

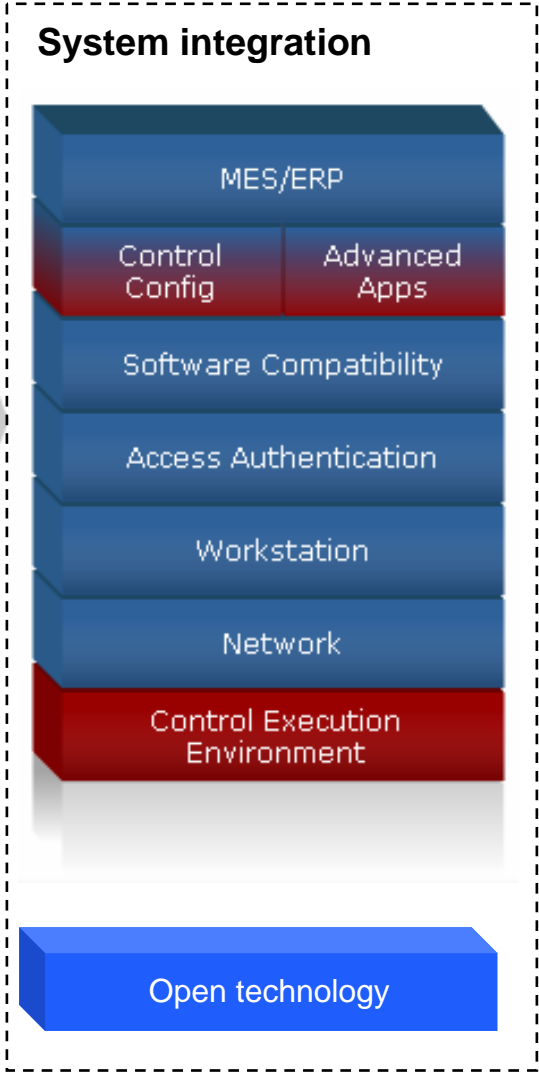
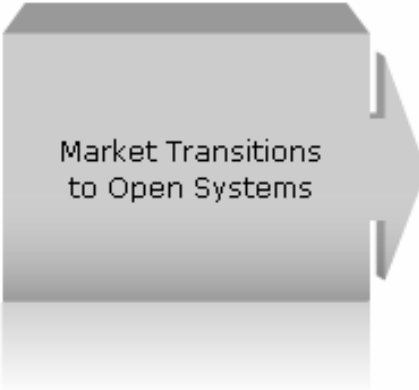
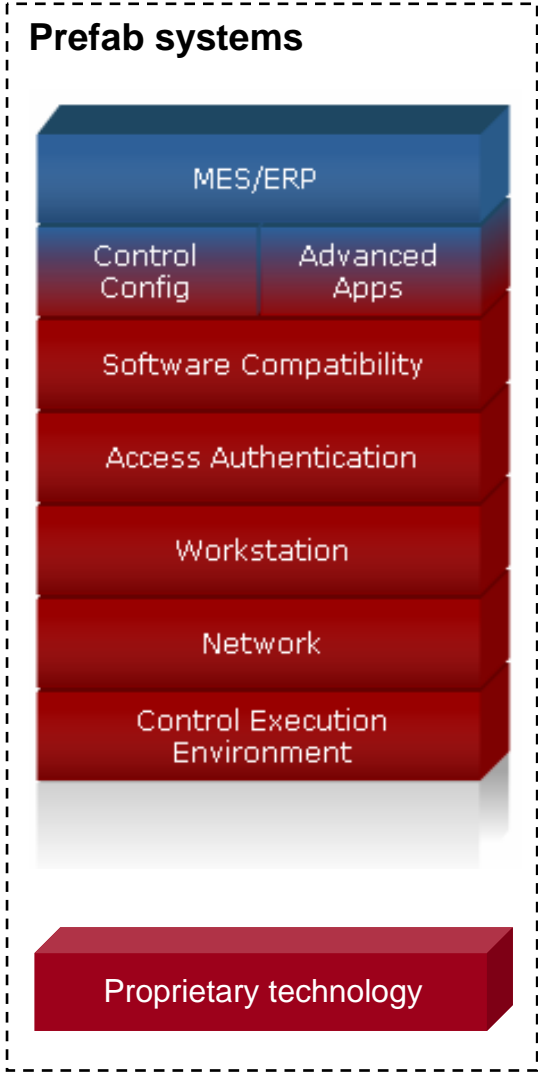


# The vendor security challenge

SANS - SCADA Vendors Security Leadership Panel

**Honeywell**

# The security challenge



## Four areas we focused on:

- **Architecture**
- **Products**
- **Services**
- **People**

- **Adopted the ISA SP 99 security model**
  - Layered zones / conduits model
  - Defense in depth
  - Single point of access
  - Control firewall, MODBUS TCP firewall
- **Use common security model for all applications**
  - Experion PKS R400, OpenBMA, PHD will have common role based security model
- **Integrated industrial security**
  - Instant location systems
  - Video
  - Access control

- **Reduced number of network ports used**
  - Firewall “friendly” applications
- **Security certification of products**
  - I.e. C300 controller has Mu Security Industrial Control (MUSIC) certification
- **Validate security patches of open platform with Honeywell products**
  - Validate Microsoft patches within 7 days (actual performance for Experion PKS was an average of 3 days over 2007)
- **Validate compatibility with key security controls such as virus protection software, data recovery software**
  - McAfee, Symantec (Norton)

- **Developed a new portfolio of Open Systems Services with security as a central focus**
  - Security assessments (Identify vulnerabilities, advise best practices)
  - Security incident handling (Response on i.e. malware infections)
  - Patch management (Maintain appropriate patch level)
  - Virus protection management
  - Secure remote connectivity
  - Perimeter management
- **Security focus over the full life cycle of the systems**
  - Build system, maintain system, remove system (components)

- **Established new Open Systems Services teams**
  - **Focus on certification**
    - ◆ Security - CISSP, CISM, GCIH, GCEH
  - **Engineers with a mix of business IT and process IT skills**
  - **System integration skills**
- **Introduced ISMS for project and service teams**
  - **Improve security awareness**
  - **Common security policies**
  - **Deliver and maintain secure systems**

**Security is a continuous process with no end  
for architecture, products, services, people  
so for vendors.**