GLOBAL THINKING...GLOBAL SOLUTIONS™

Defense-in-Depth Strategies for Secure, Open Remote Access to Control System Networks

A look at multi-vendor access strategies

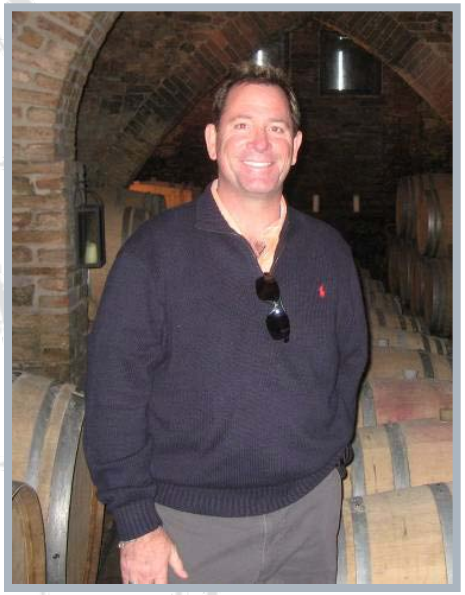
Joel Langill
TÜV FSEng ID-1772/09, CEH, CPT, CCNA
Security Consultant / Staff Engineer
ENGlobal – Automation
Houston, Texas

About the Presenter

Joel Langill is a Staff Engineer and Security Consultant for ENGlobal's Automation segment based in Houston, Texas. ENGlobal is a specialty automation contractor and solution partner with many of the leading control system vendors.

Joel brings a different slant to industrial security, focusing more on the importance of people and processes in order to combat potential threats and how this fits into a comprehensive defense-in-depth strategy.

Joel is a TÜV certified Functional Safety Engineer, Certified Ethical Hacker, Certified Penetration Tester, and a Cisco Certified Network Associate, and is a member of ISA84, ISA87 and ISA99 committees. He has contributed to various technical publications and magazines on security, and is a featured writer for InfoSec Institute relating to ICS security.



ID: 1772/09
S I S
TÜVRheinland FS Engineer

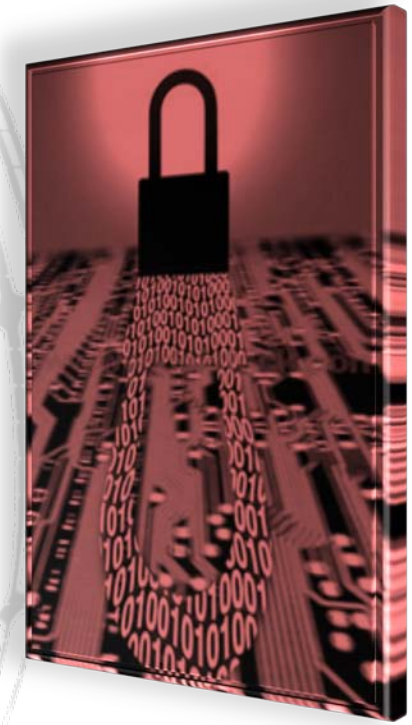
CCNA
CISCO
CERTIFIED

C|EH
Certified Ethical Hacker

CERTIFIED PENETRATION TESTER
IACRB

Topics Covered

- Understanding the Security Perimeter
- Industrial Control System Landscape
- Cyber Threat Trends
- Control System Vulnerabilities & Security Issues
- Unique Aspects of Remote Access
- Security Objectives of Remote Access
- Defense-in-Depth Strategies
- Industry Standards
- Tools
- Additional References



Where is the Perimeter?

Free Wi-Fi
for everyone.
Now at Starbucks.

Who is Securing the Perimeter?

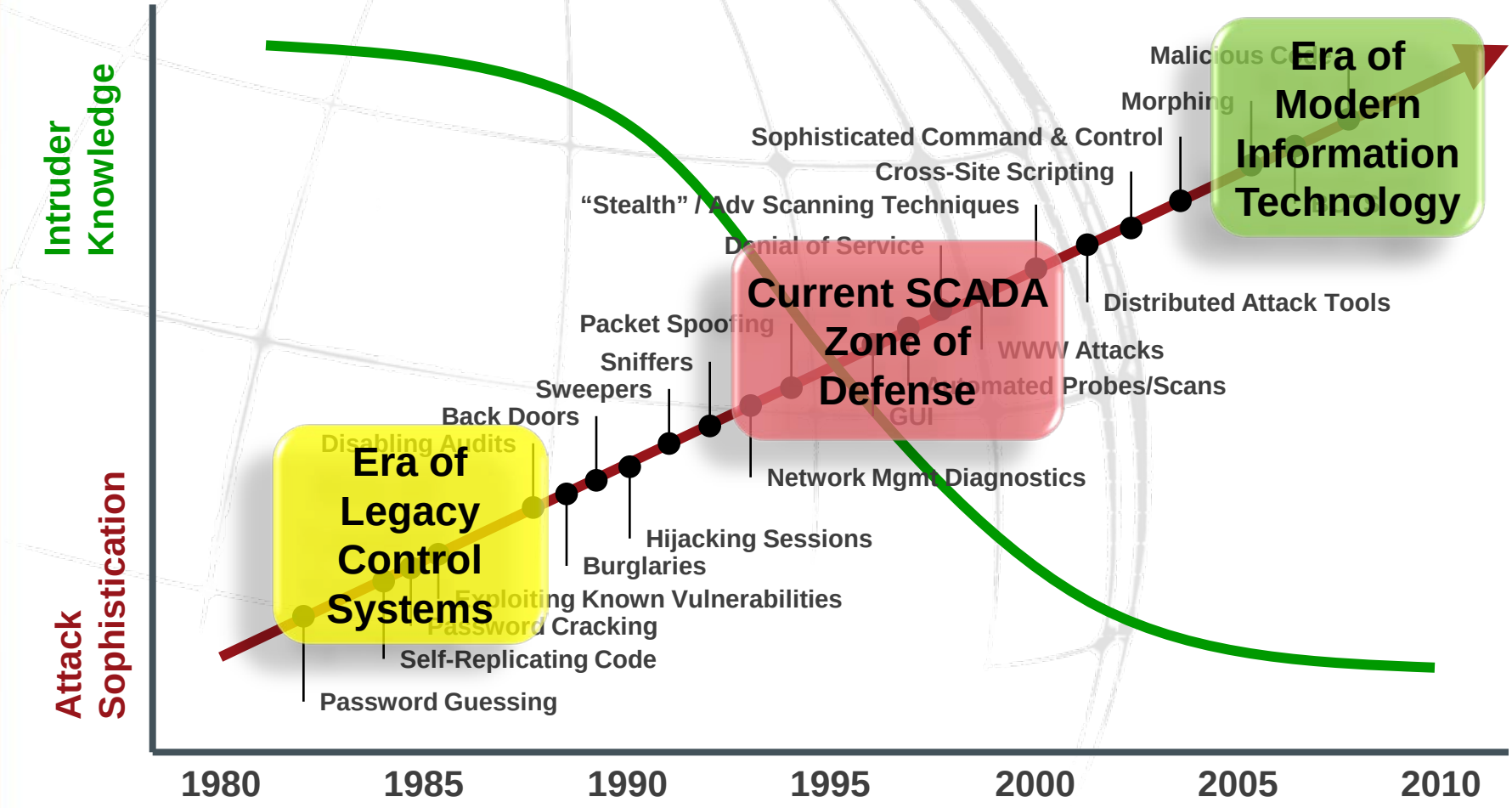
Industrial Control System Landscape

- Modern networking increases manufacturing productivity and reduces costs through integration of external, corporate and control system networks
- Protocols and communication standards that provide this increased interoperability are often the same technologies that have been exploited and compromised on the Internet and corporate networks
- Leads to vulnerabilities that can significantly reduce the cyber security posture of a manufacturing organization
- Can expose mission-critical control systems to cyber threats

Why is the problem escalating?

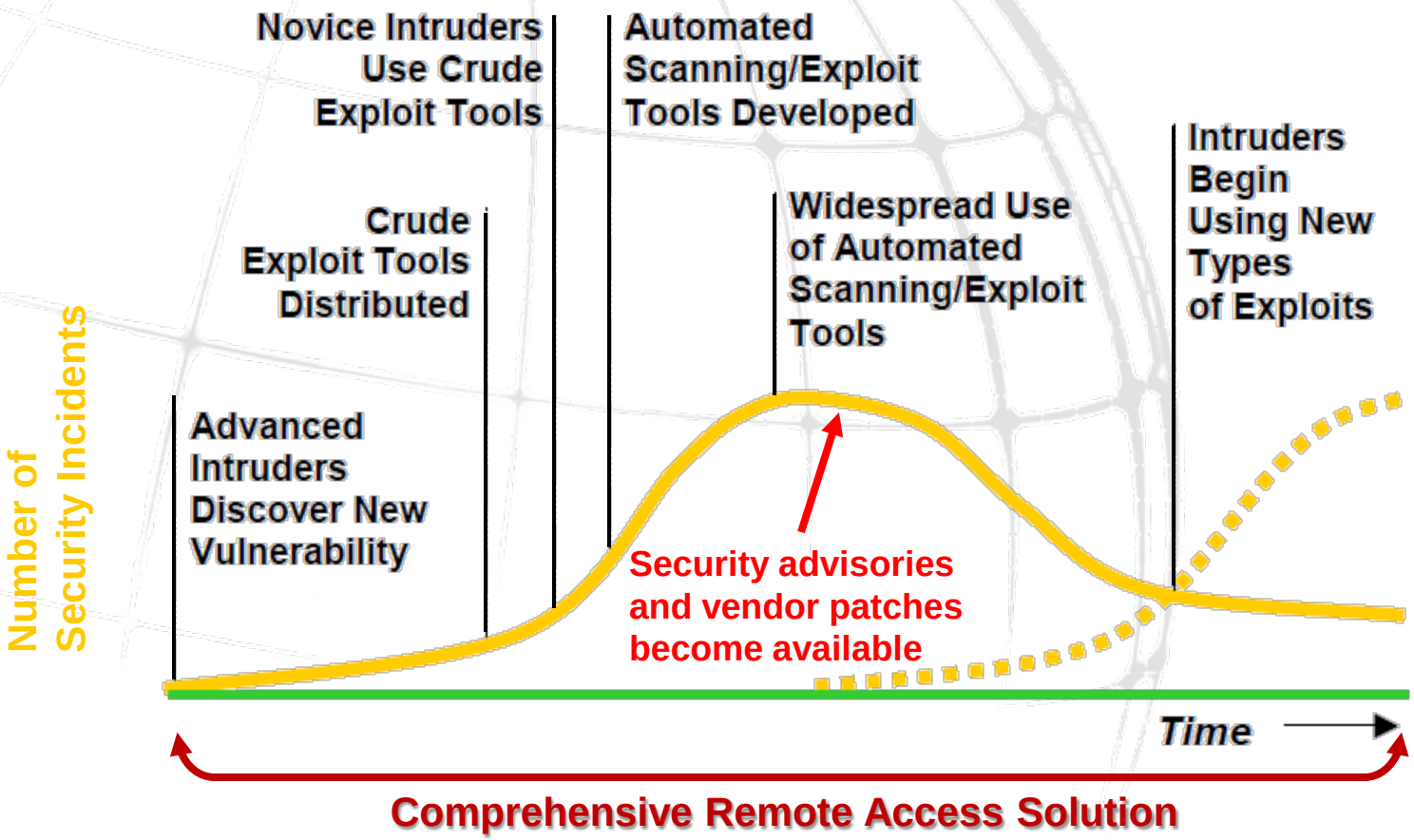
- Insecure connectivity to external networks
- Usage of technologies with known vulnerabilities
- Lack of qualified cyber security resources
- Lack of a cyber security business case and security program specific to control systems
- Vendors provide features that are often only enabled if the engineer/administrator is aware of the capability
- Control system protocols lack basic security functionality such as authentication and authorization
- Open source information

Cyber Threat Trends



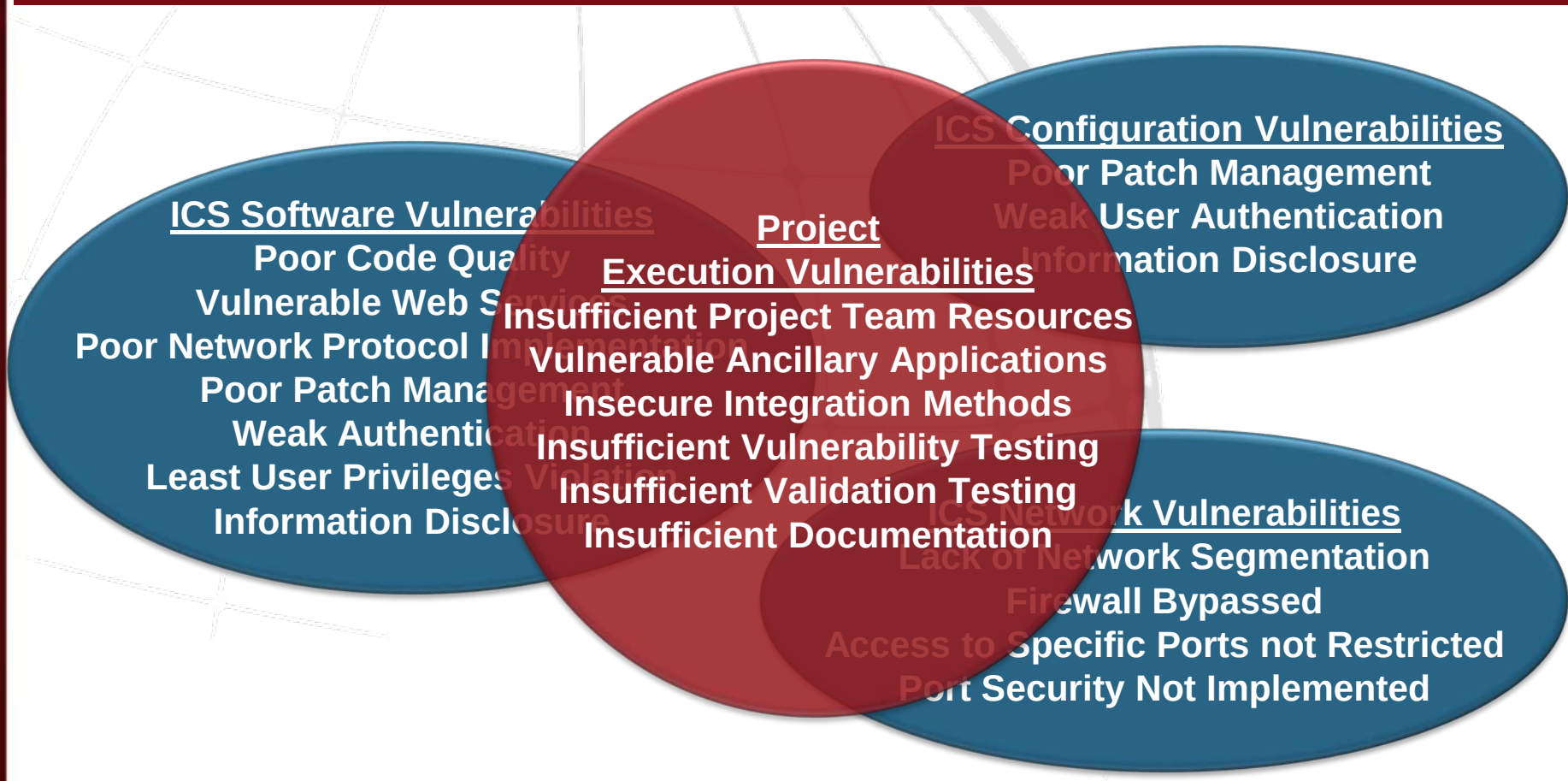
Lipson, H. F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009, November 2002

Staying ahead of the curve



Lipson, H. F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009, November 2002

Control System Vulnerabilities

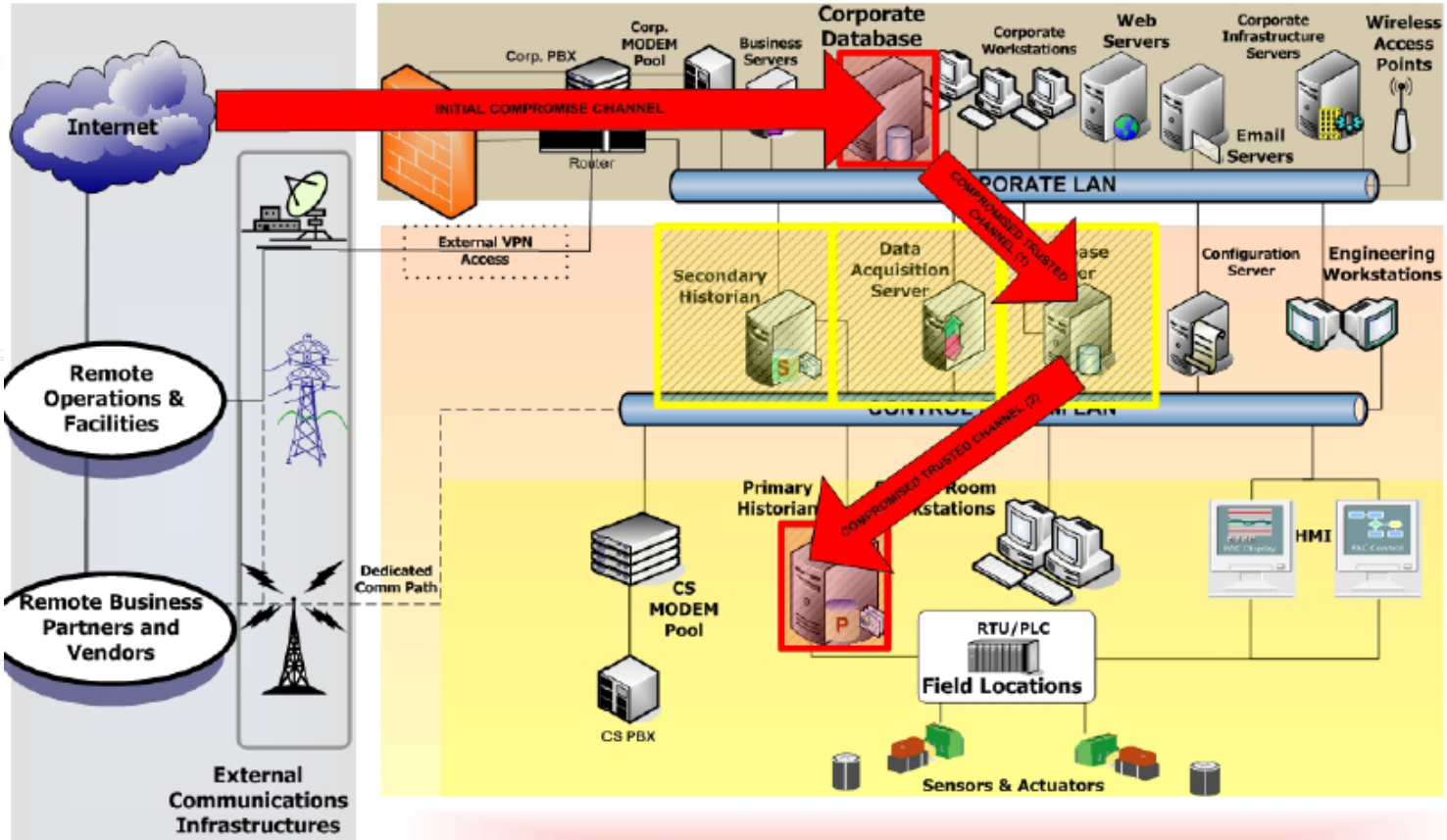


"Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments", DHS CSSP, July 09
"Incorporating Cyber Security into your Automation Project's Execution Methodology", ENGlobal, April 2010

Addressing Control System Cyber Security Issues

- Backdoors and “holes” in the network perimeter
- Devices with little or no security features
- Vulnerabilities in common protocols
- Attacks on field devices
- Database attacks
- Communications hijacking and Man-in-the-Middle attacks
- Improper or nonexistent patching of software and firmware
- Insecure code techniques
- Improper cyber security procedures for internal and external personnel
- Lack of control systems specific mitigation technologies

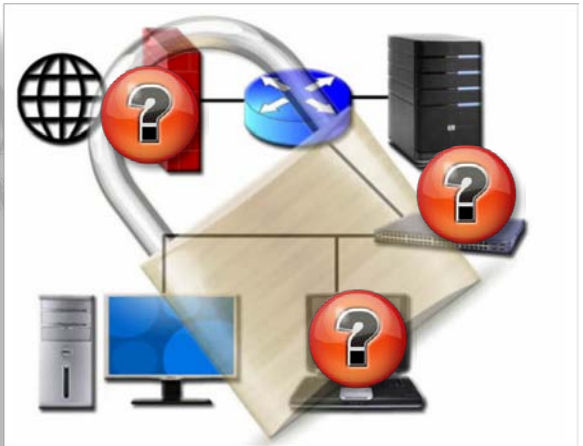
Attacking via Databases and Trusted Relationships



A Simple VPN+Firewall Solution is Not Enough

“”Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense in Depth Strategies”, DHS CSSP, October 09

Security Objectives for Remote Access

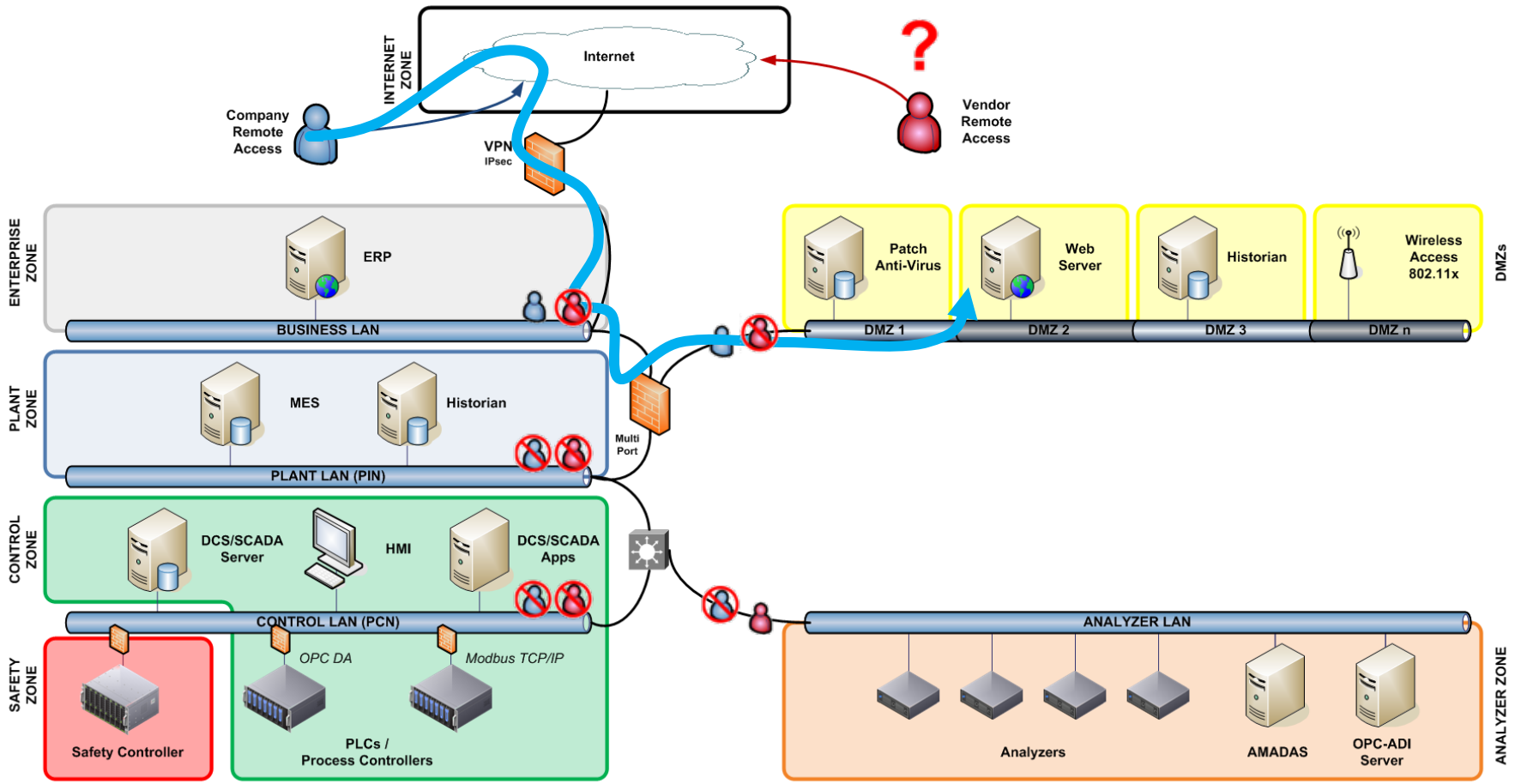


- **When designing a remote access solution for control system networks, the following security objectives should be considered:**
  - "Keep the bad guys out of the network"
  - "Keep the bad guys in"
  - "Keep everyone in the playground"
  - Completely isolate the remote client from specific networks (PCN, PIN, ELAN, WAN)
  - Encrypt all data in transit outside the enterprise
  - Monitor remote access traffic for any unusual or suspect activity
  - Correlate information from multiple-sources for rapid threat identification
  - Ability to quickly revoke access
  - Platforms are not company-controlled which limits applications, policies, etc.
  - Must consider various IT security policies including required firewall configurations, port access, etc.

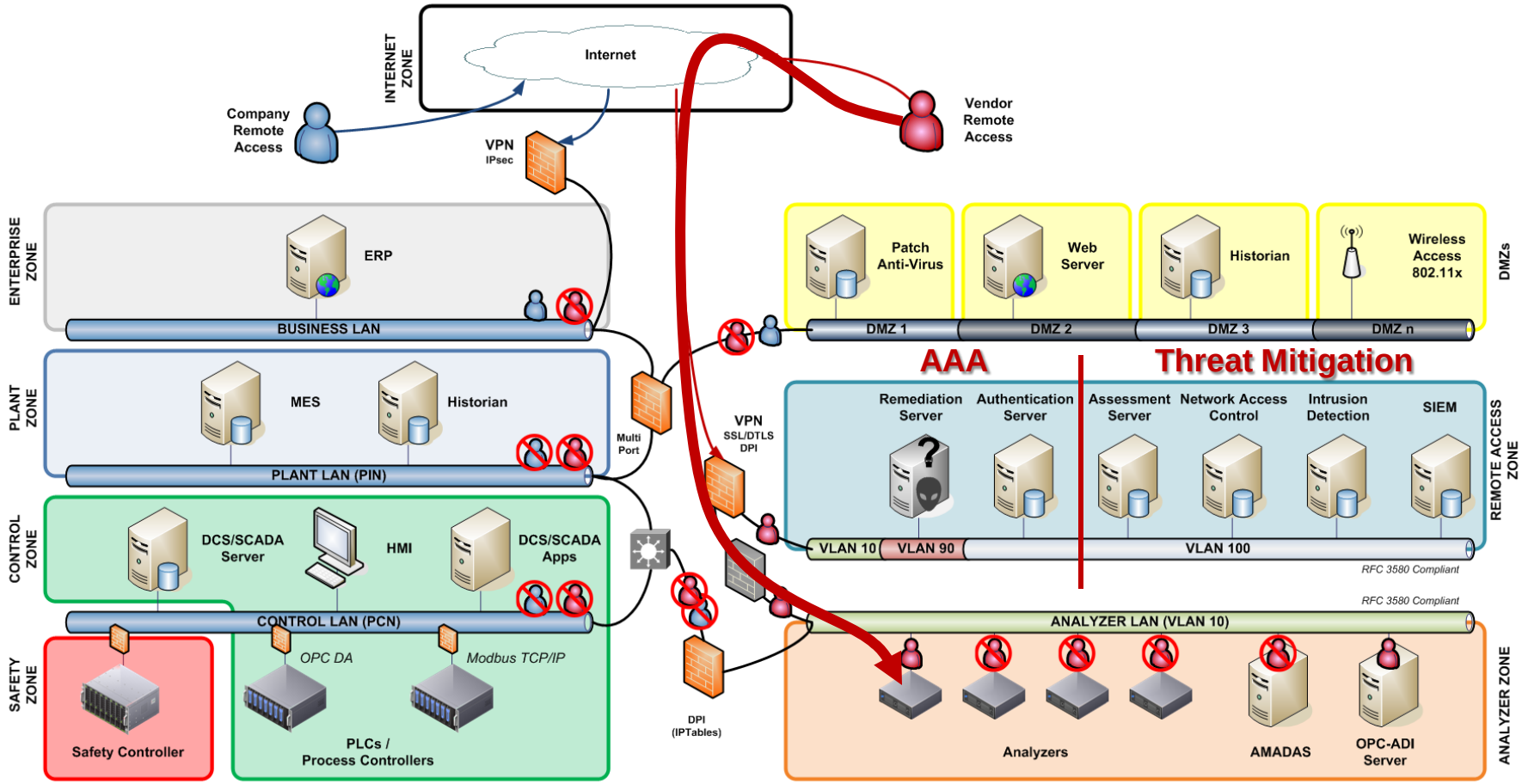
DiD Disclaimer

- The solution and architecture that follows is meant to be a representation of the functionality and components that comprise an overall DiD strategy
- The implementation specifics are heavily dependent on the actual vendors chosen
- Components described on the following pages are available from most of leading suppliers of hardware and software solutions

Remote Access Profiles (Internal vs. External)



Remote Access Profiles (Internal vs. External)



Review of Defense in Depth Strategies

• Security Risk Assessment & Quantification	Process
• Security Policy	People
• Network Segmentation (Zones & Conduits)	Process
• Demilitarized Zones	Process
• VPN with Encrypted Tunnel	Product
• Strong Two-Factor Authentication	Product
• Virtual LANs	Product
• Network Access Control for Role or Policy-based Access	Product
• Secondary Firewall from Different Vendor	Product
• Firewall to Control Systems Network	Product
• Security Information Event Management	Product
• Intrusion Detection	Product
• Equipment Selection & Procurement	Process
• Security Awareness & Training Program	People
• Incident Response & Forensics	Process
• Vulnerability Testing	Process

How much does this solution cost?

• Firewall with SSL/DTLS VPN Access	$1,500 - $5,000
• Firewall using Hardware/Software (Linux IPTables)	$1,000 - $1,000
• Authentication Server	$1,000 - $2,000
• Network Access Control	$0 - $25,000
• SIEM	$5,000 - $45,000
• Intrusion Detection	$1,100 - $10,000
• TOTAL	$9,600 - $88,000

Thank you for attending!

JOEL LANGILL
TÜV FSEng ID 1772-09, CEH, CPT, CCNA
Staff Engineering / Security Consultant

ENGlobal Automation
15534 West Hardy Road
Suite 100
Houston, TX 77060
http://www.englobal.com

(281) 726-9813
joel.langill@englobal.com

@jtlangill joel.langill

Global Thinking ... Global Solutions™