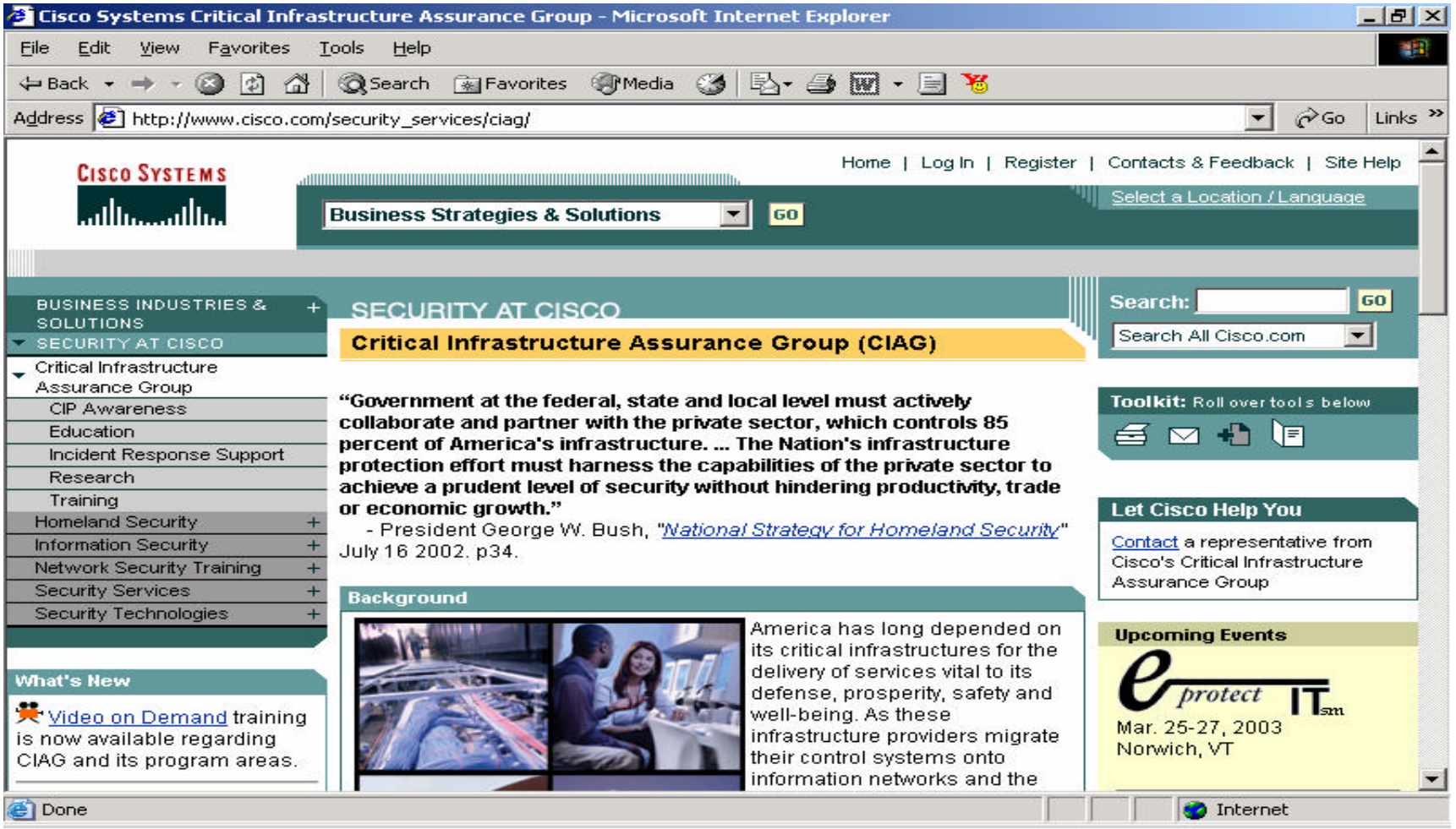
- I'm *just* a security researcher and relatively new to SCADA/DCS
- My primary focus has been looking at security in Industrial Ethernet protocols and devices
- I know I have a very IP-centric view of the problem
- My focus is on technology – I know that policy and culture are just as important if not more so
- Feel free to "educate" me after the presentation or off-line ☺

Agenda

- Introduction
- Cisco and control system security
- A outsider's view of the IT-control system gap
- Analysis of control system vulnerabilities
- Assessment existing security products and technology
- Recommendations
  - Device hardening
  - Protocol enhancement
  - Architecture development
- Conclusions

Critical Infrastructure Assurance Group (CIAG)

Cisco.com



http://www.cisco.com/go/ciag/

CIAG Research Initiatives

- **Internal Research Projects**
  - **BGP Security Analysis & Testing**
  - **TCP/IP Stack Evaluation**
  - **Protocol Implementation Test Tools**
  - **Mobile/Wireless Security**
  - **Secure BIND Replacement**
  - ***Control System Security***
- **Coordination & Advisory**
  - **Interface with Government Cyber Security Organizations**
  - **Industry Working Groups (AGA-12, SP99, IETF, etc.)**
- **Research Sponsorship**

Cisco's Interest in Industrial Networking

- **Industrial Ethernet is a new and growing market**
- **Identify unique security requirement to enhance Cisco products and secure customer networks**
- **Share our security expertise with the community**
  - **Participation in SCADA/DCS security initiatives**
  - **Collaboration with other vendors**
  - **External publication of findings**
- **Raise awareness of control system security issues– especially within IT security community**

CIAG Control System Research Initiatives

Vulnerability research – analysis and testing of design/implementation flaws in industrial products and protocols

Feature enhancement – identify new features in security and communication devices to reduce vulnerabilities and mitigate threats to control systems and networks

Architecture development – secure deployment and configuration of communication and security devices

Collaboration/advisory – participation in control system security forums and initiatives, leverage expertise in network and product security testing and evaluation

Some naïve observations…

- Seems to be a tendency to automatically reject the use of "IT" products, technology, and procedures–and a desire to reinvent the wheel
- There have been a few anecdotal presentations of some unique control system vulnerabilities, but no systematic analyses of device and protocol vulnerabilities have been published
- Widespread use fuzzy terminology and non-standard architecture
- Much of the focus on security solutions has been on encryption—and overcoming performance limitations
- How many SCADA/DCS security initiatives does it take to screw in a lightbulb?
- Just who are these much-maligned "IT folks" and what did they do to deserve the scorn of control engineers?

… and a few not so controversial assumptions

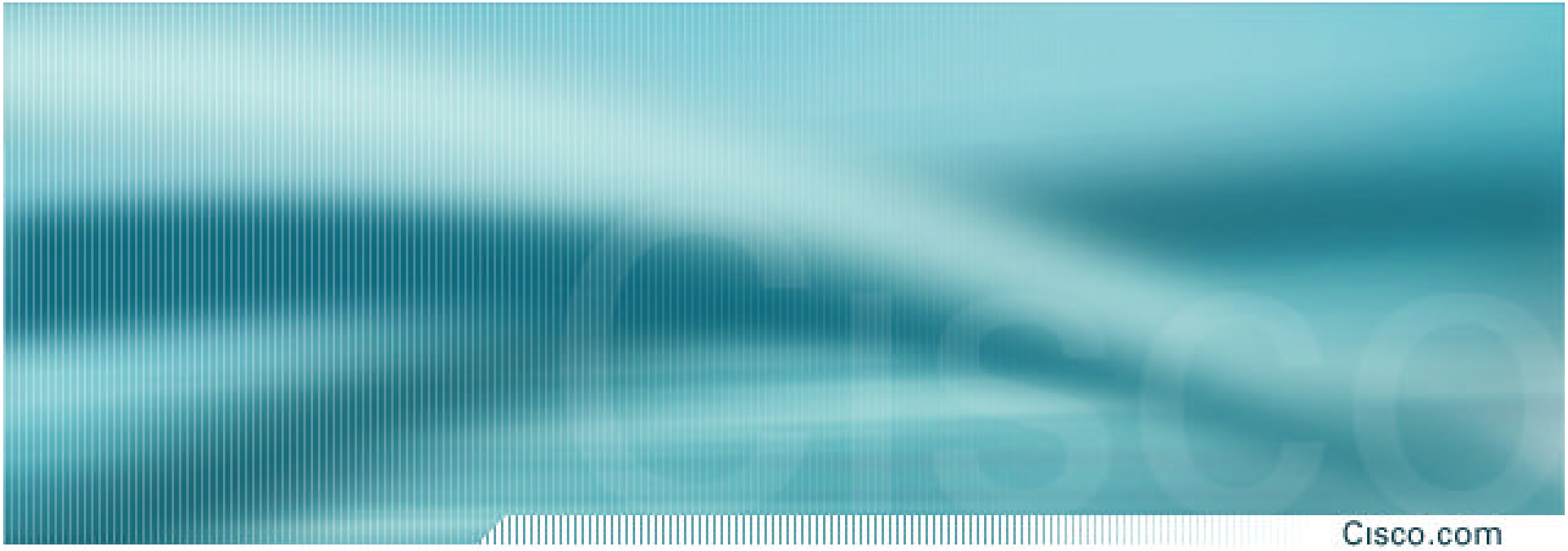
Cisco.com

- **We need to move the discussion from subjective cultural and operational differences between "IT" and "control systems" to objective technical requirements that can drive new products and technology**
- ***Communications systems* and Information Assurance (IA) principles are ubiquitous**

  Think in terms of threats and vulnerabilities that impact Nodes and Links and Protocols

  Risks must drive countermeasure design and implementation

- ***"IT"* may not be what you think it is!**
- **Users and vendors must accept responsibility for use of COTS for critical applications**



Analysis of control system vulnerabilities

Interest among Security Researchers?

“Have you already tried launching a DOS attack against an Allen Bradley PLC? I only have Siematic PLC's here with me to play with.”

Security Consultant on Pen-test Mailing List (9/28/2001)

Where do vulnerabilities occur in products, protocols, and systems?

- **Definition & Design**
  - **Inadequate or unrealistic security requirements**
  - **Lack of security features (i.e. encryption authentication authorization)**
- **Implementation**
  - **Insecure coding practices**
  - **Narrow focus on functionality testing**
- **Configuration & Deployment**
  - **Insecure features enabled by default**
  - **Failure to configure devices and applications properly**

Known Vulnerabilities in Control System Networks

Cisco.com

Design	Implementation	Configuration
Insecure comm links	TCP/IP stack issues?	802.11 Defaults
Insecure devices & protocols	Protocol flaws?	Weak/default passwords
Less than weak authentication in devices and protocols	OS/App flaws?	Inadequate filtering on router/firewall
Cleartext passwords	Windows HMI BO	OS defaults
Insecure remote access	WEP Flaws	
Undocumented commands/backdoors	Network infrastructure device DoS	

Product Evaluation (CC) | **Security Testing Code Audits** | **Vulnerability Assessments**

Threat-Vulnerability Analysis

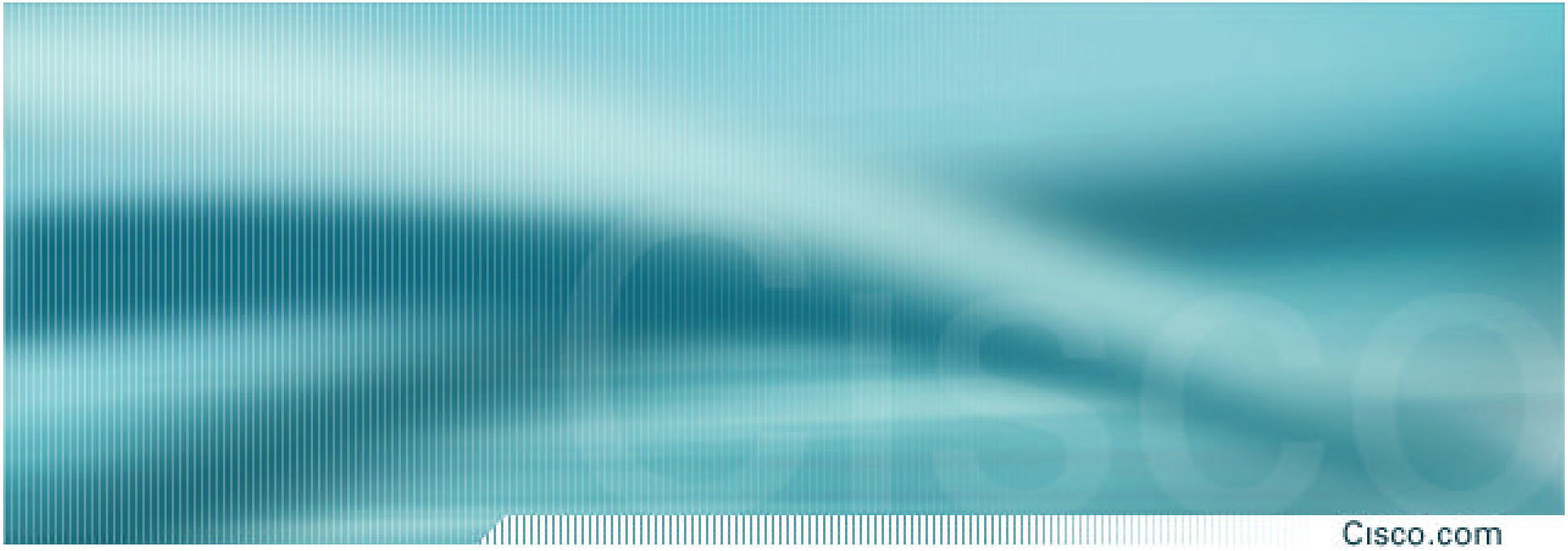
- **Impossible to anticipate/reproduce all attacks, but by exposing devices, protocols, and systems to a range of known and new attacks, we can:**
  - **Uncover (and hopefully eliminate) new vulnerabilities**
  - **Provide assurance that a given set of threats will not impact a product or network**
  - **Determine the effectives of countermeasures**
- **"Attack Trees" are a useful means of identifying potential attacks and organizing test results—start with a few high-level goals and then decompose**

Threat-Vulnerability Analysis (cont.)

- **Brainstorm "comprehensive" set of attack sequences, but only test a subset of attacks based on:**
  - **Sophistication required – known vulnerabilities, availability of exploit code and tools**
  - **Outcome of successful attack – read write modify degrade destroy**
  - **Techniques available – recon sniffing/replay flooding malformed hijacking/mitm**
  - **Access required – blind/non-blind local/remote authenticated/unauthenticated**

Vulnerability Reporting and Disclosure

- **Vendors should establish a security POC/team to handle product security incidents in a timely and effective manner**
  - **Issue security advisories–including 3rd party products**
  - **Determine level of detail and when to disclose**
  - **Identify fixes and workarounds**
- **Security researchers should inform vendors and follow "responsible disclosure" norms before going public with vulnerabilities**
- **Should the same rules/concerns as IT product apply to industrial devices?**



Analysis of existing security products and technology

The question of countermeasures

- **Security cannot be added everywhere**
- **So assuming we understand the control system requirements, threats, and vulnerabilities–where do we deploy countermeasures???**

  End devices – device authentication and authorization

  Protocol – message integrity and authorization

  Applications – user authentication and authorization

  Network Devices – protocol awareness, integrity, traffic encryption, user/traffic authentication

- **Assuming we can address performance, but how do we address complexity?**

Analysis of existing security technology

- **Network IDS**
  - If we don't know exactly what the vulnerabilities are, how can signatures be created?
  - How much understanding of protocol is necessary to detected attacks or anomalies?
  - How do we share alerts with operator consoles and other applications?
  - Passive IDS should have no impact on performance
- **Host-based FW/IDS/AV**
  - Compromise of general purpose OS is greatest risk?
  - HMI or other applications need extensive testing and vendor certification
  - May need safety override, depending on application?

Existing security technology (cont.)

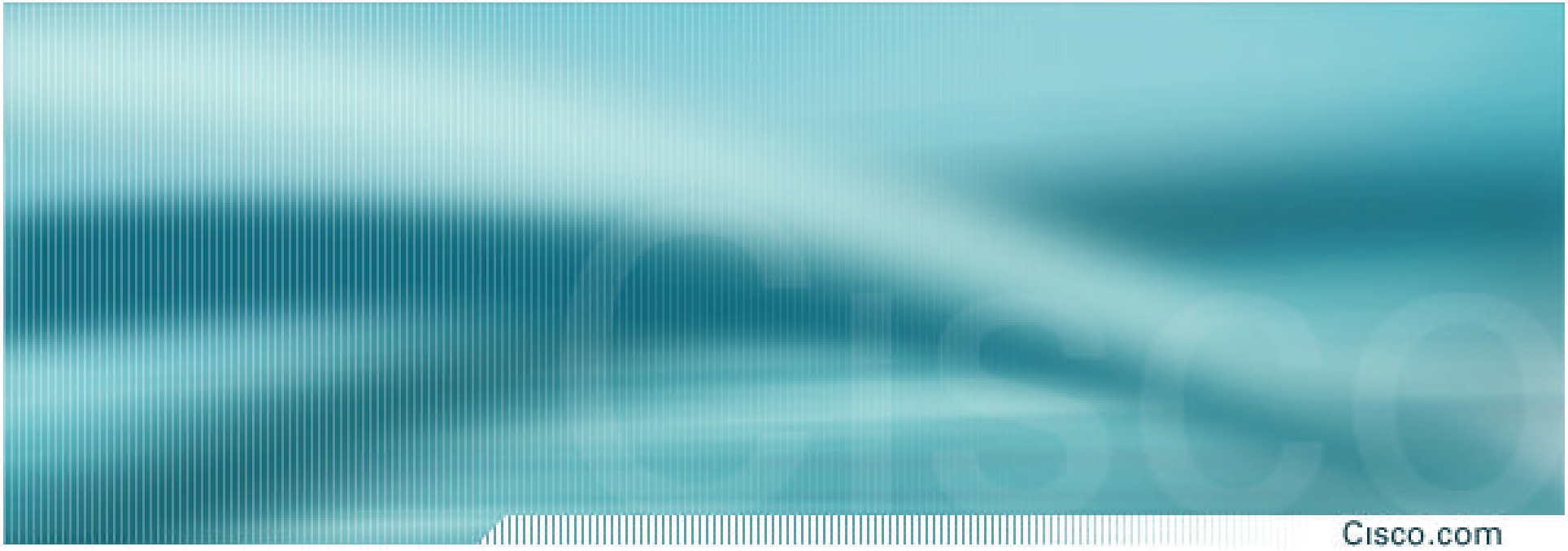
- **Network firewalls**
  - **Need appropriate rule-sets for specific control protocols and applications**
  - **Add application inspection of control system protocols (i.e. filter on Modbus/TCP function code)**
  - **How do we manage large numbers of micro-firewalls or is virtualization the answer?**
  - **Add filtering capability to Ethernet/Serial-Xbus devices**

Existing security technology (cont.)

- **VPN (LAN-LAN and Remote Access)**
  - **Not all control system traffic is “real time” (i.e. programming and configuration)**
  - **Protect traffic from enterprise (terminate on CS edge), but what about Internet VPN?**
  - **Provides more scalable authorization than access control lists?**
  - **Add protocol awareness and QoS—what can we learn from V3PN?**

Example of Securing Time Sensitive Traffic (V3PN)

- With VoIP we have had to deal with applications that can be significantly impacted by packet loss, delay, and jitter—across the Internet
- Protocol understanding of H323/SIP/Skinny added to firewalls
- Only possible with hardware acceleration
- Requires packet classification prior to encryption mark IPSEC datagrams
- Header compression required to address additional encapsulation layer (IPSEC/GRE)



Recommendations

Device Testing Baselines

- **Vendors and security researchers should conduct security testing against all Ethernet-enabled devices and communication modules**
  - **Determine TCP/IP/OS Signature**
  - **Conduct known TCP/IP attacks**
    - **Spoofing, Flooding, Malformed Messages**
    - **Well-known application-layer attacks**
  - **Evaluate unique protocols, features, or applications and test based on risk/criticality**

Protocol Security: Lessons from the Internet

- **Like control system protocols, the majority of Internet protocols were not designed with security in mind**
- **Retrofitting critical Internet protocols (i.e. BGP, DNS, etc.) has proven to be extremely difficult:**
  - **Vendors have been slow to implement security features**
  - **Customers seldom use available security features**
  - **Lack of realistic threat model and inadequate testing has slowed activity in standards bodies**
- **100% solutions are unlikely…**

Protocol Enhancement

- **Although the majority of protocols have minimal to no "security"—knowing only that doesn't help much**
  - **Security testing needs to be conducted against actual implementations in a realistic environment to determine the difficulty of exploitation and the true impact**
  - **Enhancements to the protocol and devices need to be bask on risk–what is the easiest to exploit and causes the greatest damage**
- **"Attack Trees" provide informal yet structured approach of performing technical risk analysis**
  - **Allow all likely compromise scenarios to be identified and analyzed**

Use of Attack Trees to Analyze Protocols

Cisco.com

- Develop list of high-level attacker goals that can be accomplished using the protocol
- Identify potential vantage points of the attacker to determine necessary preconditions for an attack to be successful
- Continue to refine attacks until they are specific enough to be tested, identifying all possible means of achieving the goal
- Develop attack trees for a specific site/application and link with protocol attacks to determine risk

Sample High-Level Attacker Goals for a SCADA Protocol

- Program a slave device
- Write data to a master
- Read data from slave
- Disable slave
- Compromise slave
- Disable master device
- Disrupt master-slave communications
- Compromise master

Attack Tree: Program Slave Device

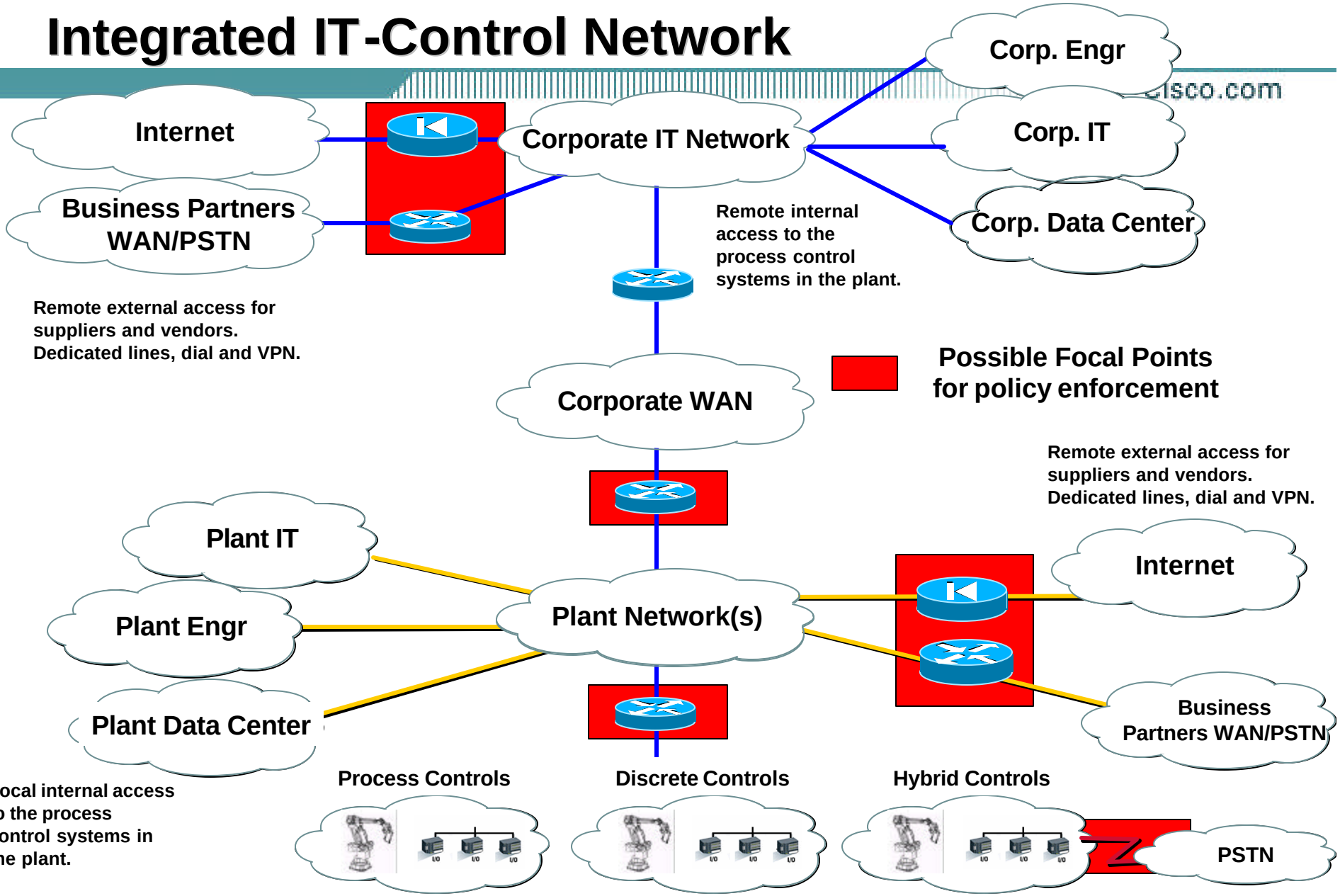
Cisco.com

```
OR  1. Program locally
       AND 1. Gain physical access
           2. Have programming software
           3. Learn/Guess Password
    2. Program via network
       OR  1. Have programming software
           2. Compromise master with
              programming capability
           3. Send SCADA protocol commands
```

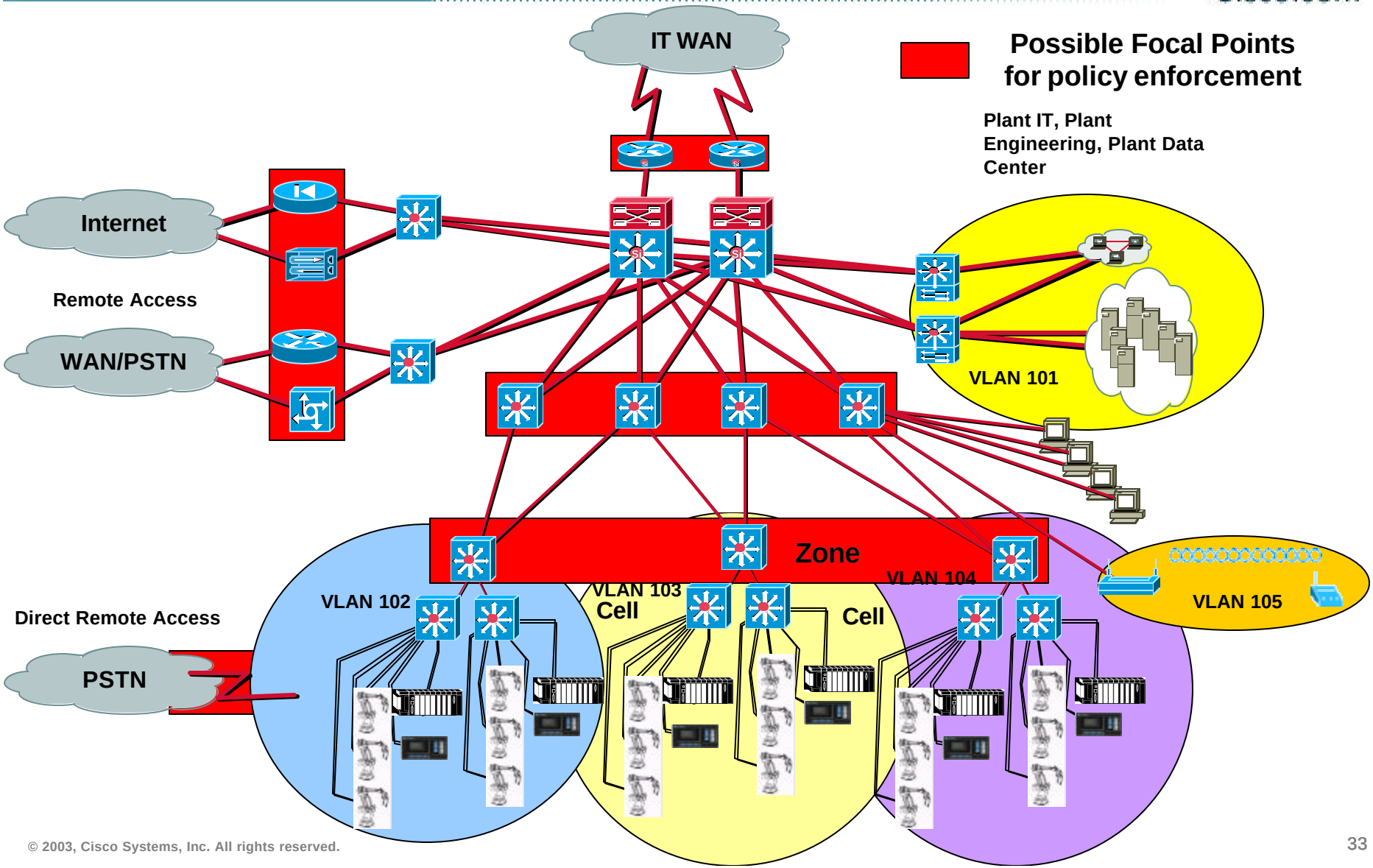
Architecture Definition & Development

- **Security reference architectures provide the necessary context for threat-vulnerability analysis and testing**
  - **What are the specific performance (latency, jitter, packet loss) requirements for the control system applications**
  - **Capture realistic assumptions about threats**
  - **Identify policy enforcement points, and traffic flows that need protection and**
  - **Integrates cyber and physical and allow system level vulnerability analysis**

Integrated IT-Control Network



Logical Industrial Ethernet Plant Topology

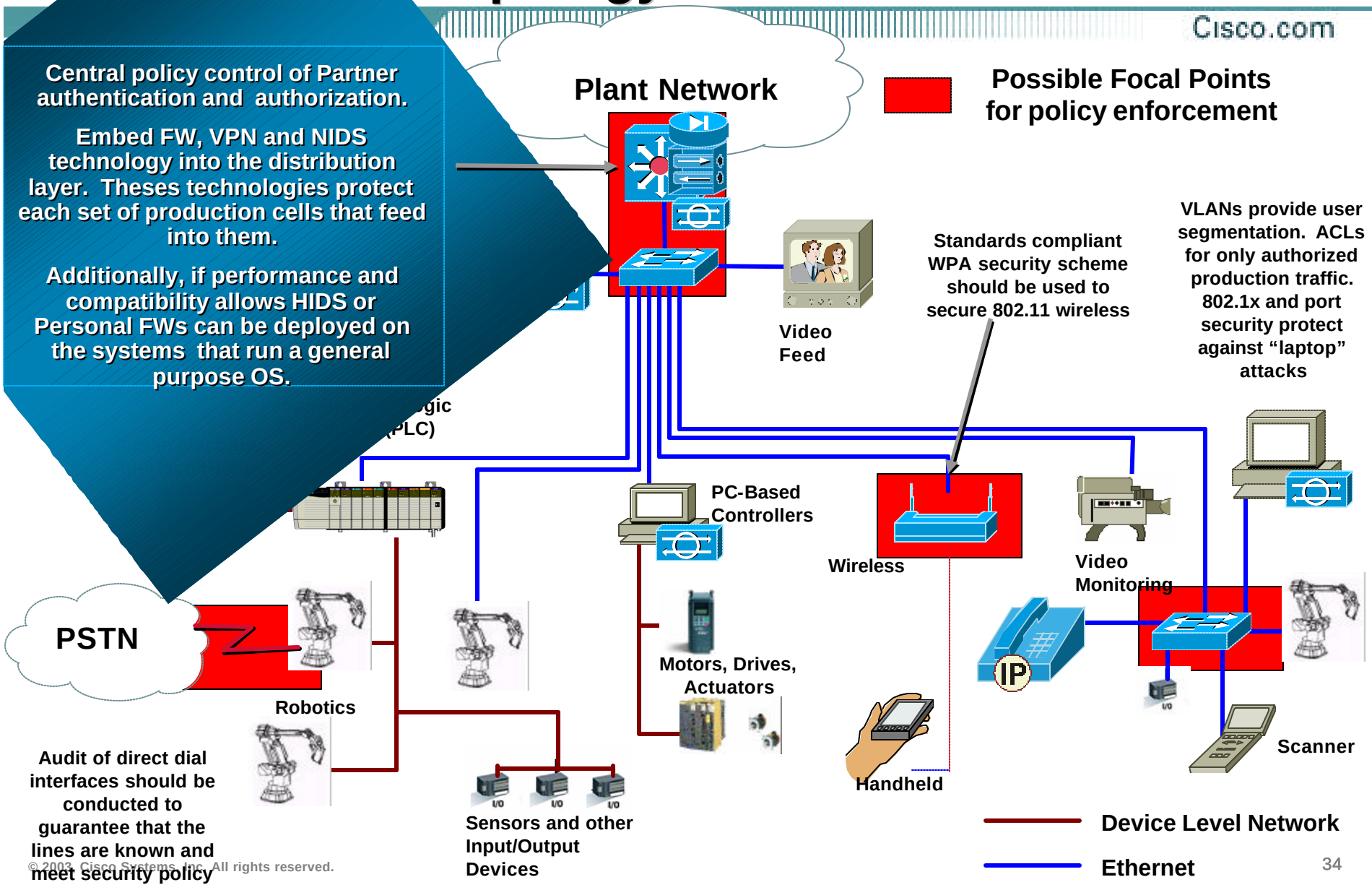


I e Topology

Central policy control of Partner authentication and authorization.

Embed FW, VPN and NIDS technology into the distribution layer. Theses technologies protect each set of production cells that feed into them.

Additionally, if performance and compatibility allows HIDS or Personal FWs can be deployed on the systems that run a general purpose OS.



Conclusions

- Significant testing effort is needed to identify specific device/protocol vulnerabilities as well as the effectiveness of countermeasure
  - How can we effectively use existing products
  - What new technology needs development
- Given the large number of security initiatives and multi-faceted problem/solution space, what concrete actions need to be taken stakeholders
  - Researchers
  - Vendors (both IT and automation)
  - System integrators and consultants
  - Customers
- What are the cyber-physical interdependencies—what can really be done assume compromise of network devices and comm links?

References

- "Attack Trees: Modeling security threats." *Dr. Dobb's Journal* December 1999 by Bruce Schneier

  http://www.counterpane.com/attacktrees-ddj-ft.html

- "An Attack Tree for the Border Gateway Protocol." Convery, Cook, Franz.

  http://www.ietf.org/internet-drafts/draft-convery-bgpattack-00.txt

- "Attack Modeling for Information Security and Survivability." Moore, A., Ellison, R. and R. Linger, March 2001.

- RFPolicy 2.0

  http://www.wiretrip.net/rfp/policy.html

References (cont.)

- **Cisco PSIRT**

  http://www.cisco.com/go/psirt

- **Voice and Video Enable IPSec VPN (V^3PN)**

  http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/v3pn/index.shtml