Shell Global Solutions

An end-user perspective on implementing process control security services

Presented in Amsterdam

2008 European Community SCADA & Process Control Security Summit

By Frans Martens

Presenter info

- Frans Martens

  Principal Control & Automation Engineer
  Shell Global Solutions International B.V.

Bio: 26 Years of experience in both the upstream as wel as downstream parts of Shell. Covering field devices, telemetry and process control systems. Over the past four years involved in the development and implementation of a secure architecture for process control systems, including the security services to sustain them.

Member of WIB Working Group on Plant Security

Introduction

- This presentation is not about process control security standards, it's about how system vendors and end-users interface on security aspects
- Some of the security services are described
- What goes well, what goes bad ?
- What is Shell's ambition in this area ?
- How can we improve, to our mutual benefit ?

You are welcome to ask questions during the presentation or at the end.

Information security services

What exactly do we mean ?

- Patching (flaw remediation)
- Antivirus (malicious code protection)
- Backup and Restore
- Remote User Access
- PCD Assist Desk (internal)
  - DMZ services

Aspects considered:

- Technical
- Procedural / contractual
- Organisational

Outside of the scope of this presentation but also relevant:

- Staff Awareness
- Training
- FAT / SAT procedures

Start with: System Hardening

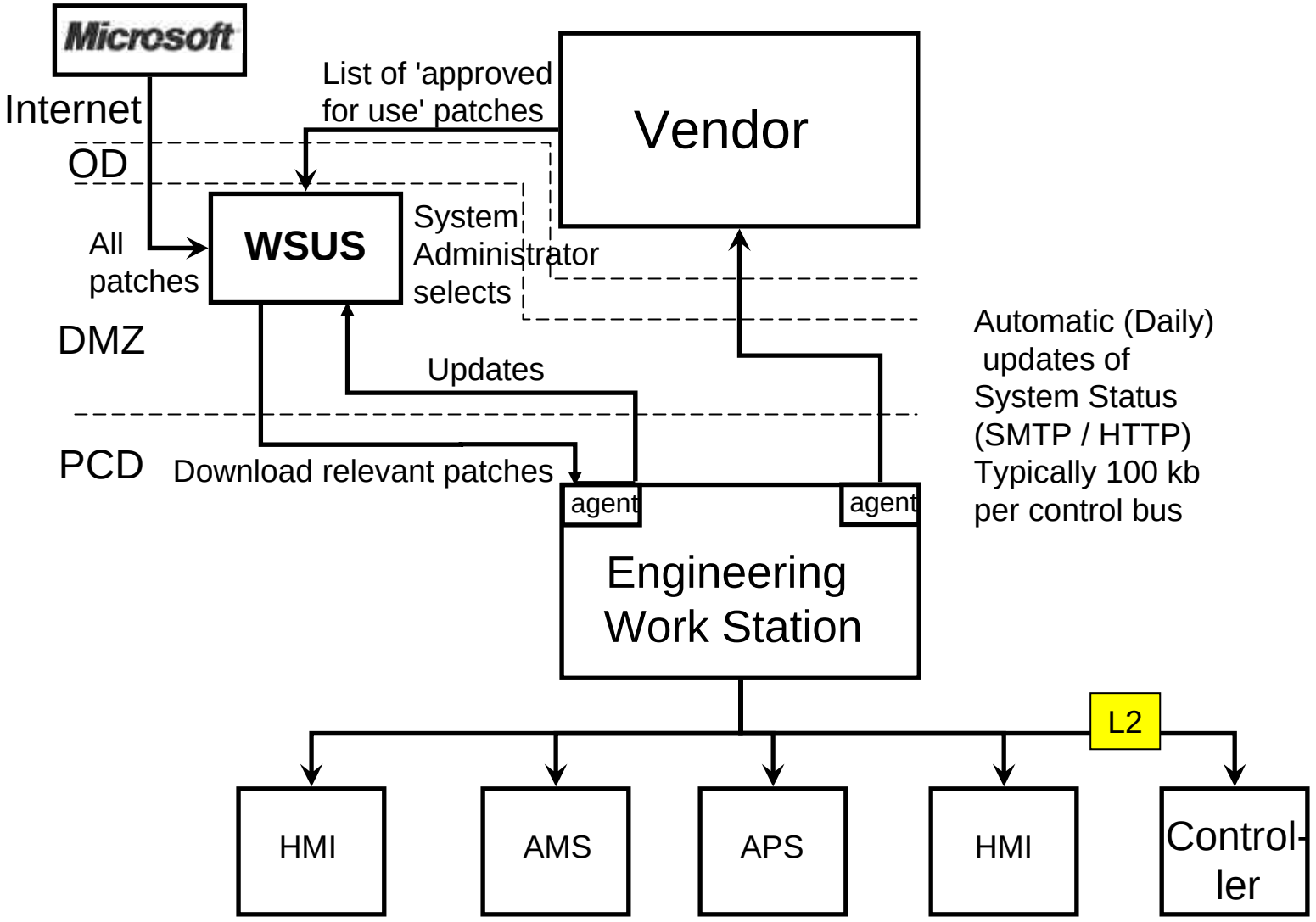
- Hardening is a basic requirement for succesfull patching
- Hardening, what do you mean with that ? A different understanding…
- MBSA, a simple tool to indicate vulnerabilities as a result of poor hardening
- Balance the business value of additional functionality and the incremental risk, potentially caused by that application

	By Vendor	By End-User
Logical	Minimal hardware and software functionality, apply patching, disable ports and drives, apply ACL and password rules, use split file systems, (single sign-on)	Through the location of the system in the architecture, segmentation of networks, firewalls, apply patching, additional functionality (eg OPC, SMTP etc), procedural coverage
Physical	Through the mechanisms provided on the system, locks, physical (USB/Ethernet) port protection	Through the choice of the location for the device, buildings, rooms, cabinets, key management, checks on state of third party laptops, KVM, separation between system and HMI

Patching (Flaw Remediation)

- Patching effort is significantly reduced when hardening is done properly
- Microsoft WSUS is the industry standard to evaluate the patching completeness of Microsoft systems
- Re-distribution of patches should be avoided
- So-called redundant systems are not really redundant, makes patching difficult, e.g. a single OPC server
- Patching of systems is a new subject and needs lots of attention (soft-skills)
- Often, system reboots are required

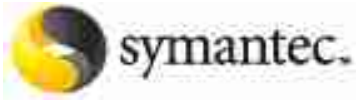
Structure (Shell's ambition)



Anti-Virus (Malicious Code Protection)

- Symantec and McAffee accepted as AV vendors by most PCD vendors
- Software agents are required on individual systems
- AV management console on a network level
- Often, AV definition files have to be distributed using portable media since architecture is not suitable to distribute from Level 3
- Often, a restart is required to upgrade the AV-agent

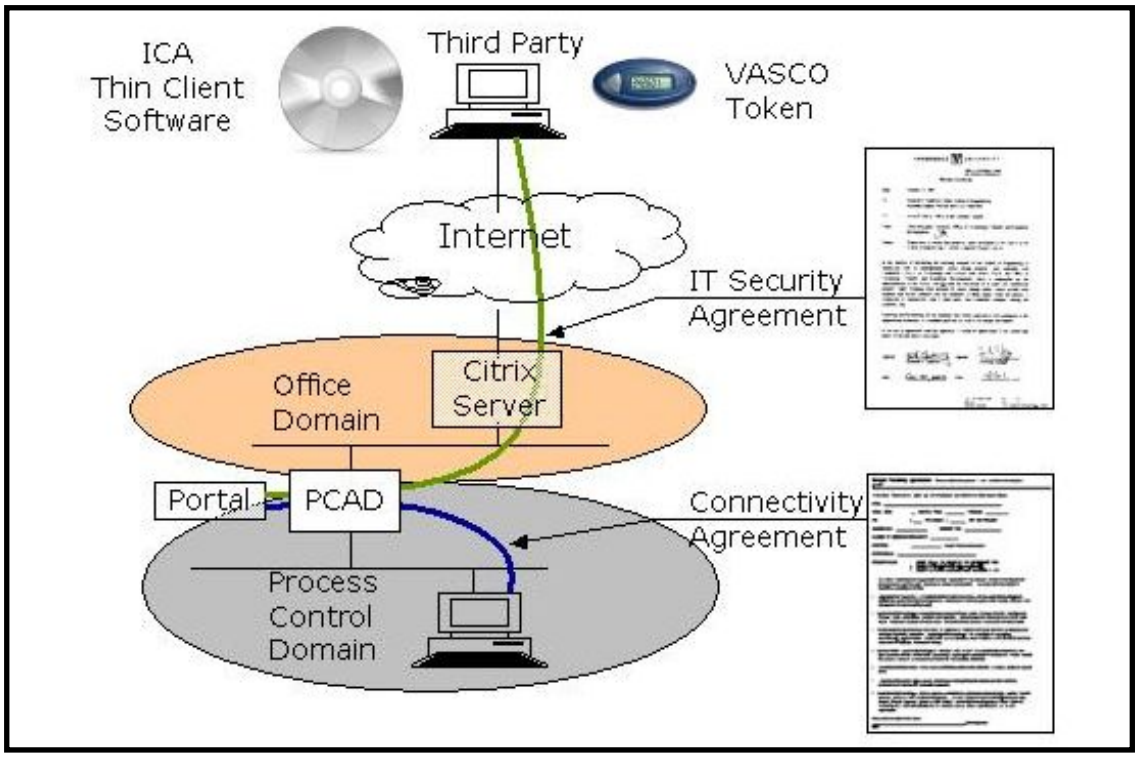
Backup and Restore

- The traditional method for restoring systems (CD-ROMs) is not adequate anymore
- There is no 100 % guarantee that the restored system is identical to the way it was before
- Backups can often only be made when system is off-line
- A traditional restore typically takes 12 hours and requires highly skilled staff
- 

Backup Exec solves all these issues

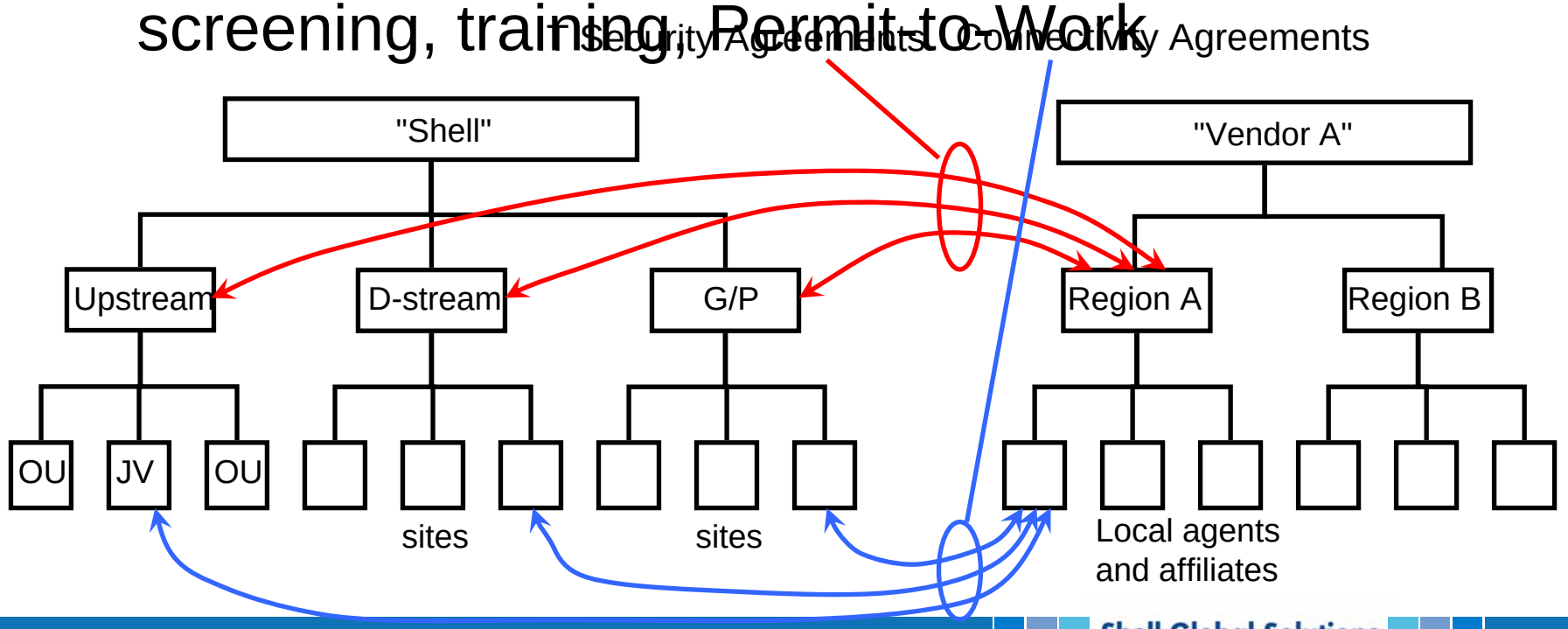
Remote User Access

- Mainly for remote system maintenance and engineering by vendors from their offices
- Driven by cost and HSSE (avoiding travelling to remote sites)
- Selection of appropriate thin client
- The technical infrastructure provides a good solution, but…

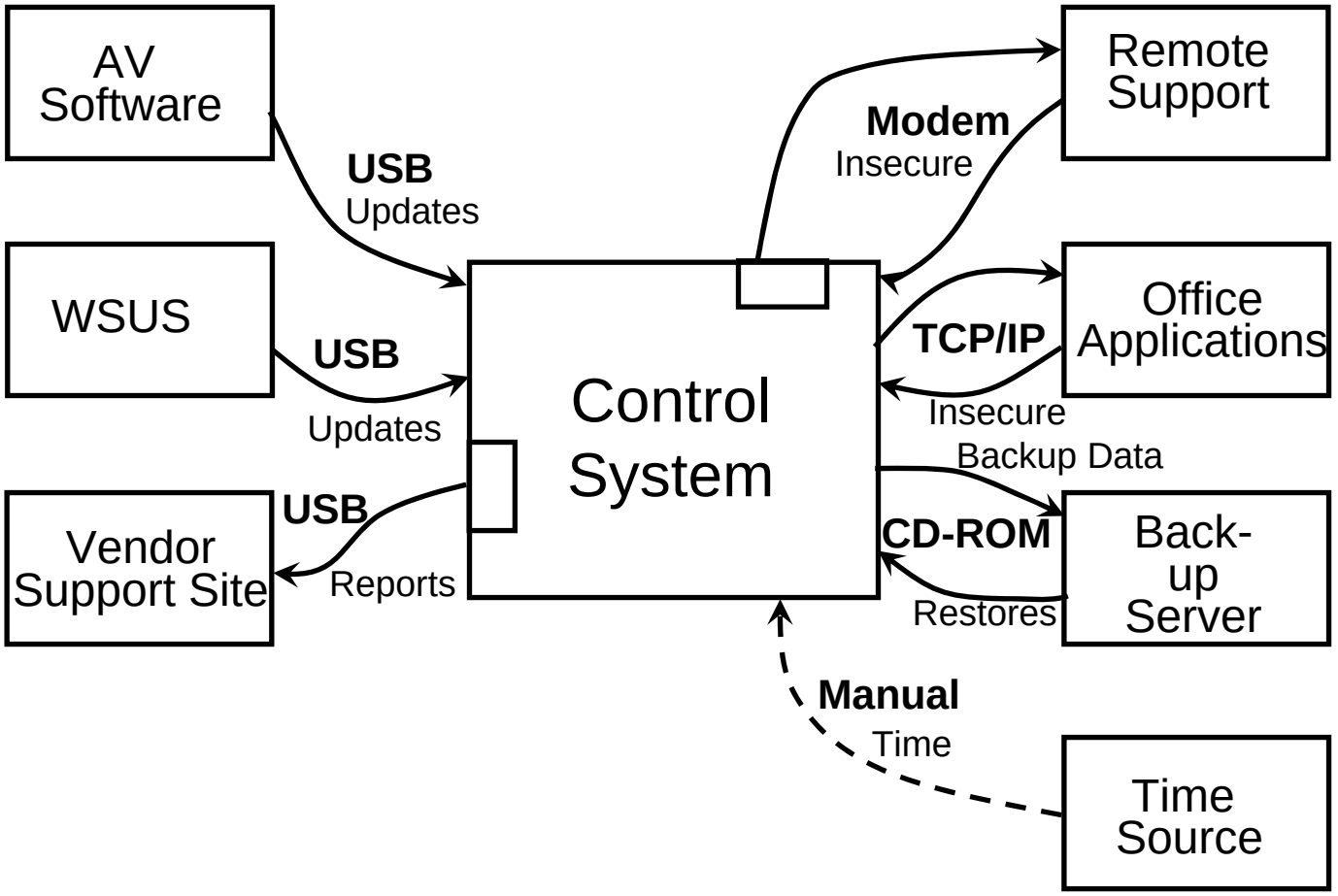


IT Security Agreement

- How to organise this ?
  - Global, regional, local
  - Legal and contractual implications are difficult to handle
- Third Party personnel, security agreement, screening, training, Permit-to-Work

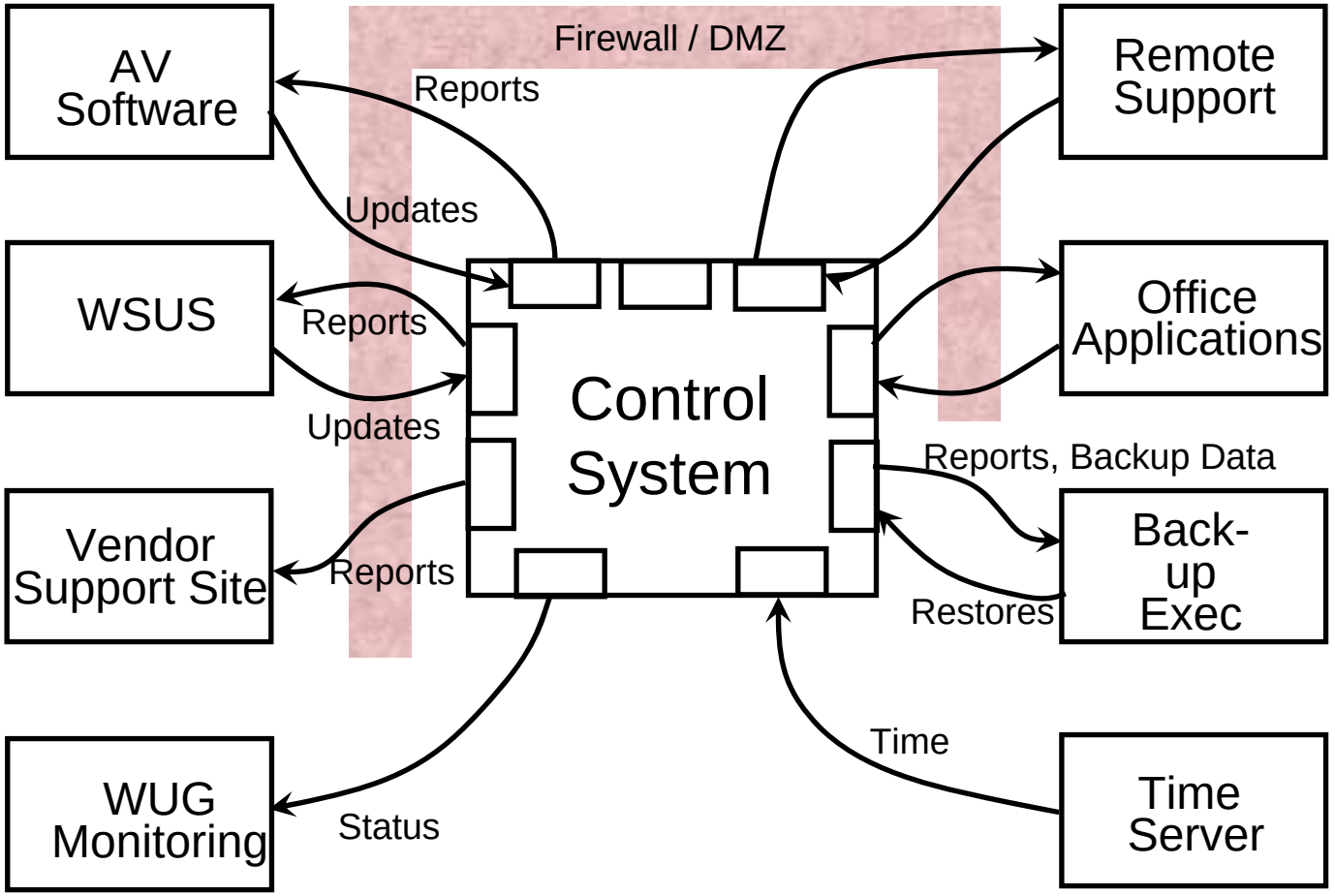


Overview of interfaces (Past)



*Requires agents or changes to registry settings

Overview of interfaces (Future)

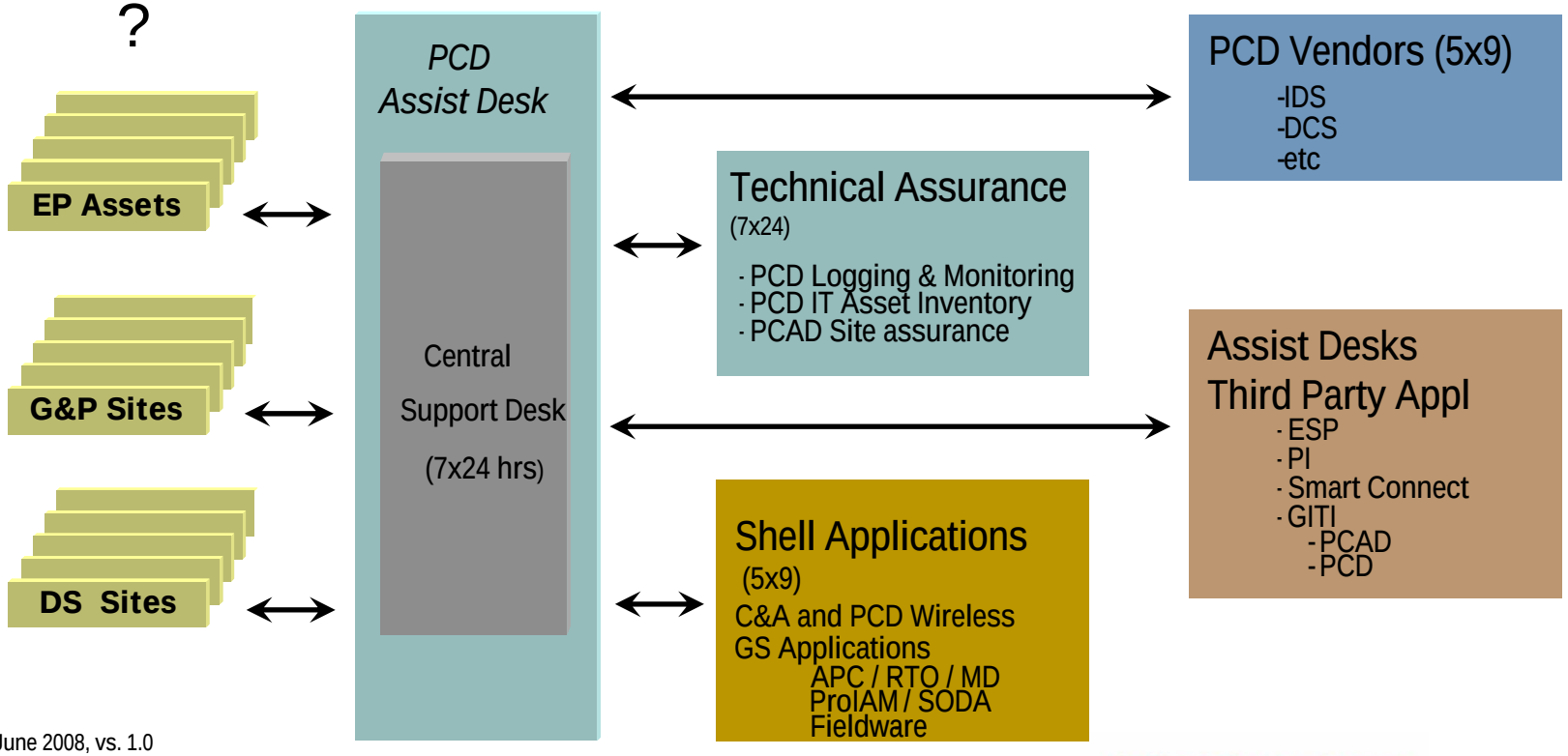


Compliance / requirements

- Shell working on document 'Minimum DACA Requirements for PCD Vendor'
- Not a standard but a compliance document
- WIB initiative, end-users converging towards international standards and legislation
- Which international standards ISO, ISA, etc…
- Shell involvement in EuroSCSIE to influence the legislative environment regarding information security in the PCD

Shell's Global Support Model

- The PCD Assist Desk
  - What is covered, what is not
- Expansion of the service in the future
  - How should the contacts with the vendors be handled ?



Conclusion

- Interfaces for security services are slowly maturing
  - Structure for AV and Patching automation
  - Standardised software agents
- Mutual understanding between end-user and vendor growing
- Strong need for harmonisation in a multi-vendor environment
- Additional Capex spend on security efforts will reduce system lifecycle cost

Summary

- The subject of security services is slowly getting the attention it requires
- This will impact on Capex but will enable Opex savings and increase system availability, integrity and confidentiality
- Any feedback, questions ?

- Thank you for your attention