INDUSTRIAL DEFENDER®

Critical Infrastructure Protection Solutions

Karl Henderson
Senior Security Consultant

SANS SCADA Conference

September 2008

Company Background

- Industrial Defender is a Global Cyber Security company focused on Protecting Critical Control Systems that are vital to a Nation's Economy
  - Main Headquarter USA, Foxboro, MA
- 16-years of real-time process control/SCADA industry experience
- 4 years experience in Cyber Security specifically for Process Control Systems
- We understand what are the priorities and risks when securing Control Systems:
  - Business Systems: Confidentiality -> Integrity -> Availability (CIA)
  - Control Systems: Availability -> Integrity -> Confidentiality (AIC)
- The only company with complete "Risk Prevention Life-cycle" Solution:
  - Security Assessment -> Solution Design & Implementation -> Support & Life Cycle Maintenance
  - Industrial Defender Solution is DCS/SCADA supplier neutral

Trusted Partner in Critical Infrastructure Cyber Security

INDUSTRIAL DEFENDER - CYBER SECURITY PROTECTION

Risk Assessment

Professional Services

INDUSTRIAL DEFENDER® Consulting Services

- Regulatory Compliance Audits
- Network Architecture
- Security Assessments
- Penetration Testing
- Red Team Testing
- Disaster Recovery
- Cyber Forensics
- Security Training
- Application Engineering
- Custom Software Engineering

Risk Mitigation

Defense In-Depth Technology Suite

INDUSTRIAL DEFENDER® Technology Suite

- Industrial Defender SEM
- Industrial Defender Guard
- Industrial Defender NIDS
- Industrial Defender HIDS
- Industrial Defender EGP
- Industrial Defender RTAP

Risk Management

Co-Managed Security Services

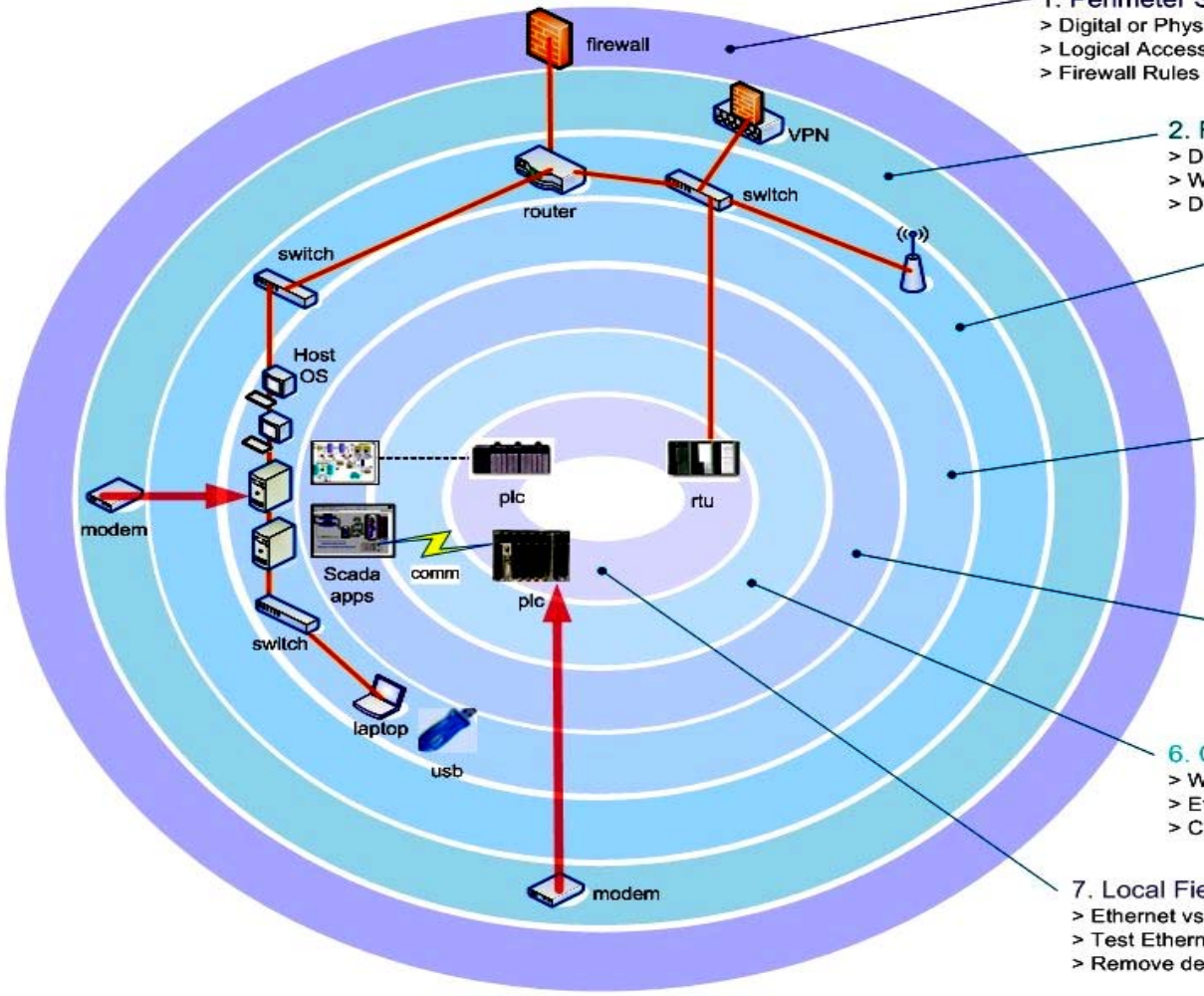
INDUSTRIAL DEFENDER® Co-Managed Security Services

- Security Monitoring
- Performance Monitoring
- Firewall Co-Management
- UTM Co-Management
- NIDS Management
- HIDS Management
- Security Device Deployments

Industrial Defender Security Consulting Approach

Defense-in-Depth Approach

> Building Security into each SCADA System Component



1. Perimeter Security

> Digital or Physically Isolated
> Logical Access Controls
> Firewall Rules (map out open ports)

2. Remote and 3rd Party Access

> Document all remote access points
> War-dial for modems
> Document VPN or other Remote Access

3. Network Architecture

> Discover all network devices & hosts
> Conduct Protocol / Traffic Analysis
> Conduct Wireless Audit
> Analyze switch/router configurations

4. Host OS & Removable Devices

> Check OS for vulnerabilities
> OS Patch Management
> Prevent USB or Removable Devices from use inside Control Room
> Restrict foreign laptops from connecting

5. SCADA Applications

> Monitor network for clear text transfer
> Ensure use of individual accounts
> Test for access to desktop

6. Communications to Field Devices

> Wired vs. Wireless Communications
> Ethernet vs. Serial Communications
> Capture Traffic on Ethernet connections

7. Local Field Controllers

> Ethernet vs. Serial connected devices
> Test Ethernet devices in lab for vulnerabilities
> Remove default vendor passwords

Trusted Partner in Critical Infrastructure Cyber Security

INDUSTRIAL DEFENDER - CYBER SECURITY PROTECTION

Risk Assessment

Professional Services

INDUSTRIAL DEFENDER® Consulting Services

- Regulatory Compliance Audits
- Network Architecture
- Security Assessments
- Penetration Testing
- Red Team Testing
- Disaster Recovery
- Cyber Forensics
- Security Training
- Application Engineering
- Custom Software Engineering

Risk Mitigation

Defense In-Depth Technology Suite

INDUSTRIAL DEFENDER® Technology Suite

- Industrial Defender SEM
- Industrial Defender Guard
- Industrial Defender NIDS
- Industrial Defender HIDS
- Industrial Defender EGP
- Industrial Defender RTAP

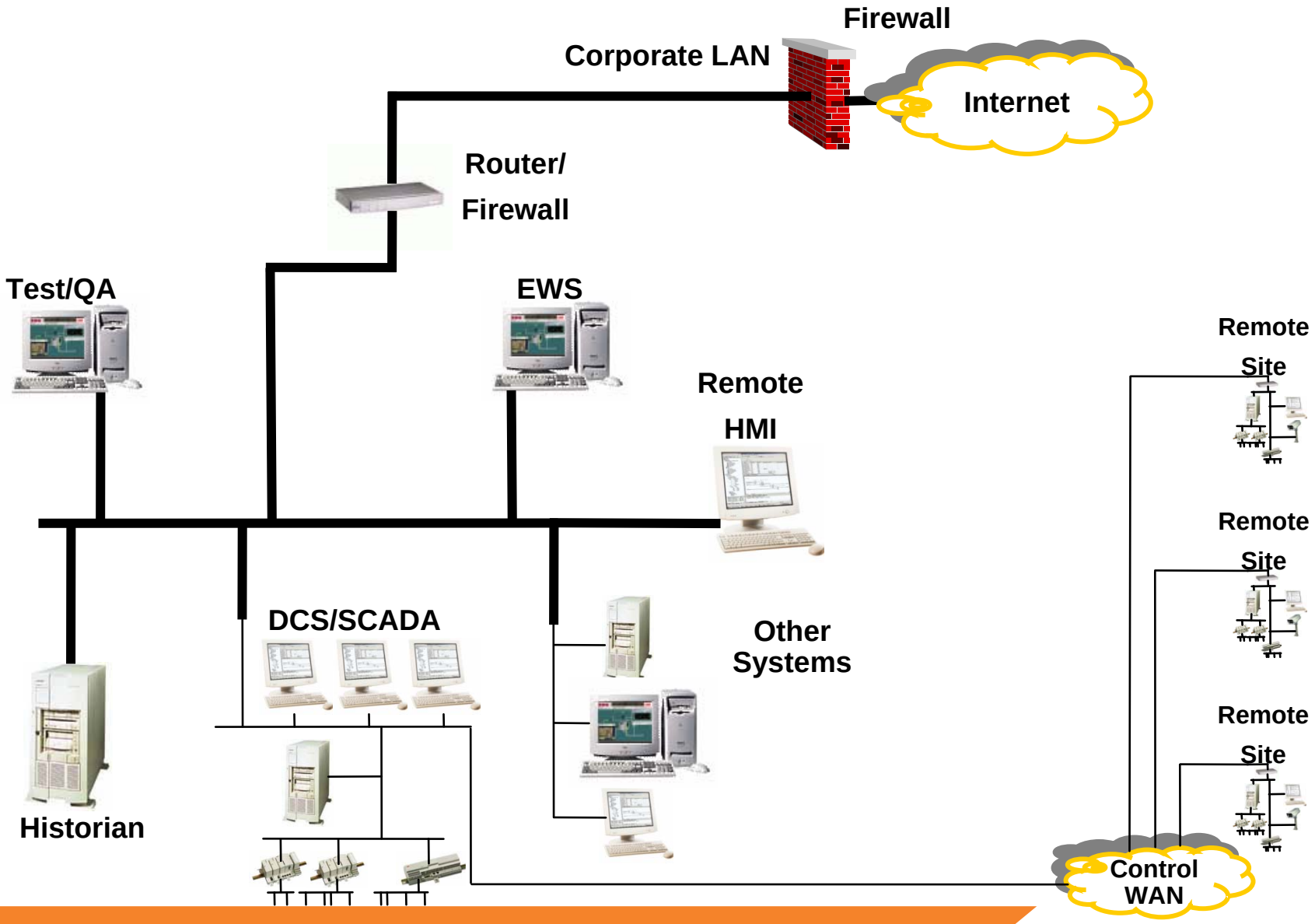
Risk Management

Co-Managed Security Services

INDUSTRIAL DEFENDER® Co-Managed Security Services

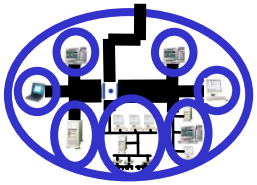
- Security Monitoring
- Performance Monitoring
- Firewall Co-Management
- UTM Co-Management
- NIDS Management
- HIDS Management
- Security Device Deployments

Typical Control System

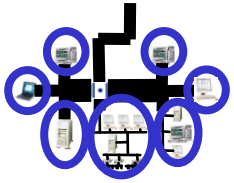


Multiple Security Layers

Perimeter Protection



Subsystem Protection

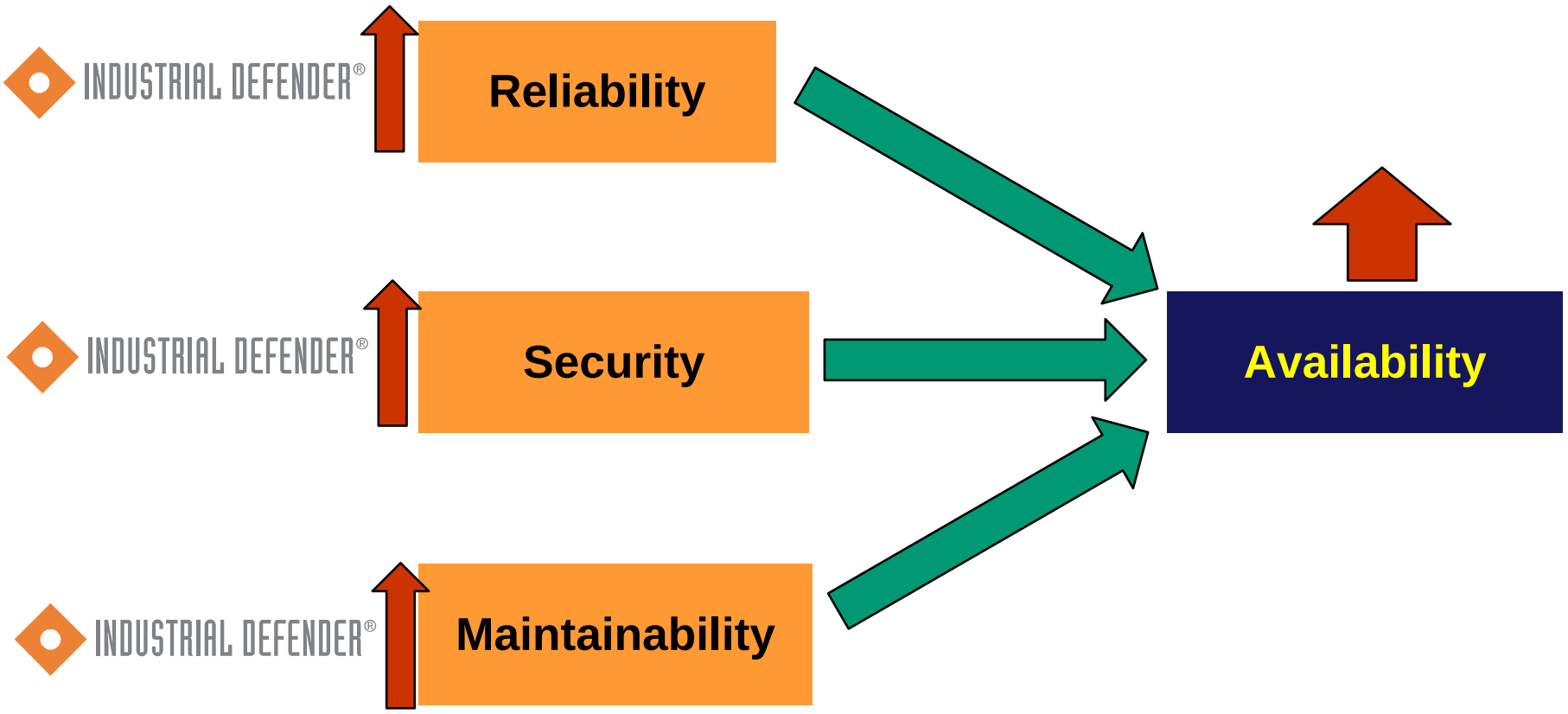


Control Network Monitoring

Host Monitoring

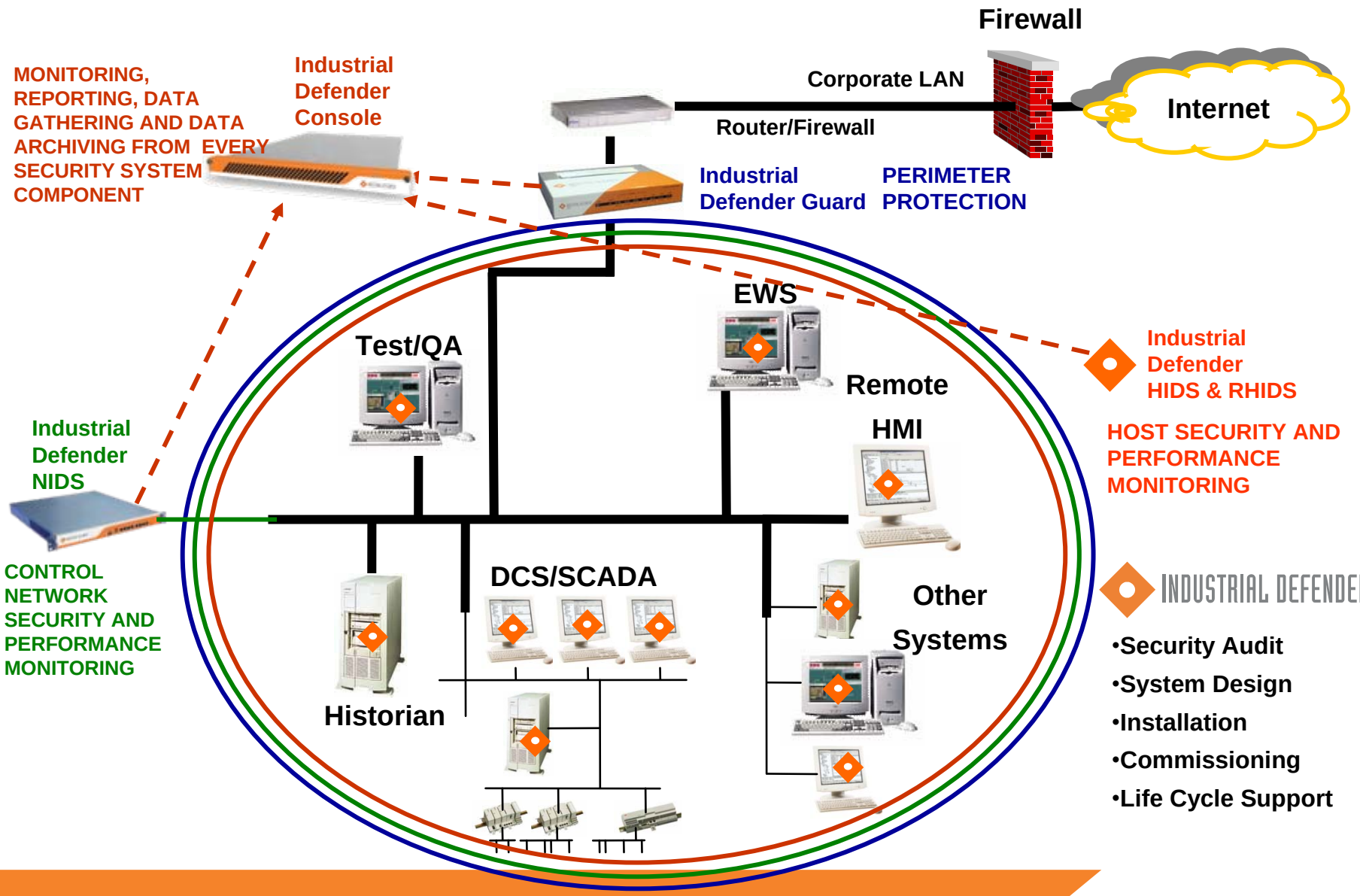
Control Application Monitoring

Control System Availability



Source: ANSI/ISA–99.00.01–2007

Industrial Defender Complete Solution



INDUSTRIAL DEFENDER®

- Security Audit
- System Design
- Installation
- Commissioning
- Life Cycle Support

INDUSTRIAL DEFENDER®