Using a Fully Open Infrastructure for a DCS: Dream Come True or Nightmare?

William R. Hodson, P.E.
Honeywell Process Solutions

ISA Expo 2004 Conference, Houston, TX
Using a Fully Open Infrastructure for a DCS: Dream Come True or Nightmare?

- Background
- Performance
- Testing for Performance, Capacity, & Topology
- Interoperation
- Security
- Robustness
Using a Fully Open Infrastructure for a DCS: Dream Come True or Nightmare?

- Background
- Performance
- Testing for Performance, Capacity, & Topology
- Interoperation
- Security
- Robustness
Background

The search for true Openness!
Background

In the beginning…

Control Highways by Process Control Companies

- Value in distribution of control
- Communication needs:
  - Fast
  - Extremely Reliable
  - Secure
  - Environmentally Hardened
  - Specialized Services (Control connections, Alarms, Downloading, Display Update Services, Parameter Change Services, Trends, History, etc.)
Background

Nothing Available ➔ Make Your Own (Proprietary)!

- IEEE 802.4 Token Passing Highway
- PROWAY (ISA SP72)
- Manufacturing Automation Protocol (MAP)
- TCP/IP, IEEE 802.3/Ethernet
- IEC ISA SP50 Fieldbus IEC61158
Background (Cont’d)

- **Ethernet-Based Protocols**
  - MODBUS/TCP
  - Ethernet IP
    - ControlNet
    - DeviceNet
  - FF HSE
  - PROFINET
  - Make-Your-Own…
Using a Fully Open Infrastructure for a DCS: Dream Come True or Nightmare?

- Background
- Performance
- Testing for Performance, Capacity, & Topology
- Interoperation
- Security
- Robustness
Performance of Open Protocols

- Not designed for large system requirements
- K.I.S.S. (e.g., one-at-a-time pub by devices)
- Communications Overhead
- Smart devices encourage more measurements
- Large point counts
- More application consumption
  - Asset Management
  - Optimization
  - Reports
  - Scheduling, etc.
Performance of DCS Protocols

- Advanced process point collection systems
- Data-Managing “interface” devices vs. “Linking devices”.
  - Interfacing networks of different magnitudes of speed.
  - Servicing large numbers of network nodes.
  - Maintains database of data relationships.
    - Vendor-description-information base.
    - Utilizes most efficient messaging services for the need.
    - Cached for performance.
    - Age and reference managed cache scheme.
    - Control connection priorities.
    - Gather-scatter techniques
    - Robustness guaranteed.
- Performance Optimization does **not** show on a network diagram.
Using a Fully Open Infrastructure for a DCS: Dream Come True or Nightmare?

- Background
- Performance
- Testing for Performance, Capacity, & Topology
- Interoperation
- Security
- Robustness
DCS Testing for Performance, Capacity, & Topology

- Every update, Every release.
- Under stress.
- New Equipment.
- Old equipment.
- Mixed era operation.
  - 2 decades support typical
  - Hardware versions
  - Software versions
  - Firmware versions

Regression testing & recording.

Over 100 FF transmitter just to prove performance, capacity, interoperability, stability, and general robustness for installation, operation, and maintenance!
DCS Testing for Performance, Capacity, & Topology

- Real FF & HART devices are wired into terminal blocks, power supplies, field termination assemblies, and interface modules as in the real applications, so as to create realistic loading simulations.
DCS Testing for Performance, Capacity, & Topology

- Banks of FF Device Electronics for “load” testing:
DCS Testing for Performance, Capacity, & Topology

- For realistic display and application loads, plan on large numbers of operator stations staffed by a team of test engineers.
DCS Testing for Performance, Capacity, & Topology

- To support the applications and displays, dozens of up-to-date computers will be needed. Plan to replace them every two years.
DCS Testing for Performance, Capacity, & Topology

- Maintain extra controllers “just” for testing and retesting as each element changes.
DCS Testing for Performance, Capacity, & Topology

...and don’t forget the older, legacy generations of equipment. Spare sets for testing must continually revalidate its ability to continue to work with newer generations of equipment.
DCS Testing for Performance, Capacity, & Topology

- Much capital, installation costs, maintenance costs, testing labor costs.
- Various Configurations & Complexions
- Develop, Review, Execute, Test Plans; Record Execution Results.
- Cost without direct revenue.
- Test it or accept the risks associated with not testing it.
Using a Fully Open Infrastructure for a DCS: Dream Come True or Nightmare?

- Background
- Performance
- Testing for Performance, Capacity, & Topology
- Interoperation
- Security
- Robustness
DCS Testing for Interoperability

- Consortium Tests Necessary but not Sufficient.
  - Test subset of specifications
  - Device-oriented, not host system-oriented
  - Specifications good but not perfect
    - Ambiguities
    - Errors
    - Areas of silence
    - Creative device vendors’ imaginations
  - Host system support issues
  - Stress testing

- Direct testing with device vendors

- Testing includes incidentals (power supplies, conditioners, network switches, etc.)
Using a Fully Open Infrastructure for a DCS: Dream Come True or Nightmare?

- Background
- Performance
- Testing for Performance, Capacity, & Topology
- Interoperation
- Security
- Robustness
Security Issues

Potential Vulnerabilities

- Viruses, Worms, Mal-Intended Executables
- Designed for Microsoft & open technology
- Denial-of-Service
  - Could be accidental overload
  - Could be deliberate
- Delivery mechanisms not limited to e-mail requiring user assistance.
Security Issues

- Potential Consequences
  - Render Control Inoperative
  - Render View-Access Inoperative
  - Cause Non-Operation, Mis-Operation, or Mal-Operation
  - Production Loss
  - Equipment Damage
  - Personal Injury
  - Death
Security Issues

- In general, the More Open, the More Vulnerable.
- DCS Vendor Designs minimize these threats
- Do-It-Yourselfers using Open Components need to address these issues.
Using a Fully Open Infrastructure for a DCS: Dream Come True or Nightmare?

- Background
- Performance
- Testing for Performance, Capacity, & Topology
- Interoperation
- Security
- Robustness
Robustness Issues

- Control and Monitoring Functions Must be Particularly Robust
- Failure Modes & Effects Analysis (FMEA)
  - Cause & Effect
  - Severity
  - Probability
  - Ability to Detect
  - Action to Address
- Majority of DCS logic deals with failure mode handling.
- Do-It-Yourselfers Must Address the Same Issues
Trends

- Increasing power of Microprocessors
- Increasing speed of Networks
- Increasing interoperability capabilities
- Increasing security threats
Open Control Systems can be...

- ...vulnerable to fault conditions
- ...vulnerable to overload conditions
- ...problematic with non-validated products (which are sometimes rushed to market)

But DCSs are tightly integrated & tested sets of control elements with distributed functions.
Dependable DCS Vendors…

- Protect their users:
  - Limit open access,
  - Qualify third party devices,
  - Execute comprehensive interoperability tests,
  - Execute extensive Performance, Capacity tests under various topologies,
  - Insure Robustness,
  - Provide guidelines for acceptable loading, interoperation, and security,
  - Re-Test periodic releases.
Do You Want to Do-It-Yourself?

Here are some guidelines..
Guidelines for Do-It-Yourselfers

- Control & Limit open access
- Qualify third party devices (& each revision)
- Execute comprehensive interoperability tests
- Execute extensive Performance & Capacity tests under various topologies.
- Insure Robustness / Stress Resistance
- Provide guidelines for acceptable loading, interoperation, and security.
- Periodically re-test as each element is updated.

(More)
Guidelines for Do-It-Yourselvesers (Cont’d)

- Allocate capital for high-capacity “test” lab.
- Allocate capital for continuing updates to the test lab equipment.
- Employ well-trained test engineers.
- Prepare and review comprehensive test plans.
- Execute and document all tests.
- Repeat test suites when anything changes.
- Consider automating testing wherever possible.
Dream Come True or Nightmare?

- True Openness does not come without a price.

- If we want to connect…
  - anyone’s
  - anything
  - anywhere
  - anytime

- …we must follow the guidelines or accept the risks:
  - Untested elements may not function as intended!
  - Untested elements may interfere with other elements!
  - Costly, unpredictable loss of plant production… or worse could be the consequence!
Questions?

William R. Hodson, P.E.

Honeywell