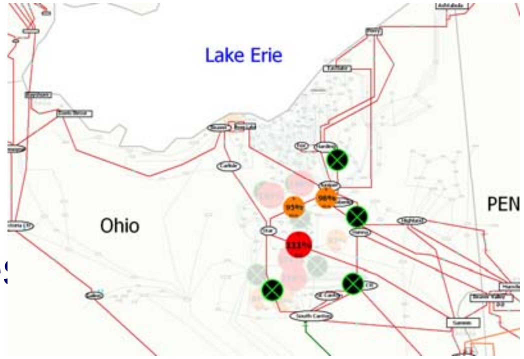
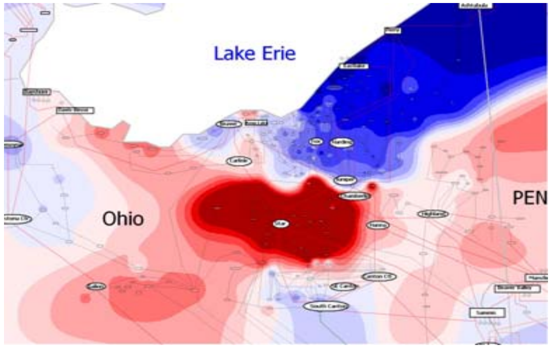
High Confidence Computing Technology and Power Grid Research

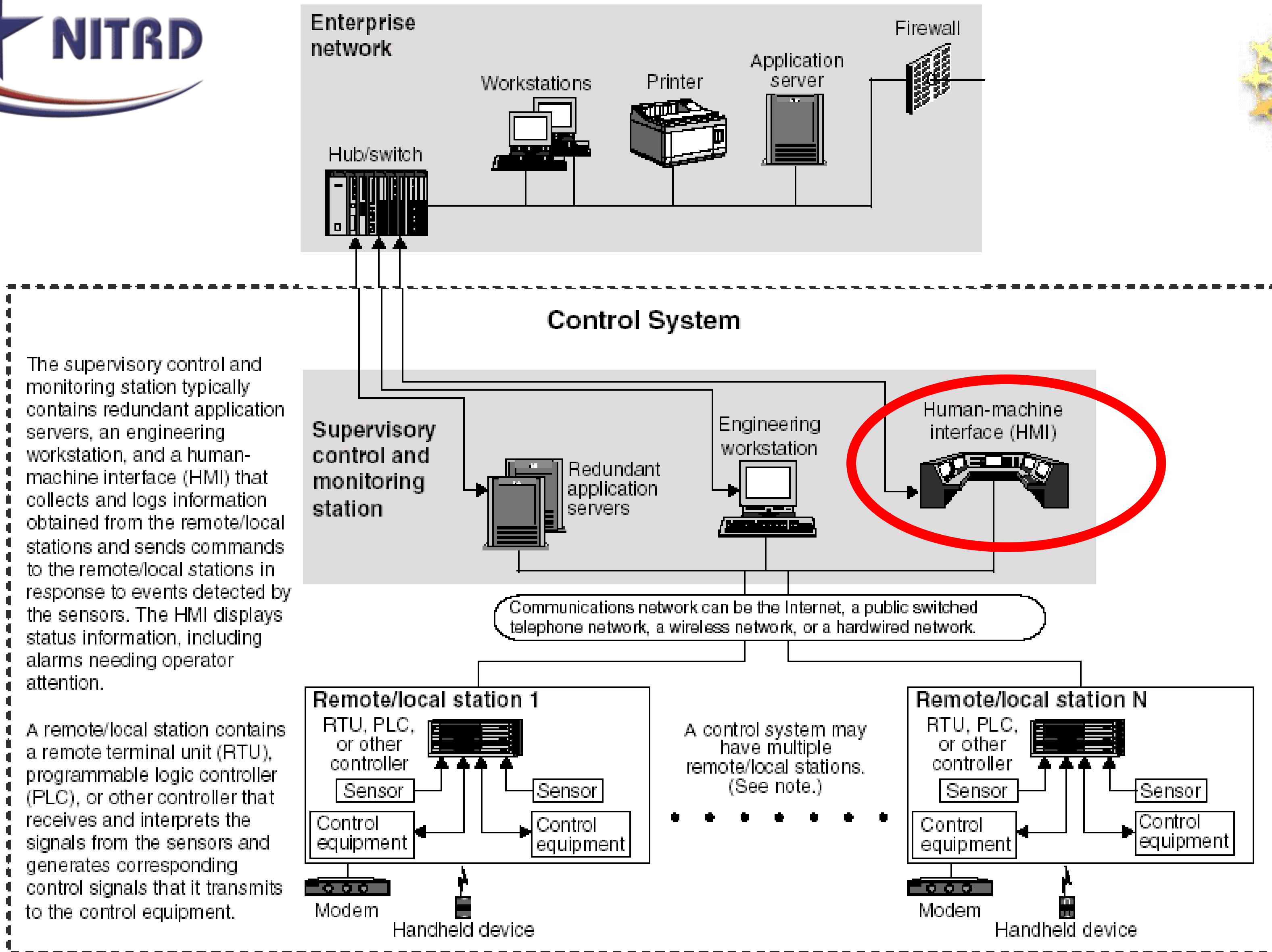
Helen Gill, Ph.D.
CISE/CNS
National Science Foundation

U.S. Power Grid: Well-Known Challenges

- Status
  - Vulnerability to failures, attacks, misuse
    - Cascading failures, market manipulation
    - Waning expertise, training limitations
    - Insider threats
    - Interdependencies of Critical Infrastructures
  - Slow pace of technology insertion
    - Micro-grids
    - FACTS, PMUs, etc.
  - Technical, market barriers to change
- A Critical Infrastructure, in need of:
  - Protection (cyber security)
  - Renewal







Illustration, GAO Report: CRITICAL INFRASTRUCTURE PROTECTION Challenges and Efforts to Secure Control Systems (GAO-04-354)

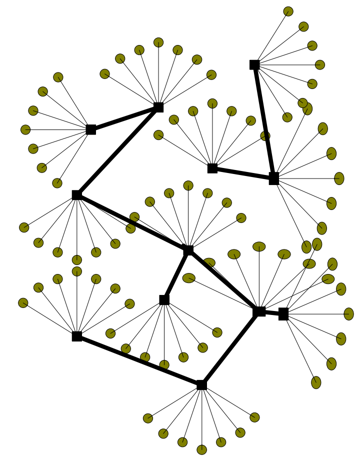
From the Outside: A View of The Power Grid

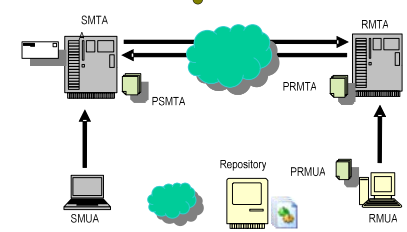
- Current
  - Human-centric system of systems, information-enabled regional coordination
  - Static structure, with protection equipment, human operation
  - Built infrastructure; stressed by power routing; complex market, regulatory, and advisory environment
  - No storage, shrinking stability margin
  - Not secure, minimal cost incentive to change
  - Enterprise/market/control interaction, air gap violated

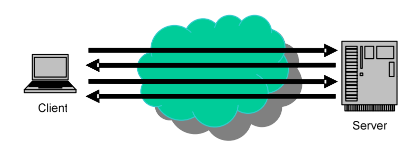
- Midterm
  - FACTS – better flow control
  - PMUs – better local state information
  - Super-capacitors – better buffering, increased stability
  - GridWise, GridStat, ...-- better global information
  - NERC 1200 Security Standard: guidelines, progress toward industry-specific IT security standards, SCADA security

The Outsider's Strawman (Continued)

- Long Term, "Energy Independence" Future Goal
  - Physical System
    - Highly decentralized, distributed generation, configurable sources, ubiquitous measurement and flow gating devices
    - Intermittent sources, smart motor loads
    - Storage? (Hydrogen, battery, ...)
  - Information Technology
    - ***Next generation supervisory control***
      - System of real-time embedded systems, muti-authority (local? regional?) structure,
      - Real-time, multi-modal, mixed-initiative control
      - Open, dynamic topology
    - Security built in, policy-driven, adaptive





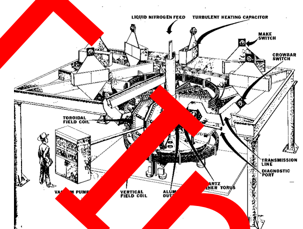


Diagrams, courtesy UIUC/Cornell U./Dartmouth U./WSU

A (fairly obvious) prediction about the Future of Physical and Engineered Systems

IT Inside

- Power generation and distribution
  - Deregulation, competition
  - Mix of generation technologies
    - Fossil fuels
    - Solar, wind
    - Hydrogen, fuel cells
    - Fusion?



- Future airspace
  - Airspace management
    - Free flight
    - UAVs
    - Critical Infrastructure Protection
  - Higher performance vehicles

- Health care
  - Infusion pumps, ventilators,...
  - EMT and ICU of the future
  - Triage and transport
  - Home care

- General transportation
  - Highway system technologies
  - Vehicle technologies
    - Hybrid engines, alternative fuels
    - Coordinated motor, braking, transmission
    - Continuously varying transmission control
    - ABS, regenerative braking, etc...

- Environmental monitoring
  - Global warming
  - Environmental observation instrumentation, control
- Agriculture and ecology
  - Herd health monitoring
  - Remote veterinary care
  - Crop condition monitoring
- Emergency response
  - Rescue robotics
  - Command and control

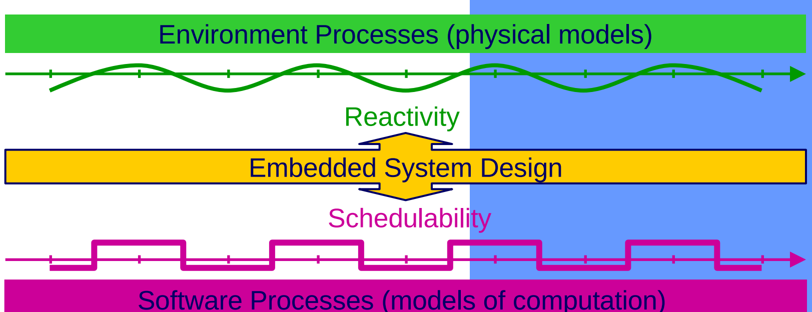
Photo Credits: Boeing, GM, Medtronics

Status Check: Embedded Systems for Engineering and Science

- Embedded systems, expanding scope (simple to complex, HW-SW to full system)
- IT multiplier for engineered system capability
- Risk set, reliance changes (e.g, critical infrastructures)
- Increasing assurance obligation
- Need for global interoperability, harmonization

End-to-end problems, but previously-separate research areas:

- Real-time embedded systems
- Control theory and engineering
- Networking
- Physical device and platform design
- Security and privacy
- Human-computer interaction
- Science and engineering research domains



(Diagram, courtesy of R. Alur, U. of Pennsylvania)

Current NSF/CISE High Confidence Embedded and Control Systems Research

- NSF funds core research
  - Strong scientific, engineering, and implementation base for complex, adaptive, embedded sensing and control systems
  - Improved basis for certification of systems
- Individual investigator research in core program, plus Information Technology Research
- SCADA research poses interdisciplinary challenges
  - Long-term research
  - Community/project-oriented research strategies
    - Centers
    - Problem-driven research
  - Technology transition and standardization

Context: Power Network Complexity

- Regulatory goals: spur competitive pricing, enable market entry
- Other strategic goals: improve National energy independence posture, reduce vulnerability (distributed generation, co-generation, renewables, hydrogen, biomass, ...)
- Issues: reliability of the power infrastructure
  - Need for stable bulk power market vs.
    - Changing load and generation characteristics
    - Connectivity, transmission capacity
    - Market structure and dynamics (e.g., Independent System Operators, public utilities, Affiliated Power Producers, Independent Power Producers)
  - Potential regulatory shifts
    - Functional sub-sector separation (generation, transmission, distribution)
    - Other structural proposals
- Industry ambition: power electronics ("X-by-wire")
- Status: current IT infrastructure appears to be qualitatively inadequate for reconfigurable coordinated control, information and process security, emergency adaptation.

Generalization: SCADA and Industrial Control Systems Today

- Today's technology and methodology
  - Instrumentation, low-level process control, and telemetry
  - Local operation
  - Data acquisition for communication and human decision-support for wide-area "global" operations
- Trends, issues:
  - Deregulation (e.g., energy markets, power routing)
  - New technologies (e.g., renewables, fuel cells, ...)
  - Market effects: start-ups, scale, dynamics, indirect consequences (e.g., environment)
  - Capacity investments: where, how?
  - Operation at (beyond) capacity, shrinking safety margins
  - SCADA delivered via Internet (web services, .NET,...)
  - Interdependencies (e.g., power, telecommunications, Internet)
  - Cyber attacks attempting to penetrate process control systems
  - Reliability metrics, certification

Is today's industrial control concept enough?

Next Steps

- Examine specific critical systems requiring SCADA information technology (emphasis on power grid, but also chemical processing, water systems, petrochemical transport, ...)
- Develop a vision and research directions for future industrial infrastructure systems, considering:
  - "Vertical" integration from low-level digital control, process control, to (multi-level) supervisory control
  - "Horizontal" coordination among regions, other structures ("coalitions")
  - Interoperable, open systems service needs (not just hardware platforms) for dynamic topology, reconfiguration support, protection
  - Secure operation, interoperation (***built-in***), on a secure substrate

Challenge: Next-generation supervisory control

High Confidence Systems Technical Challenge: "Systems of Embedded Systems"

- Now: information focus, human-machine interface
  - Operator skill, "competent human intervention"
  - System, operator certification
- Future: open, multi-level closed loop, mixed initiative, autonomous systems and multi-systems
- Typical domains:
  - ***Medical:*** "plug and play" operating room of the future
  - ***Aviation:*** mixed manned, autonomous flight
  - ***Power systems:*** Future "SCADA-D/PCS" for distributed generation, renewable energy resources
  - ***National Security:*** common operating picture, global information grid, future combat systems

“Beyond SCADA”

Imagining Next Generation Supervisory Control

- Changing Requirements:
  - Open, reconfigurable topologies, adjustable group membership
  - Reconfigurable, 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 reconfigurables
  - Power system storage capacity (hydrogen, battery technology, other?)
- Changing oversight context
  - End-to-end security, “self-healing”
  - Increased attention to system certification

National CIP R&D Plan

April 8, 2005

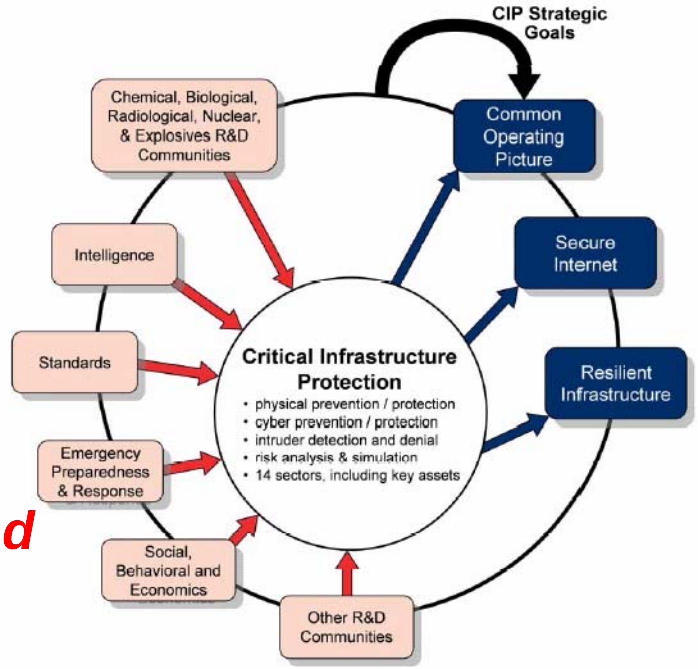
NCIP R&D Roadmap identifies three strategic goals:

- National Common Operating Picture
- Secure National Communication Network
- Resilient, Self-Healing, Self-Diagnosing Infrastructure

Themes:

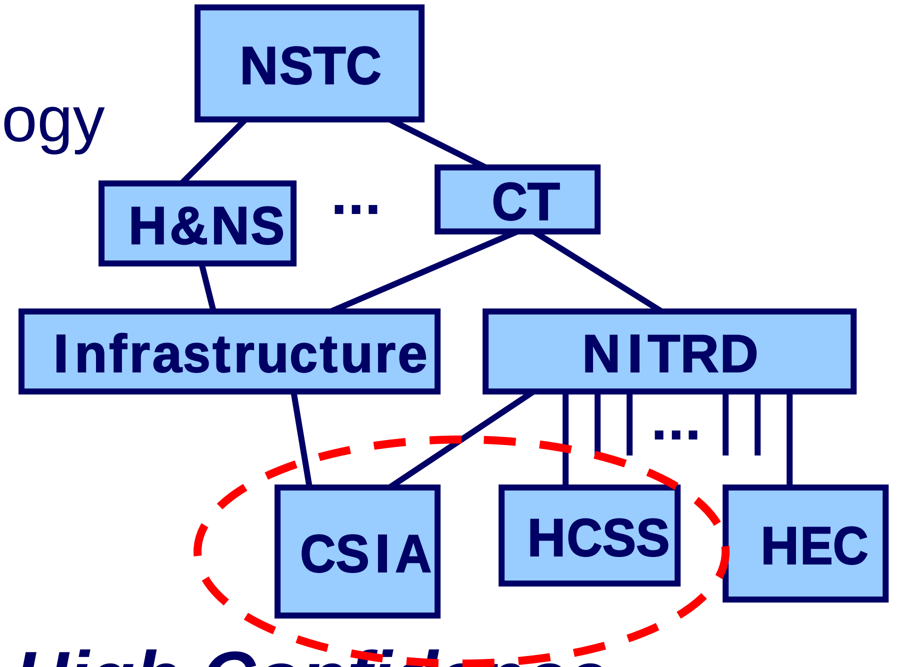
- **Detection and Sensor Systems**
- **Protection and Prevention**
- **Entry and Access Portals**
- **Insider Threats**
- **Analysis and Decision Support Systems**
- **Response, Recovery, and Reconstitution**
- **New and Emerging Threats and Vulnerabilities**
- ***Advanced Infrastructure Architectures and Systems Design***
- **Human and Social Issues**

http://www.bfrl.nist.gov/PSSIWG/documents/2004NCIP_R&D_Plan_FINAL.pdf



R&D Planning 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
    - CIIP R&D Plan



- ***NITRD R&D Planning - High Confidence Software and Systems (HCSS) Coordinating Group***
- Cyber Security and Information Assurance (CSIA) Interagency Working Group

NITRD HCSS Coordinating Group Assessment Actions

- 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
  - National Academies' study: "Sufficient Evidence? Design for Certifiably Dependable Systems", http://www7.nationalacademies.org/cstb/project_dependable.html

- National Coordination Office summary report(s) derived from workshops, industry input sessions, NAS study

NITRD HCSS Coordinating Group Assessment Actions: 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 21-22, 2005
  - National R&D Road-Mapping Workshop, venue TBD, June/July 2006

HCSS Workshops, continued

- ***High Confidence Critical Infrastructures: "The Electric Power Grid: Beyond SCADA"***
  - 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, date TBD, 2006

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

- Key areas for transformative research
  - Open control platforms
    - Reconfigurable coordinated control
  - Computational 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

Other Current HCSS Actions: Assessment of Real-Time Operating System (RTOS) Technology Base

- Starting point: single-system RTOS products, middleware appliqué for distributed systems, rudimentary open sensing and control platforms (incompatible schedulers, single-issue architectural assumptions, weak security services, ...)
- Needed: Clean OS-level support for open, hierarchical control systems, dynamic topology, coordinated action
- So what are we doing about this?
  - 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

Cross-cutting High Confidence Computing Technology Challenges

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
  - System security services
  - Recovery 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 assured design and composition technology

Making it Real

- Joint power systems and high-confidence computing research towards Advanced Infrastructure Architectures and Systems
- Example target: renewables and distributed generation/micro-grid research opportunity
  - Inherent importance: Vector for change in energy dependence picture via new and emerging markets, decentralization for less vulnerable infrastructure
  - Attractive and accessible laboratory for multi-level, time-sensitive/real-time interoperation
  - Feasible concurrent engineering and experimental setting for both: cutting-edge power systems research and real-time embedded control research
  - Fosters US competitiveness in control systems, electrical power systems, and embedded systems technologies

NSF CISE Research Venues for Critical Infrastructure, Power Systems

- CISE/CNS Computer Systems Research Program
  - Embedded and Hybrid Systems disciplinary area
  - (Watch for new emphasis areas in FY 2007 announcement)
- CISE/CNS Networking Research
  - "Clean Slate" Internet research initiative
  - Planning grant: study on real-time networking for critical infrastructures
- NSF Science and Technology Center: TRUST
  - UC Berkeley, with Vanderbilt, Cornell, Stanford, CMU, ...
  - http://trust.eecs.berkeley.edu/
- Engineering Research Centers: current competition
- Information Technology Research, competition ended, active grants remain (EU-US linkages, G.3 and D.4):
  - Secure and Robust IT Architectures to Improve Survivability of the Power Grid, CMU/WSU
  - Multi-Layered Architecture for Reliable and Secure Large-Scale Networks, CMU
  - Center for Hybrid and Embedded Systems (CHESS), UC Berkeley
- Infrastructure Programs
  - Major Research Infrastructure: Laboratory to Study FACTS Device Interactions, U. of Missouri at Rolla
- Cyber Trust
  - FY 2005 Center-Scale portfolio, Trustworthy Cyber Infrastructure for the Power Grid, University of Illinois at Urbana-Champaign

Thank you

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
- 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