High Confidence Software and Systems (HCSS)

NITRD Agencies: NSF, OSD and DoD Service research organizations, NIH, NSA, NASA, NIST
Other Participants: DOE (OE), FAA, FDA

HCSS R&D supports development of scientific foundations and innovative and enabling software and hardware technologies for the design, control, assurance, verification and validation, and certification of complex, networked, distributed computing systems and cyber-physical (IT-enabled) systems. To be capable of providing advanced services, these systems, including their software, must be reliable, predictable, adaptable, robust, safe, scalable, secure, stable, and in many cases certifiably dependable. The goal is to provide a sound and practical technology base for deeply and fully integrating embedded computation and physical dynamics, communication, networking, and control in a unified, coordinated, and continuous manner to routinely build high-confidence, optimally performing computing systems that interact properly with humans and the physical world in changing environments and unforeseen conditions. These systems, often components of larger physical and IT systems, are essential for effectively operating life-, safety-, security-, and mission-critical applications. These include defense and intelligence systems that are vital to U.S. military success and leadership, large-scale enterprise applications that can accelerate and enhance U.S. industrial competitiveness, global-scale critical infrastructures that provide foundational services for economic security, and human-utility devices that can improve citizens' quality of life.

President's FY 2009 Request

Strategic Priorities Underlying This Request
To build these fundamentally new classes of sensing, communication, and control technologies that uniformly integrate physical dynamics and computation in complex distributed systems, research is required in:

New scientific foundations for building high-confidence cyber-physical systems (CPS): New computational concepts, methods, and tools including new architectural principles, frameworks, dynamic models, and protocols for platforms and software systems and for engineered systems that currently are beyond human capability to construct reliably and predictably. These systems will have cyber capability deeply integrated in physical components; will be networked at every scale; are complex at multiple temporal and spatial scales; will dynamically reorganize and reconfigure; and will be highly automated and even autonomic. These systems will require understanding and reconciliation of the fundamental interactions between the cyber and physical worlds.

High-confidence, real-time, critical core technologies: Composable, configurable, real-time certifiable embedded systems technology substrates to reduce dependence on an aging and increasingly obsolete technology base; reconfigurable, reliable, predictable, and secure physical and engineered systems whose operations are integrated, monitored, and controlled by a computational core that is usually real-time, networked, embedded, composable, and distributed. These next-generation systems are poised to render obsolete today's systems software architectures (e.g., monolithic real-time operating systems [RTOS] designed for single-system applications; middleware as ad hoc extensions to enable, support, or effect networked systems; and virtual machines with RTOS as a general-purpose fixed architecture).

Next generation of assured, high-confidence critical CPS infrastructures: Critical cyber-physical systems that must be built on a solid basis of science and engineering include: *aviation and air space management* (adaptive avionics, air-traffic control systems, control of aircraft, and unmanned aerial vehicles); *transportation networks* (intelligent automotive and highway systems): *medical device and electronic health management systems* (dynamically configured, integrated intensive care or emergency transport units; secure nationwide health records system; hospital information systems; home care; assisted living); *intelligent industrial, manufacturing, and building/home environments (automated production, heating, lighting, and air conditioning generation, distribution, monitoring, and usage made operational via supervisory control and data acquisition [SCADA] and other networked control systems); first-responder systems* (reliable systems for emergency responders); *national and homeland defense systems* (counterterrorism, missile defense, war fighter protection, reconnaissance, and counterintelligence)

Highlights of Request

Cyber-enabled Discovery and Innovation (CDI): Expanded focus to include software for tomorrow's complex systems, including cyber-physical systems; address challenges of large-scale interacting systems, investigate their non-linear interactions and aggregate or emergent phenomena to better predict capabilities for design, control, and decision-making about complex systems – NSF

Cyber-physical systems: Continuing effort to develop a next-generation real-time technology base for architectures and virtualization of CPS, including complex embedded, hybrid, autonomous, and adaptive

systems, parallel and distributed operating systems; high-confidence system service composition – NSF, AFRL, ARO, NSA, NASA, NIST, FAA, FDA

High-confidence systems and foundations of assured computing: Methods and tools for modeling, measuring, analyzing, evaluating, and predicting performance, correctness, efficiency, reliability, dependability, scalability and usability of complex, real-time, distributed, and mobile systems; high-confidence platforms for sensing and control; virtualization, architectures, components, composition, and configuration; systems of systems governance, engineering, analysis and testing of software and hardware; programming language semantics and computational models; design, development, verification, and validation for reliable computing – NSF, OSD, AFRL, ARO, NSA, NASA, NIST, FDA

Information assurance requirements: Methods and tools for constructing, analyzing security structures such as management architectures and protocols; assurance technologies for cross-domain sharing of sensitive information; assured compilation of cryptographic designs and specifications to platforms of interest – NSA; cross-enterprise document sharing in electronic health systems, conformance measurements for health information networks – NIST

Flight Critical System Software Initiative (FCSSI): New applied research start (Mixed Critical Architecture Development, a follow-on to development of certification requirements for embedded systems design); add formal methods for V&V to certification focus on infinite state systems – AFRL, NSF with other DoD Service research organizations, NASA, NSA

Standards and test methods for industrial control systems (ICS) and networks: Approaches to balancing safety, security, reliability, and performance in SCADA and other ICS used in manufacturing; ensuring performance and interoperability of factory floor network communication devices and systems – NIST

Verification Grand Challenge: R&D to develop deployable assurance technologies; annual conference on verified software and roadmap – NSA, NSF

Planning and Coordination Supporting Request

National Workshop Series: Academic, industry, and government stakeholder workshops to identify new R&D needed and develop roadmaps for building next-generation, real-time, high-confidence CPS technologies for life-, safety-, and mission-critical applications; topics have included:

- **Verified Software, Theories, Tools, and Experiments (VSTTE) Planning Workshop** – NSA
- **Stimulating and Sustaining Excitement and Discovery in K-12 STEM Education** – NSA, NSF
- **National Workshop on New Directions in Composition and Systems Technology for High-Confidence Software Platforms for Cyber-Physical Systems** – NSF, NSA, NASA, NIST, FDA
- **Joint Workshop on High-Confidence Medical Devices, Software, and Systems & Medical Device Plug-and-Play Interoperability** – NSF, AHRQ, ARO with NIH, FDA

National Academies Symposium released the study, *Software for Dependable Systems: Sufficient Evidence?* – NSA, NSF with ARO, ONR, NASA, NIST, FAA, FDA

Eighth Annual HCSS Conference: Showcasing of promising research to improve system confidence – NSA with NSF, ONR, NASA, FAA

Hybrid Systems Workshop – NSA, NSF

Static Analysis Methods/Tools Summit: Annual summit on software security for vendors, users, academics – NIST, NSA, NSF

Software Assurance Metrics and Tool Evaluation: Annual workshop series for users and developers to compare efficacy of techniques and tools, develop taxonomies of vulnerabilities and tools – NIST, NSA

Mixed Criticality Architecture Requirements (MCAR) Planning Review Workshop – Phase II of systems requirements for design for certification – AFRL, NSF with other DoD Service research organizations, NSA, NASA

Joint Laboratory for the Assessment of Medical Imaging Systems – NIH, FDA

Biomedical imagery: Development of technical standards for change measurements in patient therapeutic applications – NIH, NIST, FDA, CMS

Standards and software assurance metrics for SCADA and ICS: Collaborative development activity – NIST, DOE/OE; ICS procurement language specification project – NIST, DOE/OE

Scholar-in-Residence Program – Ongoing interagency partnership for the investigation of emerging scientific and engineering trends in medical device technologies – NSF, FDA

Cooperative proposal evaluation – NSF, AFRL, NSA, NASA, NIST

Additional 2008 and 2009 Activities by Agency

NSF: Joint exploratory research (CISE and ENG directorates) towards CPS; ongoing core research in computing processes and artifacts; ongoing core computer systems research (CSR)

OSD: Technologies for assuring that software is free from vulnerabilities

AFRL: R&D in technologies, design methods, and tools for safety and security certification of onboard aircraft embedded systems operating in a system-of-systems environment (e.g., unmanned aerial vehicles); emphasis on "mixed criticality" (air safety combined with security) interdependencies requiring deep

interaction, integration of hardware and software components; Flight Critical System Software Initiative Symposium

AFOSR: Integrated specification and verification environment for component-based architectures of large-scale distribution systems; a framework for modeling and analyzing this system

ARO: Software/system prototyping, development, documentation, and evolution; virtual parts engineering research; reliable and secure networked embedded systems; reliable and effective mechanisms to monitor and verify software execution status

NIH: Assurance in medical devices such as pulse oximeters, cardio-exploratory monitors for neonates; telemedicine; computer-aided detection and diagnosis; computer-aided surgery and treatment (such as radiation); neural interface technologies such as cochlear implants, brain-computer interfaces

NSA: Assured cryptographic implementations (software and hardware); protocol analysis and verification; domain-specific workbench developments (interpreters, compilers, verifiers, and validators); assured content management and collaboration services; assured implementation and execution of critical platform components and functionality

NASA: Aeronautics research in integrated vehicle health management, integrated intelligent flight deck, and integrated resilient aircraft control; enabling V&V technologies for NextGen Airspace System (separation assurance and super-density programs); exploration systems research in reliable software technologies (automated testing, auto-coding, formal V&V, compositional verification)

NIST: Computer forensics tool testing, National Software Reference Library (funded by DOJ/NIJ); software assurance metrics, tools, and evaluation, National Vulnerability Database, Software Assurance Forum; trustworthy software (foundations, metrology, guidance and specifications for development); mathematical foundations of measurement science for information systems; ongoing standards and test methods for industrial control systems and networks; test methods for Voluntary Voting System Guidelines

DOE/OE: Next Generation Control Systems (scaleable, cost-effective methods for secure communication between remote devices and control centers; cost-effective security solutions for new architecture designs and communication methods; risk analysis; National SCADA Test Bed; secure SCADA communications protocol; middleware for inter-utility communications and cyber security; virtual architecture modeling tools

FDA: Formal methods-based design (assured verification, device software and system safety modeling and certification, forensics analysis, engineering tool foundations); architecture platform, middleware, resource management (plug-and-play, vigilance and trending systems); component-based design frameworks; patient modeling and simulation; adaptive patient-specific algorithm; requirements and metrics for certifiable assurance and safety