



High Confidence Software and Systems:

Interagency Context and NSF Perspective

**National Workshop
Beyond SCADA and DCS:
Networked Embedded Control for Cyber-Physical Systems**

**Pittsburgh, PA
November 8-9, 2006**

Helen Gill, Ph.D.
CISE/CNS
National Science Foundation
Co-Chair, NITRD High Confidence Software and Systems Coordinating Group



Overview

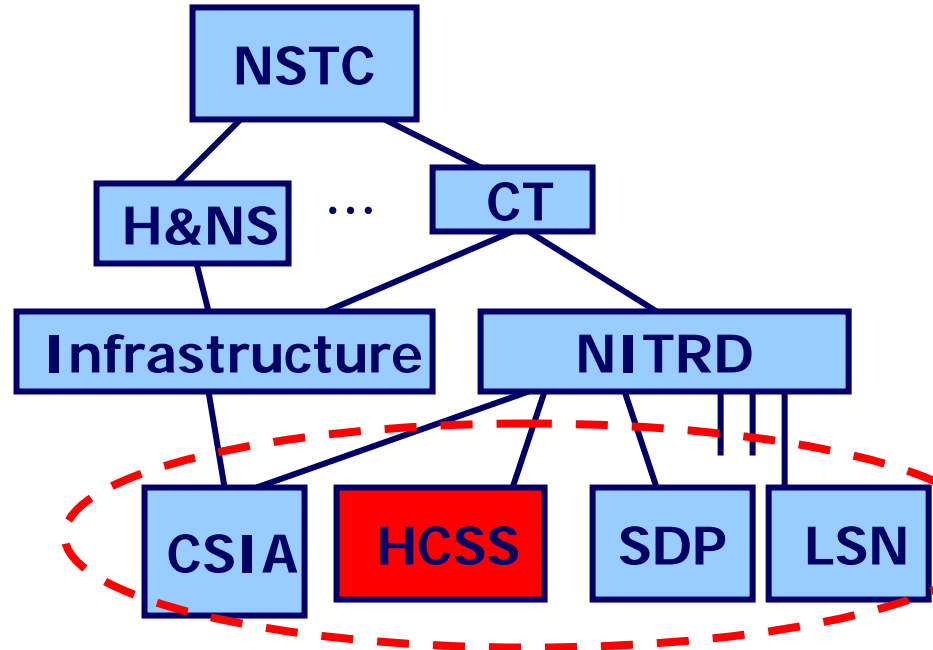
- HCSS interagency research coordination
- Workshop motivation and emerging context: technical, economic
- NSF perspective on S&T challenges
- Expectations



Interagency R&D Context in HCSS

High Confidence Software and 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
 - CIIP R&D Plan



- **NITRD R&D Planning - High Confidence Software and Systems (HCSS) Coordinating Group**
- Software Design and Productivity 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 and Air Force Office of Scientific Research*
- 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*



NITRD HCSS Coordinating Group Assessment and Actions



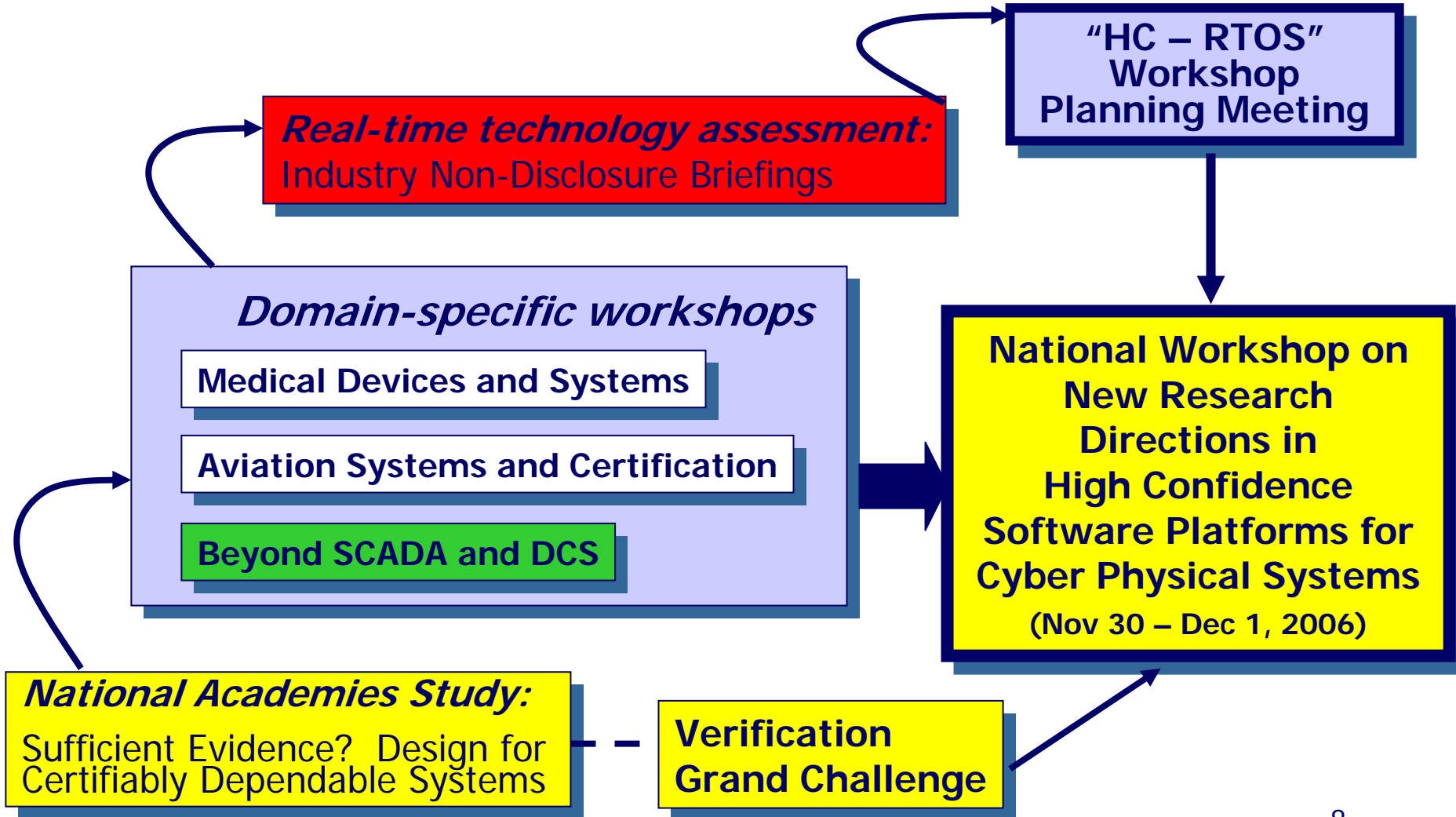
- NSF Backdrop:
 - NSF/OSTP Critical Infrastructure Protection Workshop, Leesburg, VA, September 2002, <http://www.eecs.berkeley.edu/CIP/>
 - NSF Workshop, on CIP for SCADA, Minneapolis MN, October 2003
<http://www.adventiumlabs.org/NSF-SCADA-IT-Workshop/index.html>
 - NSF Real Time GENI Workshop, Reston, 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 November, 2006 ("Justifiable Confidence"?)



- 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
 - Roadmap, executive group – kickoff September, 2006

- AFRL CerTA-FCS program
- AFOSR, ONR, ARO MURI programs
- NSF High Confidence Embedded Systems and Hybrid Systems portfolios
- OSD Advancing Software-Intensive-Systems Producibility, National Academies study; Software Wind Tunnel
- NIST Static Analysis Summit, Software Assurance Metrics and Tool Evaluation (SAMATE), intramural research
- NASA Langley intramural research, aviation safety
- NSF/FDA Scholar in Residence program
- DARPA/NSF ESCHER repository
- ...

HCSS R&D Needs Assessment





Multi-agency HCSS Activities, Planning and Coordination



www.nitrd.gov -> more -> HCSS

- HCSS 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/>
 - Aviation Software Systems for the Second Century of Flight: Design for Certifiably Dependable Systems (HCSS-AS) (NSF, AFRL, NASA, FAA)
 - Planning Workshop, Seattle, WA, November 9-10, 2005
 - National R&D Road-Mapping Workshop, Alexandria, Virginia, October 5-6, 2006
 - **High Confidence Critical Infrastructures: “Beyond SCADA: Networked Embedded Control Systems” (NSF, NIST, NSA)**
 - US Planning Workshop, Washington, DC, March 14-15, 2006
 - US National R&D Road-Mapping Workshop, Pittsburgh, Pennsylvania, November 8-9, 2006

Domain-specific workshops



- HCSS RTOS technology assessment, vendor non-disclosure briefings:
 - Integrators: Adventium Laboratory, Boeing, Ford Motor Company, Lockheed Martin, MIT Lincoln Laboratory, Northrop Grumman, Raytheon, Rockwell Collins, MotoTron
 - Technology: Sun Microsystems, IBM, Microsoft, Honeywell, Red Hat, Wind River Systems, Green Hills, LinuxWorks, Real-Time Innovations, Inc., QNX Software Systems, Ltd., BAE Systems, Kestrel Technology, BBN Technologies
- Technical gaps confirmed in vendor briefings:
 - Lack coherent framework with interoperable, scalable real-time technology services:
 - Coordination services (e.g., timed/synchronized, reactive)
 - Dynamic hard/soft real-time scheduling
 - System security services
 - Recovery services



- Technical gaps confirmed in vendor briefings (continued):
 - Secure, real-time networking capability for critical infrastructures
 - Principled system and software architectures and platforms for high-confidence sensing and control systems
 - Rational virtualization and architectural strategies to replace chaotic system stack (RTOS, virtual machines, middleware)
 - Flexible partitioning for mixed-criticality, mixed-security-level systems
 - End-to-end design and composition technology for high-confidence systems, configuration management
 - Support for certification of systems software technology, applications, design and development tools



NSF Update

Technology Substrate for CPS (continued)



- New Research Directions in High Confidence Software Platforms for Cyber-Physical System Technologies (NSF, HCSS Agencies)
 - Planning Workshop, Arlington, VA, July 10, 2006, in conjunction with OMG RTES workshop
 - National R&D Road-Mapping Workshop, Alexandria, VA, November 30-December 1, 2006

(Systems x Assurance)



NSF Update: Technology Substrate for "Cyber-Physical Systems"



- NSF Global Environment for Networking Innovation
 - GENI testbed, <http://www.nsf.gov/cise/geni/>
 - Future InterNet Design (FIND), now includes real-time component
- NSF Cyber Physical Systems (CPS) exploratory (seedling) activities
 - Community-led planning, NSF CISE and ENG directorates
 - FY 2006: CPS planning studies commissioned from senior academics
 - FY 2006: Evidential Tool Bus – exploratory research (Rushby, SRI)
 - Discussions with corporate VPs, CEOs initiated
 - CPS workshops:
 - NSF CPS Community Planning Meeting, Arlington, VA, July 27-28, 2006
 - NSF CPS National Meeting, Austin, TX, October 16-17
- FY 2007 Computer Systems Research announcement, NSF 07-504;
http://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf07504
 - ***Cyber-Physical Systems thematic area (seedling)***
 - *Related topic: Virtualization for Configuration Management*



Workshop motivation, economic and technical contexts



Premises Motivating this Workshop



- Networked embedded sensing and control will be a (the?) principal enabler of all future engineered and regulated physical systems.
- It is insufficient simply to secure existing networked sensing and control systems; today's control technology is fundamentally inadequate for tomorrow's systems.
- The systems sciences, including computational control, dynamical systems, real-time systems, fault tolerant systems, resource management, and system security, require rethinking to achieve a unified foundation.
- The cyber technology infrastructure substrate should provide support at levels of abstraction that enable systems we envision for the future.
- Design and implementation technology should support the production of evidence that the built system is safe, secure, reliable, and behaves correctly.



Economic Context: Calibrating US Competitiveness



- American Competitiveness Initiative announced:
<http://www.whitehouse.gov/stateoftheunion/2006/aci/>
- National Academies study: **“Rising Above The Gathering Storm: Energizing and Employing America for a Brighter Economic Future”**
http://www7.nationalacademies.org/ocga/testimony/Gathering_Storm_Energizing_and_Employing_America2.asp

Economic Context: Calibrating US Competitiveness



Example: EU Framework Programme 7, European Research Council, and related actions

- ARTEMIS
 - Backbone of European Research Area for Embedded Systems, <http://www.artemis-office.org/>
 - Strategic Research Agenda (SRA)
 - Joint Technology Initiative (JTI)
 - Embedded systems education and curriculum
 - “High-Level Group”
 - CEOs: ABB, Airbus, Nokia, Parades, British Telecom, COMAU, Philips, Bosch, Continental Teves, Daimler/Chrysler, ST Microelectronics, Symbian, Ericsson, Finmeccanica, Telenor, Thales, IMEC, Infineon
 - Universities and national research labs: TU Vienna, CNRS/Verimag
 - Joint public and private funding



Technical Challenges



Technical Challenges: Changing Real-Time System Characteristics



- Shift from cyclic executives + human- and information-centric operation to highly-automated, autonomous, coordinated
- Shift from single-system, closed designs to context-aware system architectures
- Shift from centralized to federated, decentralized, open and configurable
 - Fluid mix of federated and integrated architectures
 - Modularity becomes a central issue in both
 - Changing platform technologies
- Shift to multi-scale systems, mixed synchronous/reactive 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?

Example: Health Care and Medicine

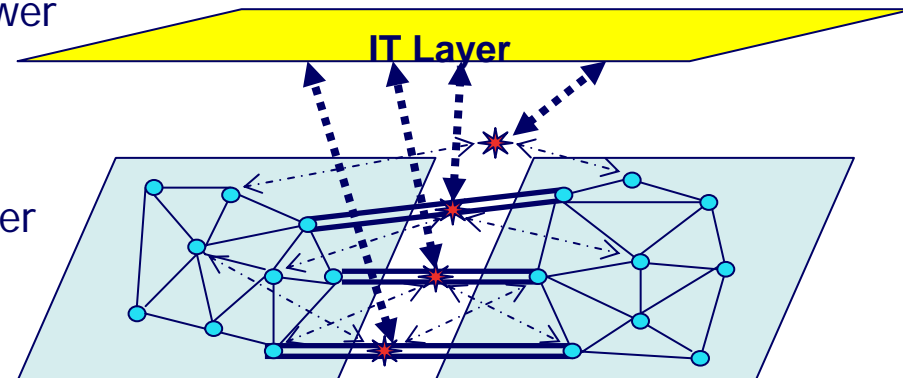
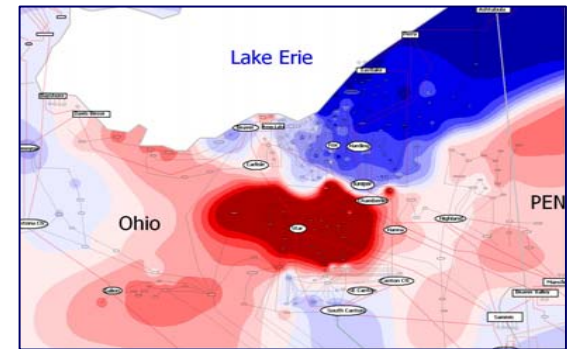
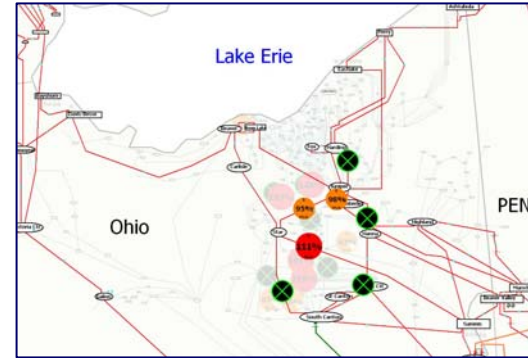
- National Health Information Network, Electronic Patient Record initiative
 - Medical records at any point of service
 - Hospital, OR, ICU, ..., EMT?
- Home care: monitoring and control
 - Pulse oximeters (oxygen saturation), blood glucose monitors, infusion pumps (insulin), accelerometers (falling, immobility), wearable networks (gait analysis), ...
- Operating Room of the Future (Goldman)
 - Closed loop monitoring and control; multiple treatment stations, plug and play devices; robotic microsurgery (remotely guided?)
 - System coordination challenge
- Progress in bioinformatics: gene, protein expression; systems biology; disease dynamics, control mechanisms



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; smart motor loads
 - 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





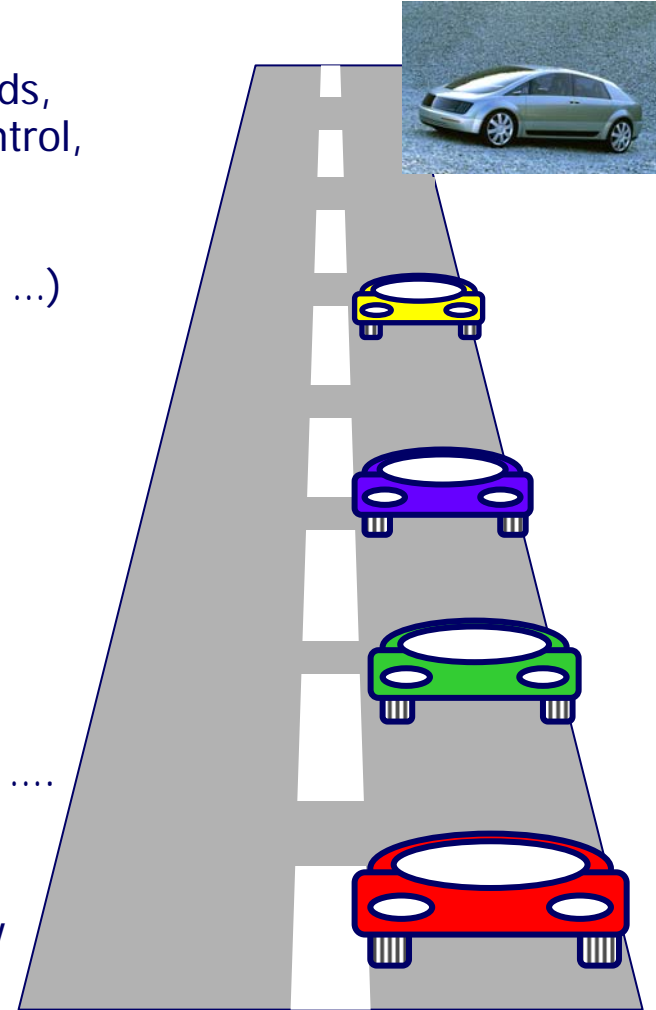
- **Current picture**

- Largely single-vehicle focus
- Integrating safety and fuel economy (full hybrids, regenerative braking, adaptive transmission control, stability control)
- Safety and convenience “add-ons” (collision avoidance radar, complex airbag systems, GPS, ...)
- Cost of recalls, liability; growing safety culture

- **Better future?**

- Multi-vehicle high-capacity cooperative control roadway technologies
- Vehicular networks
- Energy-absorbing “smart materials” for collision protection (cooperative crush zones?)
- Alternative fuel technologies, “smart skin” integrated photovoltaics and energy scavaging, ...
- Integrated operation of drivetrain, smart tires, active aerodynamic surfaces, ...
- Safety, security, privacy certification; regulatory enforcement

- **Perennial context: Time-to-market race**





- Current OS, VM, Middleware technology
 - Commercial RTOS concept: >25 years old, “full-service”, very heavyweight certification
 - Real Time Middleware: 15 years old
 - Real Time Virtual machines: 10+ years, language-specific
 - Special purpose OS for sensor nets: 7-8 years old, lightweight, low capability
- Low level service abstractions, ad hoc design and integration technology – ***silent on networked control support***
- Ad hoc layering, lack of systematic virtualization principles
 - Solution clashes, e.g.,
 - Incompatible, non-compositional real-time schedulers
 - Single-issue architectural assumptions (safety, security)
- “Test until the money runs out”

Collectively, not an adequate real-time technology base for flexibly building tomorrow's high-confidence systems



Core Underlying Problems, Not Yet Solved



- How to build predictable real-time, networked systems at all scales
- 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?

Hoped-for Outcomes of this Workshop

- **Assessment:**
 - Current state of science and technology for interacting control systems (both vertical and horizontal interaction)
 - Current state of linkage with other areas of science and technology (real-time systems, fault tolerance, security, networked communication, ...)
- **Looking forward:**
 - Opportunities for near-term progress (Generalize distributed control? Extend hybrid control?)
 - Longer-term research objectives for multi-level, multi-scale cooperative control and authority management (exploiting both cyber and physical properties)
 - Specific identification of “hard problems” that new research must tackle
- **Product:** Roadmap, action plan, hard problems list for next generation networked control technology
 - Support deeply-integrated cyber-and-physical systems where loops may close at all levels and scales (semi-autonomous, autonomous, cooperative systems and subsystems)
 - Provide certification evidence for composition, cooperation
 - Build “safety/security/assurance” culture that can bridge across domains



Thank You