NSA HCSS Conference
April 18-19, 2006

Assured RTOS:
Research Needs for Assured Real-Time Technology Infrastructure

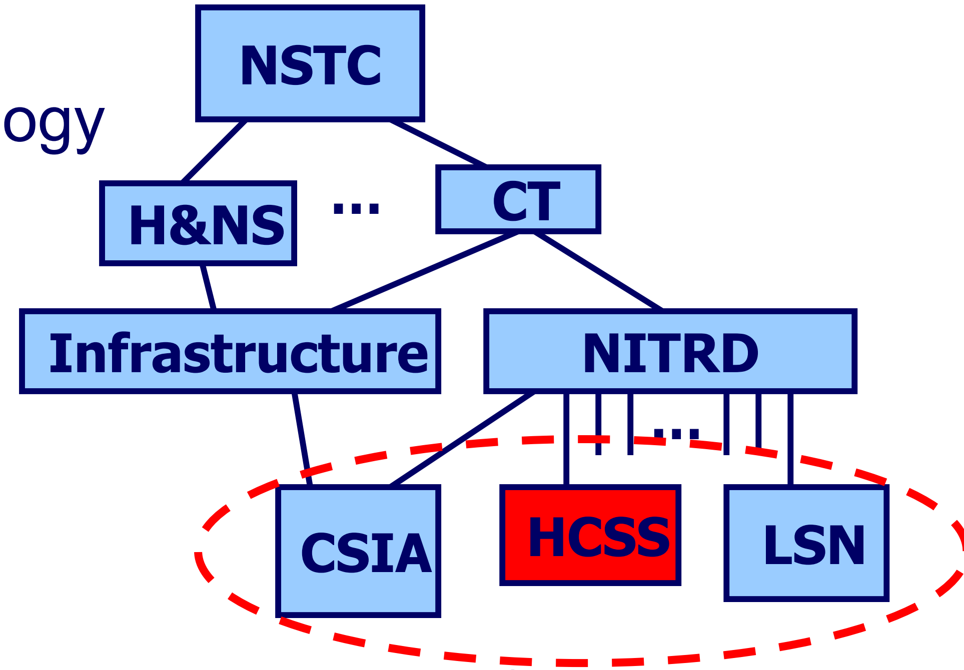
Helen Gill, Ph.D.
CISE/CNS
National Science Foundation

Outline

- High Confidence Software and Systems Coordination Context
- System Trends
- Research Needs Assessment
- Vision for the Future

R&D Coordination for CIP and High Confidence Systems

- NSTC Committee structure
- CT – Committee on Technology
  - Networking, IT R&D (NITRD)
    - Subcommittee, "blue book"
  - Infrastructure Subcommittee
    - CIP R&D Planning
    - National CIP R&D Plan



- **Networking and Information Technology R&D**
  - **High Confidence Software and Systems (HCSS) Coordinating Group**
  - Large Scale Networking (LSN) Coordinating Group
  - Cyber Security and Information Assurance (CSIA) Interagency Working Group

High-Confidence Software and Systems (HCSS) Agencies

- Air Force Research Laboratories*
- Army Research Office*
- Department of Defense/ OSD
- Defense Advanced Research Projects Agency
- Department of Energy
- Department of Homeland Security
- Federal Aviation Administration*
- Food and Drug Administration*
- National Air & Space Administration
- National Institutes of Health
- National Institute of Science and Technology
- National Science Foundation
- National Security Agency
- Office of Naval Research*

* Cooperating agencies

Embedded Systems Trends, Pressures

- Increasingly ***complex*** *multi*-systems, software
  - Mixed hard, soft real-time requirements
  - Subsystem, multi-system control must be coordinated
  - Peer-Peer, not just centralized hierarchical control
- Demand for ***dynamic, adaptive*** response
  - Operation in unpredictably changing contexts
  - Higher, variable (multi-scale) performance demands, resources
- Demand for ***autonomy***
  - Human feasibility restrictions
    - Skill, rate, complexity, attention span, physical tolerance
  - Leverage scarce human resources
- Need to exploit ***platform technology*** advances
  - GHz processors; Gbit networks
  - Integrated processing, common platform assumptions
  - Reconfigurability: FPGAs vs ASICs, DSPs; SoCs

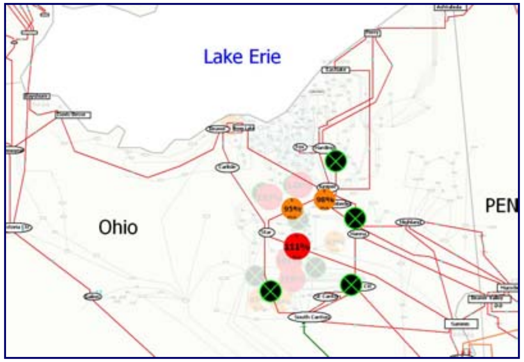
- Cost of assurance and ***certification*** for critical applications

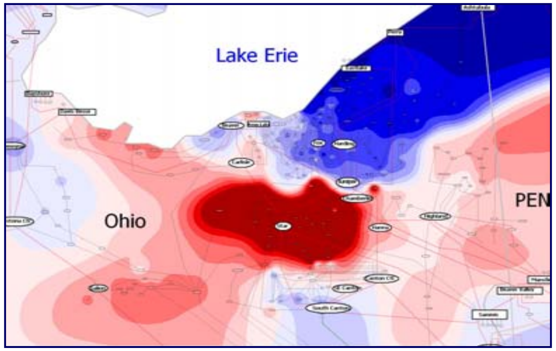
Today's Critical Systems

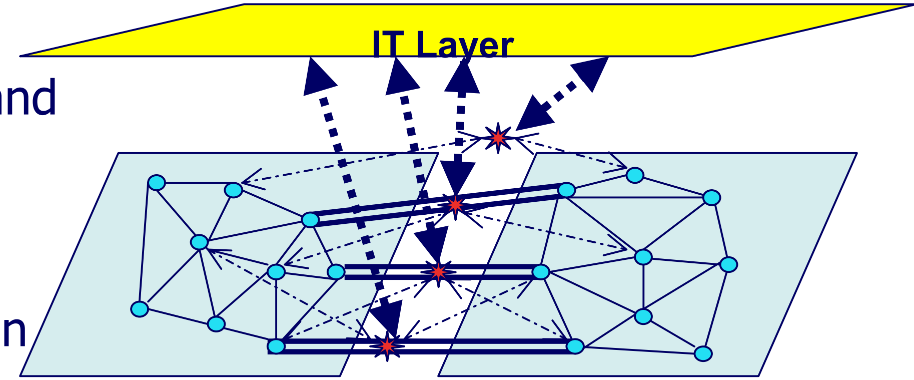
- Critical Infrastructures currently are often managed "at risk" over the Internet, often on commodity platforms
- Critical Infrastructure Protection concerns: interdependent technologies (electricity, oil and gas, telecom, water,…)
  - Cyber vulnerabilities
  - Physical vulnerabilities
- Emerging networked system challenges and ambitions: health care/medicine, power grid/energy systems, transportation, manufacturing, …
  - Many disciplines affected
  - Economic productivity/competitiveness challenge
  - Will today's Internet and today's IT systems technologies enable, impair, prevent?

Example: Electric Power Grid

- **Current picture:**
  - Equipment protection devices trip locally, reactively
  - Cascading failure: August (US/Canada) and October (Europe), 2003
- **Better future?**
  - Real-time cooperative control of protection devices
  - Or -- self-healing -- (re-)aggregate islands of stable bulk power (protection, market motives)
  - Enable green technologies
  - Issue: standard operational control concerns exhibit wide-area characteristics (bulk power stability and quality, flow control, fault isolation)
  - Technology vectors: FACTS, PMUs
  - Context: market (timing?) behavior, power routing transactions, regulation







Images thanks to William H. Sanders, Bruce Krogh, and Marija Ilic

Barrier: An Aging Real-Time Technology Base

- The second IT revolution? "X by wire", large-scale federated/distributed/plug-and-play real-time embedded systems
- Starting point today:
  - Single-system RTOS products (one-size-fits-all)
  - Low-level middleware appliqué for distributed real-time embedded systems
  - Language-centric virtual machines (above? beside? beneath?) OS and Middleware
  - Static, centralized a priori designs
  - Solution clashes, e.g.,
    - Incompatible, non-compositional real-time schedulers
    - Single-issue architectural assumptions (safety, security)
    - …
- Needed: Clean OS/Middleware-level support for assured, open, hierarchical sensing and control systems, dynamic topology, configurable services, coordinated action

Shifting Real-Time System Characteristics

- Shift from cyclic executives + human- and information-centric operation to highly-automated and autonomous
- Shift from centralized to federated, decentralized, open and configurable
- Shift from single-system, closed designs to context-sensitive system designs
- Shift to multi-scale systems
- Still real-time (perhaps wide-area, time-critical), still safety- and security-critical
- Certification still required

What would a suitable real-time technology infrastructure look like for this future?

NITRD HCSS Coordinating Group Assessment and Actions

- NSF Backdrop:
  - NSF/OSTP Critical Infrastructure Protection Workshop, Leesburg, VA, September 2002, http://www.eecs.berkeley.edu/CIP/
  - NSF Workshop, on CIP for SCADA, Minneapolis MN, October 2003 http://www.adventiumlabs.org/NSF-SCADA-IT-Workshop/index.html
  - NSF Real Time GENI Workshop, Reston, VA, February 6-7, 2006

- HCSS CG Study
  - National Academies study: "Sufficient Evidence? Design for Certifiably Dependable Systems," http://www7.nationalacademies.org/cstb/project_dependable.html
  - Kickoff workshop, April 2004, "Software Certification and Dependability" (report)
  - Final report expected May-June, 2006

NITRD HCSS Coordinating Group Assessment and Actions

- Open Verification Initiative
  - Response to Hoare Verification Grand Challenge: Open verification technology for industrial-strength system and software analysis and composition
  - Open Verification Workshop, SRI "Little Engines of Proof" Kickoff, Arlington, VA, April 12, 2004
  - NSA HCSS Meeting, Hoare Grand Challenge Panel, April 13-15, 2004
  - SRI Workshop,Menlo Park February 21-23, 2005, http://www.csl.sri.com/~shankar/VGC05
  - IFIP Working Conference, Zurich, October 10-13, 2005, http://vstte.inf.ethz.ch/
  - SRI "Mini-Workshops" – Palo Alto, CA, April 1-3, 2006
  - NSA HCSS Meeting, April 17-20, 2006

- NSF High Confidence Embedded Systems and Hybrid Systems portfolios
- NIST Static Analysis Summit, Software Assurance Metrics and Tool Evaluation (SAMATE), intramural research
- NASA Langley intramural research, aviation safety
- AFRL CerTA-FCS program
- NSF/FDA Scholar in Residence program
- …

NITRD HCSS Coordinating Group Joint Assessment Actions: Domain-Specific Workshops

- High Confidence Medical Device Software and Systems (HCMDSS),
  - Planning Workshop, Arlington VA, November 2004, http://www.cis.upenn.edu/hasten/hcmdss-planning/
  - National R&D Road-Mapping Workshop, Philadelphia, Pennsylvania, June 2005, http://www.cis.upenn.edu/hcmdss/

- High Confidence Aviation Systems
  - Planning Workshop on *Software for Critical Aviation Systems*, Seattle, WA, November 9-10, 2005
  - National R&D Road-Mapping Workshop, Washington, DC, September 2006

- High Confidence Critical Infrastructures -- “Beyond SCADA: Networked Embedded Control Systems”
  - Planning
    - US Planning Workshop, Washington, DC, March 14-15, 2006
    - EU-US Collaboration Workshop, Framework Programme 7 linkage, March 16-17, 2006
    - US National R&D Road-Mapping Workshop, October/November, 2006

Example: “Beyond SCADA”

Imagining Next Generation Supervisory Control

- Changing Requirements:
  - Open, secure, reconfigurable topology, adjustable group membership
  - Dynamic, multi-hierarchy supervisory control; vertical and horizontal interoperability
  - Complex multi-modal behavior, discrete-continuous (hybrid) control
  - Mixed-initiative and highly autonomous operation
- Changing technologies
  - System integration: Integrated, peer-to-peer, “plug and play”, service-oriented?
  - Fixed & mobile technology vectors: RF/optical/wired/ wireless networking modalities, FPGA and other reconfigurable platforms
  - Physical system technology (e.g., hydrogen, battery technology, other?)
- Changing oversight context
  - End-to-end security, “self-healing”
  - Increased attention to system certification

Further HCSS Actions: Assessment of Real-Time Operating System (RTOS/MW/VM) Technology Base

- HCSS RTOS technology assessment, vendor non-disclosure briefings:
  - Integrators: Adventium Laboratory, Boeing, Ford Motor Company, Lockheed Martin, Honeywell, MIT Lincoln Laboratory, Northrop Grumman, Raytheon, Rockwell Collins, MotoTron
  - Technology: Sun Microsystems, IBM, Microsoft, Honeywell, Red Hat, Wind River Systems, Green Hills, LinuxWorks, Rockwell Collins, Real-Time Innovations, Inc., QNX Software Systems, Ltd., BAE Systems, Kestrel Technology, BBN Technologies
- Upcoming: OMG Annual Summer Embedded Systems Workshop, Washington, DC, July 7-10, 2006

Cross-cutting Computing Technology Conclusions

Technical gaps identified:

- Lack secure, interoperable, scalable real-time technology base
- System stack (RTOS, virtual machines, middleware) needs re-factoring, extension, scaling, e.g.
  - Coordination (e.g., timed/synchronized, reactive)
  - Dynamic hard/soft real-time scheduling, resource management
  - System security services
  - Recovery services
  - Run-time configuration services
- Lack secure real-time networking capability for critical infrastructures
- Lack appropriate system and software architectures, and "middleware" components for high-confidence sensing and control systems
- Lack end-to-end, semantically-sound design and composition technology

Problems Not Yet Solved

- How to build predictable real-time, networked systems
- How to formulate and manage high-confidence dynamically configured systems
- How to organize interoperable "aggregated" systems
- How to cooperatively detect and manage interference among systems in real time, avoid cascading failure
- How to formulate an evidential (synthetic and analytic) basis for trusting systems
  - Span stages of development
  - Accommodate product, process information; achieve new design culture

Also, a programmatic challenge: How do we get from here to there?

What mix of foundational, systems, experimental work?

HCSS Vision: An Assured Real-Time (RT) OS Technology Base (ARTOS-TB)

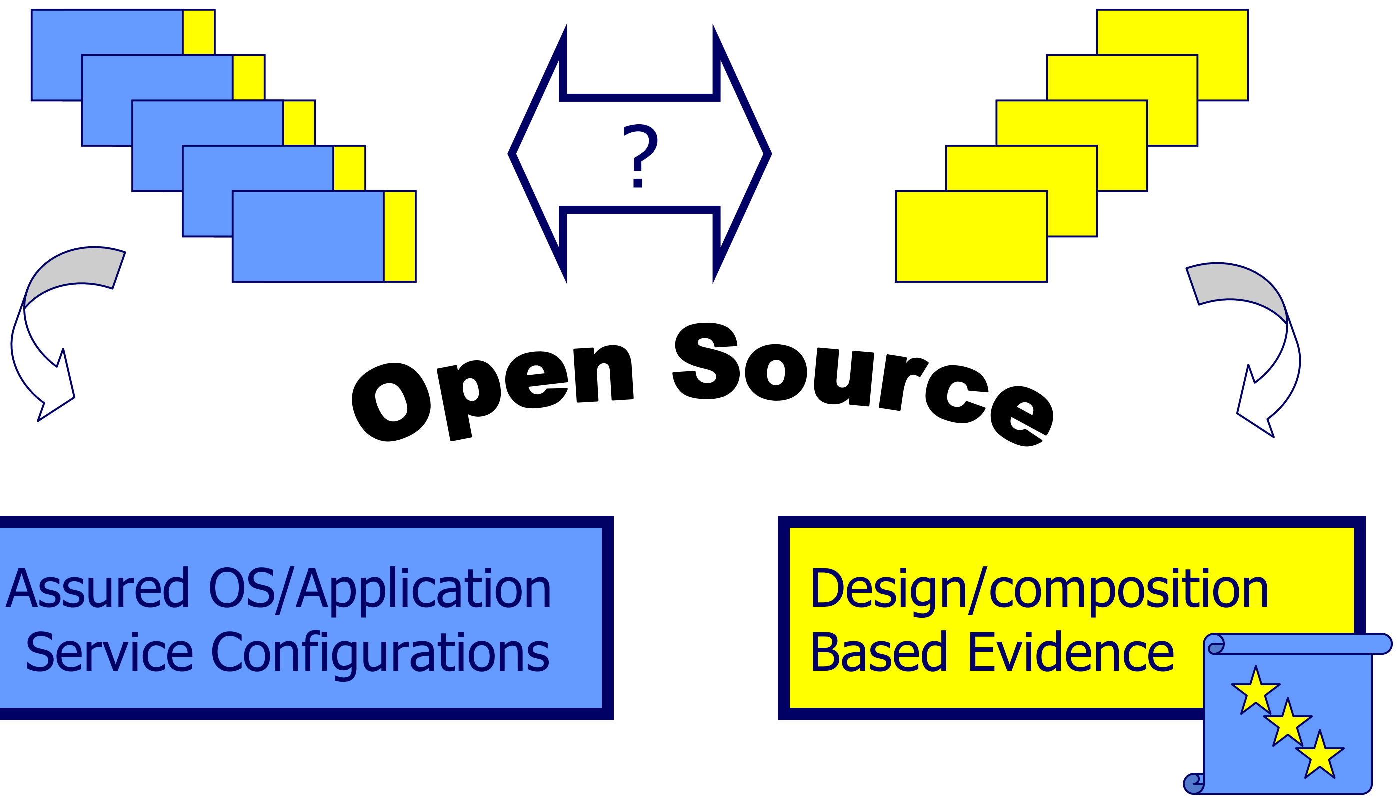
Now	Goal
Separate, closed systems	Network-enabled open RT systems
Multiple RT systems, ad hoc interaction	OS-supported management of networked RT multi-systems
Monolithic RTOS, add-on middleware, VM	Composable, parameterized, reconfigurable systems services
Manually-configured systems	Service configuration and checking
Process-oriented, test-based certification	Certification based on design and composition evidence

Taking Stock: What Can We Build On?

- Configurable platform and OS technologies
  - FPGAs, SoC technology
  - Multi-core, multi-threading (or not)
  - OS Kit, Exokernel, Vino, Spin, K42
- Global Environment for Networking Innovations (GENI)
- Configurable services, organizing mechanisms
  - Tool-chains (e.g., Eclipse)
  - Service-oriented architectures, mechanisms (e.g., OASIS Web Services Business Process Execution Language, WSBPEL)
  - Service sets, configuration checking (e.g., Common Criteria, EALs)
  - Autonomic systems (e.g., IBM, Microsoft Dynamic Systems Initiative -- DSI)
- Virtualization, middleware "narrow waist" designs
  - Provide portability, design abstraction, stability
  - Massive reuse of important technology components
- Progress in modular verification, type systems, static analysis technology
- Recognition of need for end-to-end design technology (e.g. MDA)

Overall HCSS Vision

- Composable, Assured, Real-Time Operating Systems Technologies
- Composable Evidence/Assurance Technologies



Thank You

HCSS Goal: Assured Technology Base

- Coordinated control systems applications
  - Unmanned autonomous air vehicles, automotive applications
  - SCADA systems for power grid, pipeline control
  - Remote, tele-operated surgery?
  - OR, ICU, EMT of the future?
  - Nano/bio devices, platform-level control

- Key areas for transformative research
  - Open sensing and control platforms
    - Reconfigurable coordinated control
  - Computation system and networking substrate
    - Assured RTOS, networking, middleware, virtual machines
    - Integral cyber security for system control
    - Real-time Internet
  - Assurance methods and software/system composition technology

Example Research Problems

- Devise fundamental systems mechanisms for the control and data planes of network- and software-integrated open systems
- Re-factor OS/VM/MW to develop and combine mechanisms
- Re-visit the OS/VM/MW layering philosophy
- Develop a new service- and component- structured OS technology
- Develop design technology for assembling tailored systems from ARTOS-TB, open sensing and control platforms, with evidence of correct composition
- Develop policy/specification/model-based system configuration infrastructure