



Process Control Security The bp experience

Process Control Systems Forum Spring meeting
Dallas 17th & 18th May 2005



*Ian
Henderson*



Introduction

- The bp journey to improve the security state of process control systems.
 - How we organised ourselves
 - What we did
 - What we will continue to do
 - Process control security isn't a diet, it's a change of lifestyle.
- Security Compliance testing
 - What do we do with the results?



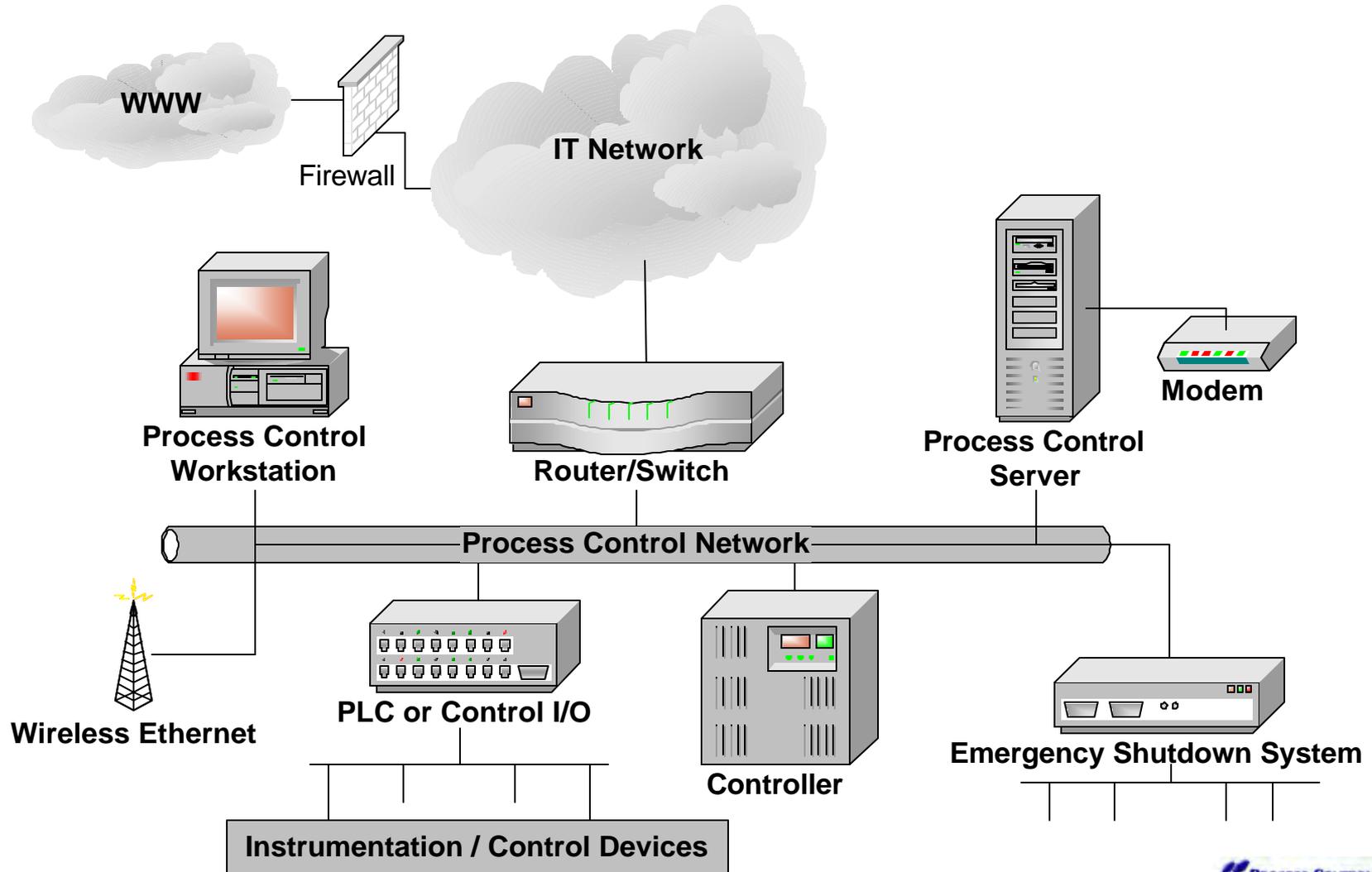
The good old days?

- Remember when control systems looked like this?
- No need to worry about internet worms here!



Today's control systems

- IP connected open systems

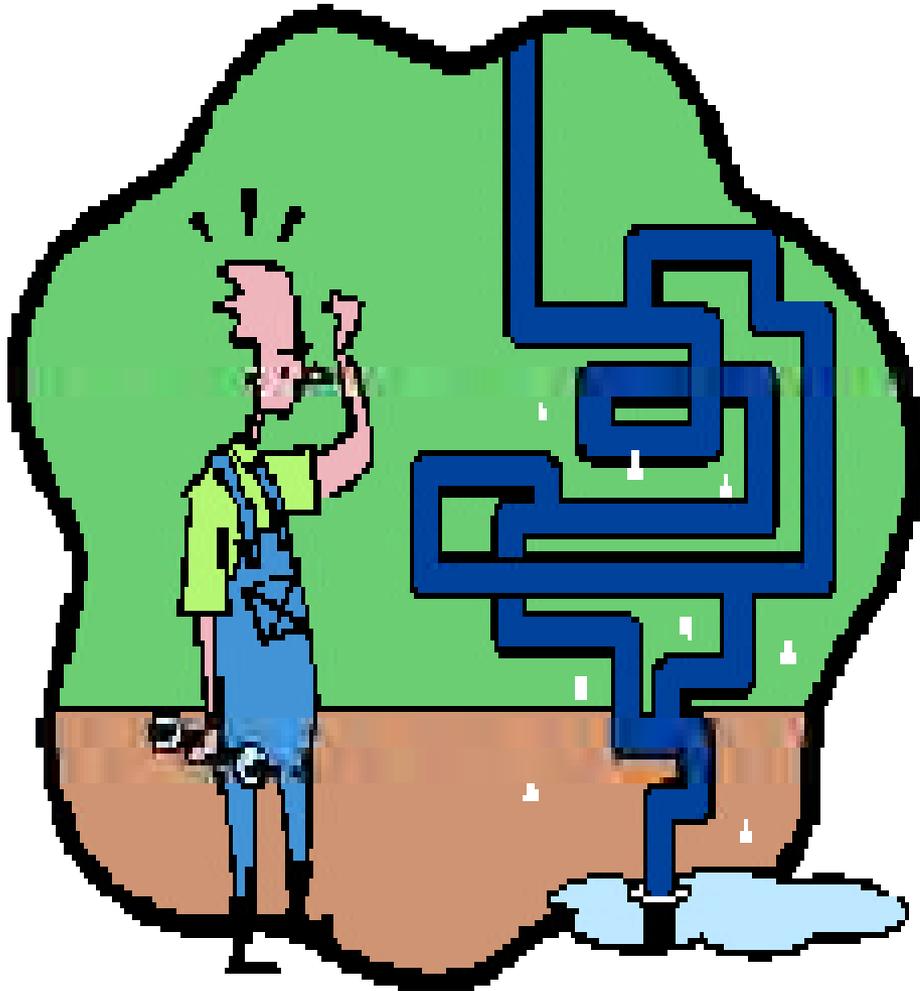


Organisation

- Typically:
 - IT organisation V's Control engineering
 - Mistrust, suspicion, outright hostility?
- In BP, the CISO is responsible for digital security of the whole organisation including process control systems
 - IT security organisation works with control engineers
 - Recognition that process control systems are “different” from IT systems
 - Also recognition that today's systems are very similar
 - Working together we're stronger!



The Problem...



- 400+ sites spread across the globe
- Enormous variation in systems (vendors, vintage, size)
- Systems managed by process control personnel with variable security expertise at sites
- Corporate Travel ban
- No standards to apply
- Resistance to IT “interference in control systems”
- This problem is too large
- Sound familiar?



A Solution?

- Hire a team of security consultants to visit each site and “do security” to local site?
- No, why not?
 - Travel ban
 - Cost
 - Timescales
 - Shortage of Industrial Security Experts

Q. Where will we be in 2 years time

A. Back where we started



Control teams at site need to own security, its part of the day job!



Our Solution

- Create a small dedicated team of digital security experts and control engineers to provide a Group centre of excellence (CE)
- The CE developed a process and tools for the sites to use
 - Risk Assessment tool
 - Remediation cookbook
- CE trialled tools at a representative sample of sites
- The CE developed remote learning tools to train sites in using the tools
 - On-line training packs
 - Audio-conference training sessions (2 – 3 hours duration)
- Training and tools rolled-out via business streams



Risk Assessment and Reduction Framework



Step 1

Complete the Risk Assessment

- Attend virtual training
- Define high level scope and agree on team and work plan
- Brief site management

Step 2

Conduct a Risk Reduction Workshop

- Prepare for the Risk Assessment
- Agree on detailed scope and focus
- Complete the Impact Assessment
- Complete the Current State Assessment

Step 3

Develop a Risk Reduction Plan

- Complete, circulate and finalise the plan
- Communicate the plan at the site and to the Stream programme

Step 4

Implement the plan

- Implement the plan in three phases

- Recognised that only site personnel have the knowledge to assess the risks to their plant and their systems
- Each site uses risk assessment tool to develop risk profile for their site

- Risk reduction plans use cookbook approach to reduce risk to level acceptable to site
- Outcome will depend on sites appetite for risk BUT need overview of corporate risk.



Measuring Impact



Summary Impact Assessment Table

Impact	Time period						
	≤ 15 mins	≤ 30 mins	≤ 1 hour	≤ ½ day	≤ 1 day	≤ 1 week	≤ 1 month
HSE event/ Damage to plant							
Non compliance with regulatory requirements / minor HSE event				3	3	3	3
Forced controlled shutdown of operations							
Elected controlled shutdown of operations	1	1	1	1	1	1	1
Reduction in operating efficiency		2	2	2	2	2	2
No impact	9	7	7	4	4	4	4

Measured impact of 10 generic scenarios

- simultaneous loss of all Microsoft-based systems
- simultaneous loss of all Unix systems
- loss of Ethernet network infrastructure



Measuring Security Posture



- Developed a single scale to measure level of current protection, and the strength of the various options given in the cookbook.
 - 🔒 Weakest of measures. Provides some protection, but leaves significant exposures
 - 🔒 🔒 Measures are effective for some threat scenarios, but do not offer full coverage of all known threats
 - 🔒 🔒 🔒 Measures are effective for most threat scenarios, but do not offer full coverage of all known threats
 - 🔒 🔒 🔒 🔒 Measures are effective for known threats
 - 🔒 🔒 🔒 🔒 🔒 Measures are effective for both known and as yet unknown future threats
- Allowed security posture to be articulated effectively to both engineers and site leadership (who funded remediation).

Summary & Learnings



- Approach worked well
 - **No world tour**
 - parallel timelines, hence earlier completion.
 - Observed travel ban.
 - **Kept things simple**. Many of the actual issues are about basics. You don't need to blind people science.
 - **Explained the issues**
 - The threats
 - The available security technologies
 - The need for robust security management practices
 - **Provided tools**
 - **Allowed sites choice**. With so many different systems in the field, no one solution fitted all.
 - **Engineers were engaged** they were doing security, not having it done to them
- Side benefits
 - **Excellent awareness tool**. Combination of the training and tools proved to be highly effective in raising engineer's awareness of digital security
 - **Process control engineers now talk with IT** , particularly when Internet worms are around.



The Future

- Having run a remediation programme, what next?
 - Digital Security Alert centre
 - Work with vendors
 - Work with external agencies, governments





- Internal bp team
 - Monitor external and internal networks
 - Close ties to MS
 - Advises on threats to IT systems AND process control environment

Alerting process

- E-mail notification of threat



ALERT
Process Control Digital Security

This alert contains information about a digital security threat that may require action at your site

The banner features a red background with the word 'ALERT' in large white letters. Below it, 'Process Control Digital Security' is written in a smaller white font. On the right side, there is a yellow circular icon with a black biohazard symbol. A thin white border surrounds the text area.

- E-mail & telephone autodialer notification of incident



INCIDENT
Process Control Digital Security

A Digital Security Incident has been declared, which will require action at your site

The banner features a red background with the word 'INCIDENT' in large white letters. Below it, 'Process Control Digital Security' is written in a smaller white font. On the right side, there is a yellow circular icon with a black biohazard symbol. The left and right sides of the banner are decorated with a yellow and red checkerboard pattern. A thin white border surrounds the text area.

Vendor Engagement 2004

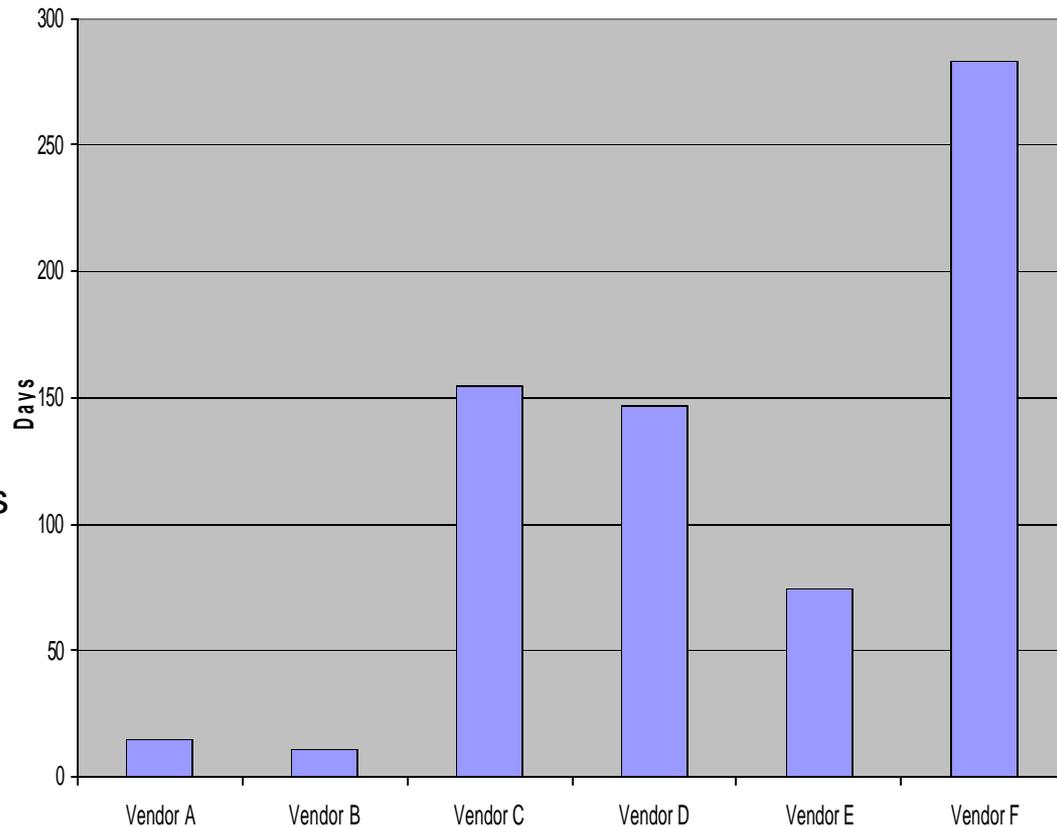


The objective:

Improve security of new products

Improve operational security of existing systems

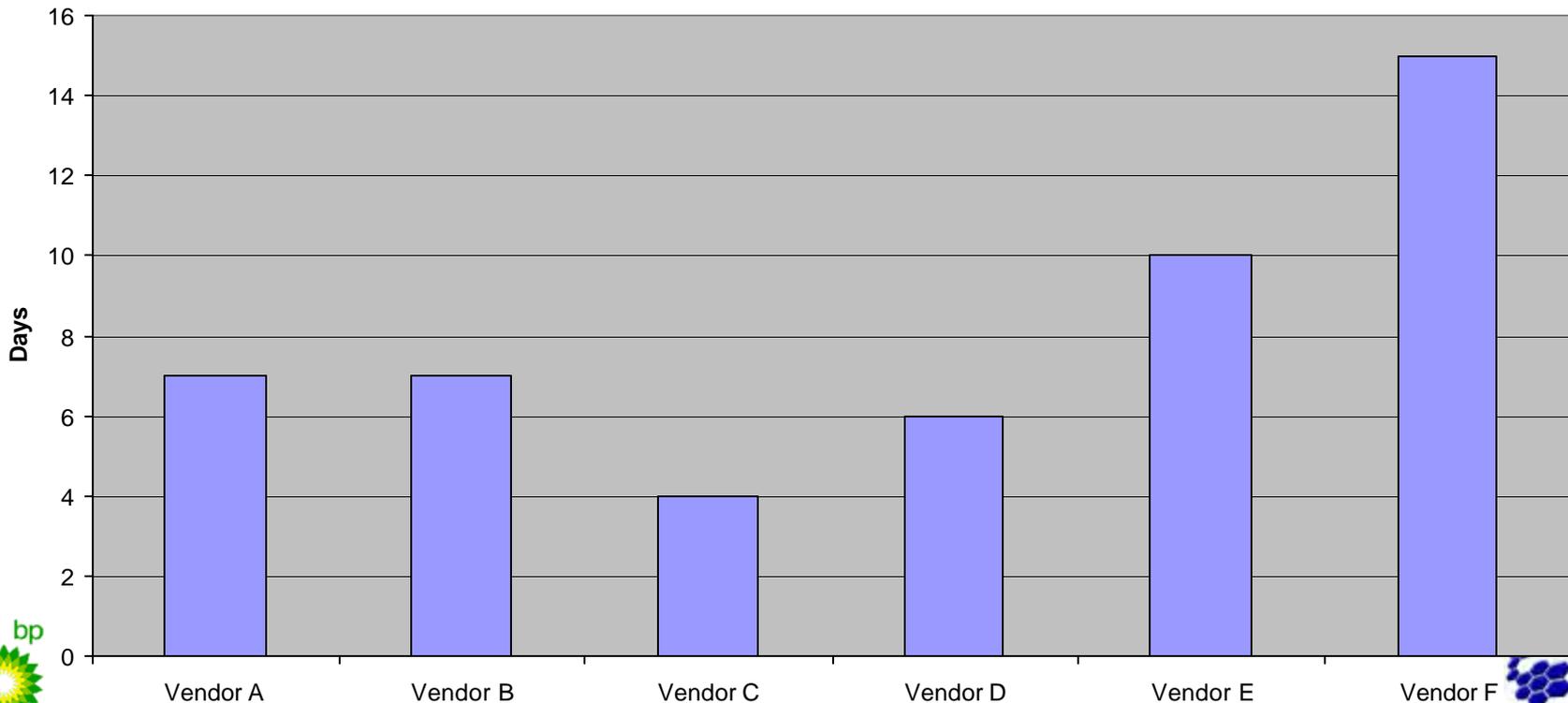
- Anti Virus accreditation
- Security patch accreditation
- Remote access methodologies



Vendor Engagement 2005



- Massive improvement:
- Anti Virus widely accredited and now comes as standard on some vendors systems
- Security patch accreditation times improved dramatically now days instead of weeks!



External Agencies

- BP contribute to standards bodies
 - ISA SP 99
 - API
- BP engaged with governmental groups
 - UK NISCC
 - European Commission
 - US DHS



Security Testing

- So we test a PLC and find its vulnerable, what do we do?
 - Traditional IT responsible disclosure
 - Contact vendor
 - Allow vendor time to produce a fix
 - Vendor publicises fix to user community & may credit the tester for finding the vulnerability and disclosing in a responsible manner.



Security testing

- PLC needs to have firmware upgrade to resolve problem
- Firmware upgrade may need EPROM change out
- May require system outage, difficult to schedule
- Once public, need to patch ASAP



Penetration Testing



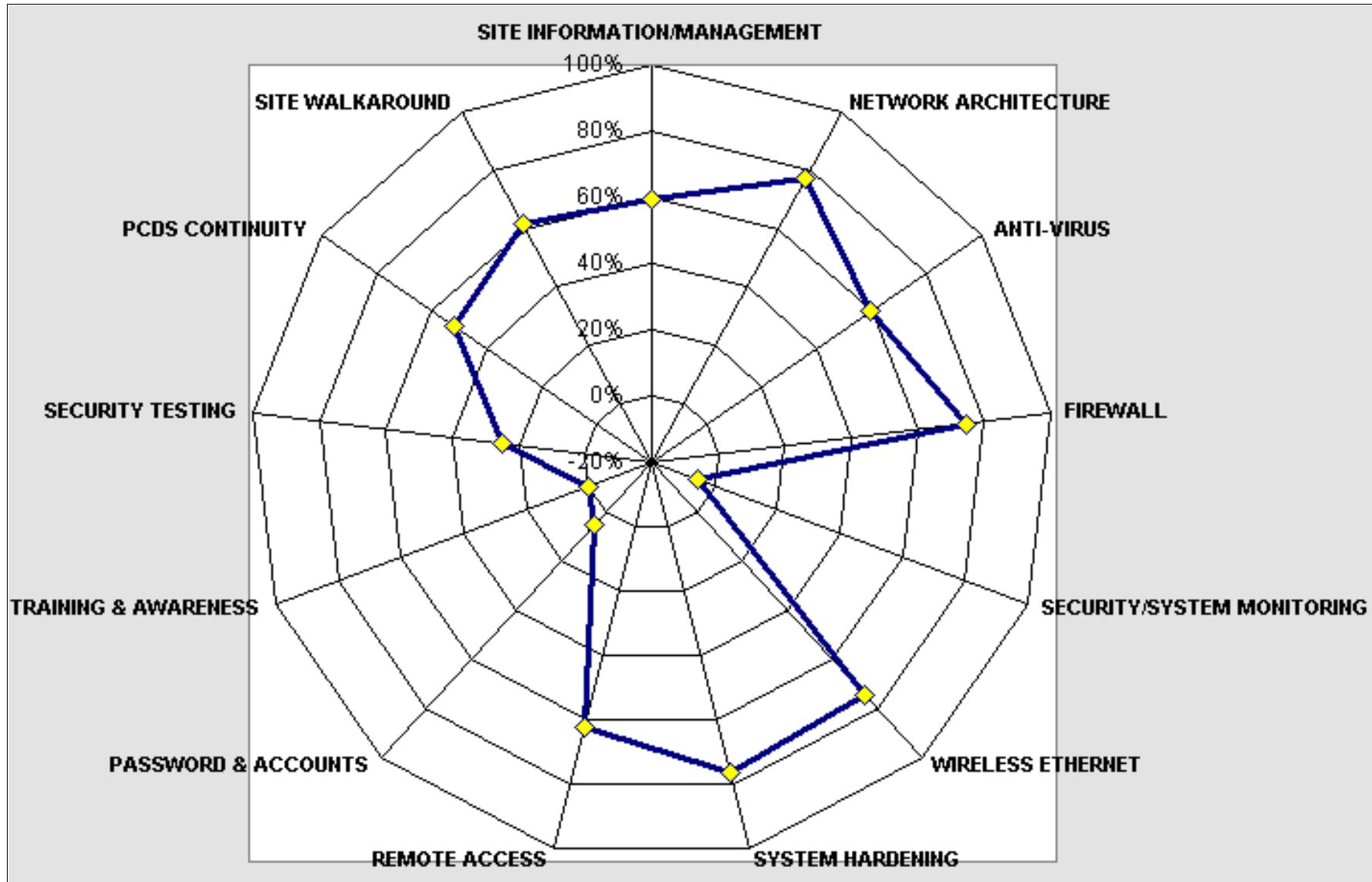
- Is this possible on a live system
 - OIM needs guarantee that nothing will fail as a result of the test
 - Can you give this guarantee?
- Are Red teams really a good idea on a production facility?
 - We're not talking about e-mail outages or server downtime
 - This is about systems that run plant

BP approach

- Testing of control systems in vendor facilities to benchmark security
- Testing at the end of FAT before system is shipped to site
- Work with vendors and academia (BCIT) to develop security test harness
- Internal security “Health check”



Health check



Questions



Ian Henderson
henderi1@bp.com

