Federal Networking and Information Technology R&D

Remarks to the HCSS-Sponsored National Workshop on Beyond SCADA: Networked Embedded Control for Cyber Physical Systems

Workshop Deliverables: Roadmap, Hard Problems, and Report

Pittsburgh, Pennsylvania
November 8, 2006

Sally E. Howe, Ph.D.
Associate Director
National Coordination Office for Networking and Information Technology Research and Development
(NCO/NITRD)

Template for Preparing NITRD Workshop Reports

- **About This Report**
- **Executive Summary**
  - Includes summary of hard problems and research roadmap
- **PART 1: Background, Scope, and Framework**
- **PART II: Technical Perspectives and Analyses**
  - For each technical topic:
    - Nature of the problem
    - What can we do well?
    - What can't we do well?
    - Why can't we declare victory?
    - R&D challenges and hard problems
    - Research strategies and roadmap
- **PART III: Conclusion**
- **PART IV: Appendices and Acknowledgements**

Recommended Contents and Features of R&D Roadmap

- Milestones
- Assessment Metrics
- Identification of Interdependencies
- Timeline
- Strategy for Deploying R&D Results
- Complete, with Minimal Overlap

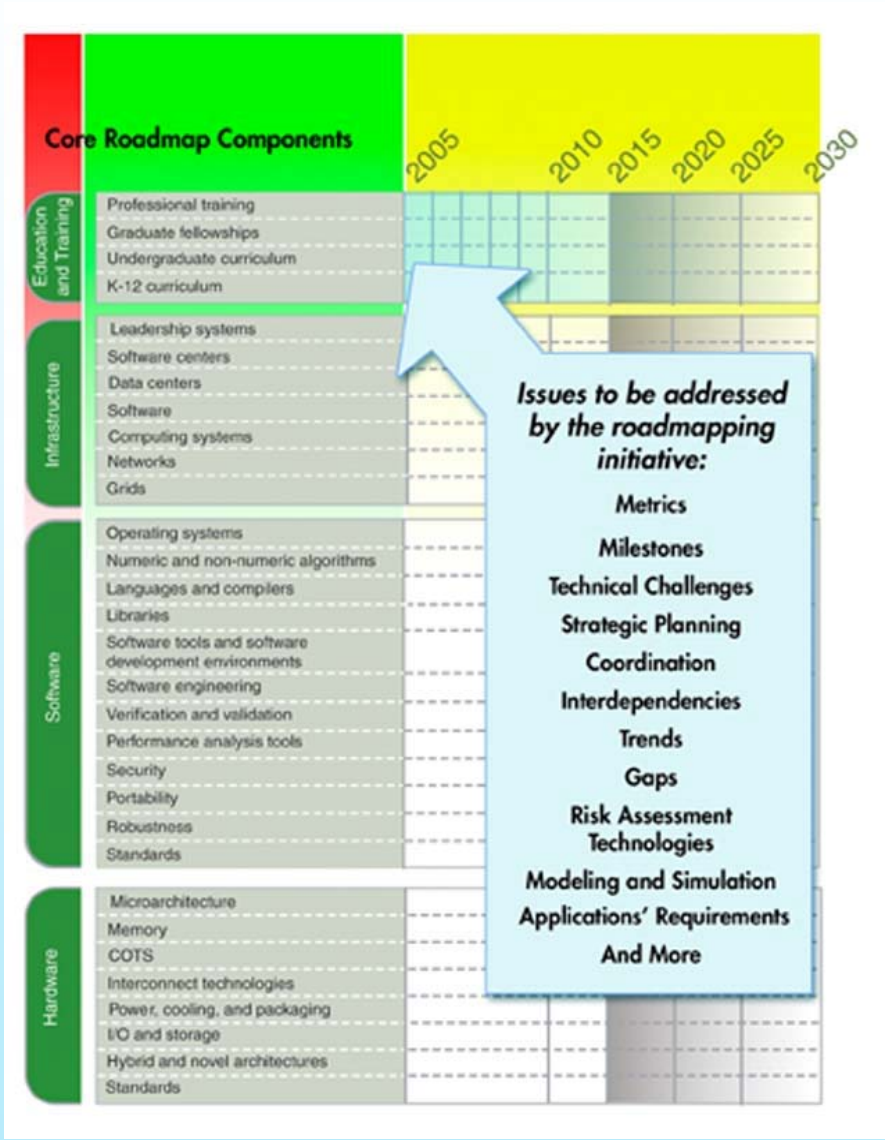
Roadmaps Are Being Developed for Other NITRD Areas

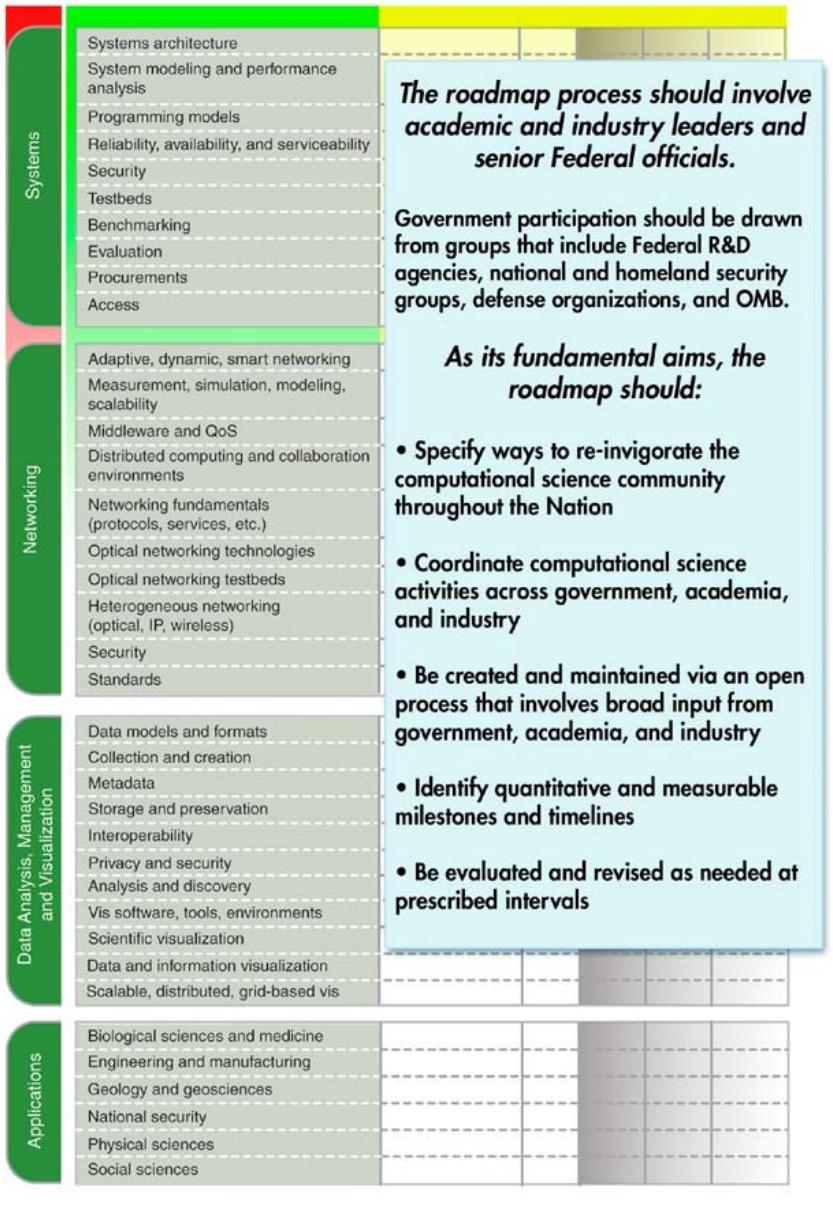
- **Cyber Security and Information Assurance**
- **High Confidence Software and Systems**
  - Medical devices
  - Aviation safety
  - Assured Real-Time Operating Systems
- **High End Computing**
- **Human-Computer Interaction and Information Management**
  - Information Integration R&D
- **Large Scale Networking**

Roadmap Examples

- **Computational Science: Ensuring America's Competitiveness**
  - 2005 report of the President's Information Technology Advisory Committee
  - http://www.nitrd.gov/pitac/reports/20050609_computational/computational.pdf
- **ASCI Technology Prospectus: Simulation and Computational Science**
  - 2001 publication of the ASCI Program, National Nuclear Security Administration, Department of Energy, Defense Programs
  - http://www.sandia.gov/NNSA/ASC/pdfs/prospectus.pdf
    - ASCI = Accelerated Strategic Computing Initiative (now the Advanced Simulation & Computing [ASC] Program)

Computational Science Roadmap: A Schematic View





Road Map for GRID SERVICES CAPABILITIES

Functional Area	CY 2000	CY 2001	CY 2002	CY 2003	CY 2004	CY 2005
Grid Accessibility	Kerberos-secured grid access services	Grid administration Resource coordination via dependencies	Kerberos-secured web access	Grid-aware programming components Personalization of grid environment		Grid scheduling
Core Grid Services		Grid monitoring service	Grid instrumentation	Limited delegation of credentials		
Grid Resource Interface		Grid interface for 10 teraOPS ASCI platform Grid interface for HPSS	Grid interface for 30 teraOPS ASCI platform		Grid interface for 100 teraOPS ASCI platform	
Local Resource Manager		Gang scheduler for 10 teraOPS ASCI platform			On-demand scheduling	

R&D Effort Indicator — ACCOMPLISHED — PLANNED — HURDLE — BARRIER

ACCOMPLISHED—Completed
PLANNED—ASCI will accomplish even with slight budget fluctuations
HURDLE—ASCI will need some help from the HPC community
BARRIER—ASCI will need significant help from the HPC community

Hard Problem Example (1): 2005 Infosec Research Council (IRC) Hard Problem List Topics

1. GLOBAL-SCALE IDENTITY MANAGEMENT
2. INSIDER THREAT
3. AVAILABILITY OF TIME-CRITICAL SYSTEMS
4. BUILDING SCALABLE SECURE SYSTEMS
5. ATTACK ATTRIBUTION AND SITUATIONAL UNDERSTANDING
6. INFORMATION PROVENANCE
7. SECURITY WITH PRIVACY
8. ENTERPRISE-LEVEL SECURITY METRICS

This material was presented by Doug Maughan, DHS, at 1/26/06 meeting of the NITRD Program's Cyber Security and Information Assurance Interagency Working Group http://www.infosec-research.org/documents.html

IRC Hard Problem Example: 3. Availability of Time-Critical Systems

- **Motivation: SCADA, military, homeland security first responders often**
  - Value availability over secrecy
  - Work in lossy, ad hoc wireless environments
- **Challenges: limited resources**
  - Computational processing power
  - Service quality guarantees given dynamics
  - Distributed systems compound problem
- **Metric: Range of circumstances over which results can be guaranteed**

IRC Hard Problem List Summary

- “Stake in the ground” from the front line
- Topics selected because of their importance to Government missions and the lack of solutions
- Not the only challenges in the IT security space
- Information security is not only about technology

Hard Problem Example (2): NITRD Program Hard Problem Areas

- **ITHP Areas are broad categories of topics of interest to the IT R&D community and reflect the breadth of the NITRD Program**
- **Advances in the ITHP Areas must be achieved in order to solve Grand Challenges (GC)**
  - NITRD GC is defined as a long-term science, engineering, or societal advance, whose realization requires innovative breakthroughs in Information Technology Research and Development (IT R&D), and which will help address our country's national priorities (NPs)
- **14 ITHP Areas were identified**
- **These ITHP Areas spanned the NITRD Program's current investments at the time of publication (2004)**

- **http://www.nitrd.gov/pubs/200311_grand_challenges.pdf**

Relationships Between the Illustrative GCs and the NPs

ILLUSTRATIVE GRAND CHALLENGES	NATIONAL PRIORITIES: Leadership in Science and Technology	National and Homeland Security	Health and Environment	Economic Prosperity	A Well-Educated Populace	A Vibrant Civil Society
Knowledge Environments for Science and Engineering	■	■	■		■	■
Clean Energy Production Through Improved Combustion	■	■	■	■		
High Confidence Infrastructure Control Systems		■		■		■
Improved Patient Safety and Health Quality			■	■		
Informed Strategic Planning for Long-Term Regional Climate Change	■		■	■	■	
Nanoscale Science and Technology: Explore and Exploit the Behavior of Ensembles of Atoms and Molecules	■	■	■	■		
Predicting Pathways and Health Effects of Pollutants	■	■	■	■		
Real-Time Detection, Assessment, and Response to Natural or Man-Made Threats		■	■	■		
Safer, More Secure, More Efficient, Higher-Capacity Multi-Modal Transportation System			■	■		
Anticipate Consequences of Universal Participation in a Digital Society	■	■	■	■	■	■
Collaborative Intelligence: Integrating Humans with Intelligent Technologies	■	■	■	■	■	■
Generating Insights From Information at Your Fingertips	■	■	■	■		
Managing Knowledge-Intensive Organizations in Dynamic Environments		■	■	■		
Rapidly Acquiring Proficiency in Natural Languages	■	■			■	■
SimUniverse: Learning by Exploring	■		■	■	■	
Virtual Lifetime Tutor for All				■	■	■

Relationships Between the Illustrative GCs and the ITHP Areas

ILLUSTRATIVE GRAND CHALLENGES	IT HARD PROBLEM AREAS: Algorithms and Applications	Complex Heterogeneous Systems	Hardware Technologies	High Confidence IT	High-End Computing Systems	Human Augmentation IT	Information Management	Intelligent Systems	IT System Design	IT Usability	IT Workforce	Management of IT	Networks	Software Technologies
Knowledge Environments for Science and Engineering	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Clean Energy Production Through Improved Combustion	■				■		■					■		
High Confidence Infrastructure Control Systems		■		■									■	
Improved Patient Safety and Health Quality	■			■		■	■	■	■	■		■	■	■
Informed Strategic Planning for Long-Term Regional Climate Change	■		■	■	■	■	■	■	■	■	■	■	■	■
Nanoscale Science and Technology: Explore and Exploit the Behavior of Ensembles of Atoms and Molecules	■		■		■	■			■				■	
Predicting Pathways and Health Effects of Pollutants	■	■		■	■	■	■	■		■	■		■	■
Real-Time Detection, Assessment, and Response to Natural or Man-Made Threats	■	■			■	■	■	■					■	
Safer, More Secure, More Efficient, Higher-Capacity Multi-Modal Transportation System	■	■		■			■	■	■	■		■	■	■
Anticipate Consequences of Universal Participation in a Digital Society	■	■		■	■	■	■	■	■	■	■	■	■	■
Collaborative Intelligence: Intergrating Humans with Intelligent Technologies	■	■		■		■	■	■	■	■	■	■	■	■
Generating Insights From Information at Your Fingertips		■		■			■	■		■			■	
Managing Knowledge-Intensive Organizations in Dynamic Environments	■	■		■	■	■	■	■	■	■	■	■	■	■
Rapidly Acquiring Proficiency in Natural Languages	■	■				■	■	■		■				
SimUniverse: Learning by Exploring	■					■			■	■				■
Virtual Lifetime Tutor for All	■					■	■	■	■	■				

Example NITRD Grand Challenge: High Confidence Infrastructure Control Systems

- **Description of the Multi-Decade Grand Challenge**
  - Ensure the continuous, safe operation of the Nation's infrastructure systems (e.g., power grid, water supply, transportation system), and protect against malicious attacks and physical and complex cascading failures
- **Focus for the Next Ten Years**
  - Supervisory Control and Data Acquisition (SCADA) systems, transformation from legacy systems to IT-enabled infrastructures, and coordinated decentralized control of new forms of distributed infrastructure (e.g., air traffic control, transportation scheduling)
- **Benefits**
  - Robust, survivable, attack and failure proof infrastructures, higher capacity systems, and the reduction of failures
- **Relationship to National Priorities**
  - National Security, Homeland Security, Economic Prosperity, and a Vibrant Civil Society
- **IT Hard Problem Areas** (see next slide)
- **Indications of Progress**
  - Reduction in mean time to recovery (MTTR), and fewer and smaller scale failures

IT Hard Problem Areas for High Confidence Infrastructure Control Systems

- **Complex Heterogeneous Systems**
  - Understand, control, and successfully react to simultaneous conflicting interactions (e.g., fault tolerance, time-sensitive recovery, maintenance of security while recovering), and to emerging, hard-to-predict behavior in SCADA systems
- **High Confidence IT**
  - Integrate security (e.g., authentication, access control, intrusion detection) into networked embedded systems, and continue operating through attacks without shutting down
- **Networks**
  - Secure and survivable networks