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 technologies for innovative systems design, systems and embedded application software, and assurance and verification to enable the routine production of reliable, robust, safe, scalable, secure, stable, and certifiably dependable IT-centric physical and engineered systems comprising new classes of advanced services and applications. These systems, often embedded in larger physical and IT systems, are essential for the operation of the country's critical societal infrastructures, acceleration of U.S. capability in industrial competitiveness, and optimization of citizens' quality of life.

President's FY 2008 Request

Strategic Priorities Underlying This Request
New classes of computationally integrated sensing, communications, and control technologies that are adaptive, distributed, networked, embedded, and real-time are needed to maximize progress towards engineering and deploying high-confidence, high-performance, and efficiently produced IT-centric systems on a large scale for life-, safety-, and mission-critical applications. Research is required to develop:

New scientific foundations for building high-confidence technologies: Innovative theories, methods, and tools including new architectural principles and frameworks – currently not well understood – are necessary to enable systems that are built from the ground up with systematic specialization, integration, and assurance. Such new approaches are needed to replace today's concepts, which have yielded increasingly inefficient, unsound, failure-prone, and frequently dangerous design results. Technical areas include design and engineering methods, distributed sensing and control, measures/metrics to evaluate confidence and assurance

High-confidence, real-time technologies: Composable, configurable real-time embedded systems technology substrate to reduce dependence on an aging and increasingly obsolete technology base (i.e., real-time operating systems [RTOS] designed for single-system applications; middleware [MW] applied atop RTOS for operation of networked systems; virtual machines [VMs] applied atop RTOS as a general purpose fixed architecture)

Next-generation critical societal infrastructures: IT-centric systems based on scientific assurance foundations. Illustrative critical applications for these "systems of systems" or "infrastructures of infrastructures" include: *aviation and air space management* (adaptive avionics, air-traffic control systems); *transportation networks* (intelligent automotive and highway systems that reduce traffic accidents, congestion, air pollution, gas usage); *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); *beyond supervisory control and data acquisition (SCADA)* (intelligent industrial and home environments with more efficient and real-time water, heating, lighting, and air conditioning generation, distribution, monitoring, and usage); *first responder systems* (reliable systems for emergency responders); *defense systems* (real-time, distributed, embedded systems in a network-centric environment for counterterrorism, missile defense, warfighter protection, reconnaissance, and counterintelligence)

Highlights of Request

Cyber-enabled Discovery and Innovation (CDI): New focus area to address the challenges of large-scale interacting systems, understand their non-linearity of interactions, and their aggregate or emergent phenomena to better predict and deduct capabilities for design, control and decision-making about complex systems – NSF

Cyber-physical systems (CPS): New R&D effort to develop a next-generation real-time technology base for architectures and virtualization (restructuring of OS/MW/VM); high-confidence system service composition; complex cyber-physical systems – NSF, OSD, AFRL, NSA, NASA, NIST, FAA, FDA

High-confidence RTOS: Research to develop next-generation high-confidence RTOS technology base – NSF, OSD, AFRL, ONR, NSA, NASA, with DOE, NIST, FAA, FDA

High-confidence systems and foundations of assured computing: Methods and tools for modeling, measuring, analyzing, evaluating, and predicting performance, correctness, efficiency, and dependability of complex systems; real-time systems; distributed and mobile systems; high confidence platforms for sensing and control; virtualization, architectures, components, composition, and configuration; analysis and testing of software and

hardware; verification and synthesis; programming language semantics and computational models; design and implementation for reliable computing – NSF, OSD, AFRL, NSA, NASA, NIST, FDA

Information assurance requirements: Intelligent, secure, flexible, self-protecting global infrastructure; safe computing platforms that can isolate, measure, and attest to correct operations – NSA

Flight-Critical Systems Software Initiative (FCSSI): New start on mixed criticality architecture requirements for embedded systems platform and integrated tool chain – AFRL, NSF, with NASA, FAA

Illustrative domain research areas for high-confidence, real-time technologies: Medical device, aviation, and critical infrastructures (e.g., power) that operate via SCADA systems – HCSS agencies

Planning and Coordination Supporting Request

Annual National Workshop Series: One cross-cutting and three domain-specific workshops comprising academia, industry, and government stakeholders to identify new R&D and develop roadmaps to build next-generation, real-time high-confidence technologies for life-, safety-, and mission-critical applications including:

- **High-Confidence Software Platforms for Cyber-Physical Systems:** Comprehensive restructuring of current software and control systems platform designs of complex, IT-centric systems to achieve a more sound and assured technology base that is correct by construction – HCSS agencies
- **High-Confidence Critical Infrastructures: Beyond SCADA - Networked Embedded Control Systems:** High-confidence device and software technologies for next-generation critical infrastructures that depend on SCADA systems for their operation – NSF, AFRL, NIST, NSA, OSD
- **Aviation Software Systems for the Second Century of Flight - Design for Certifiably Dependable Systems:** Next-generation high-confidence aviation systems V&V and specifications, design, certification, and testing for aviation software systems – NSF, AFRL, FAA, NASA, NSA
- **High-Confidence Medical Device Software and Systems:** Next-generation high-confidence medical devices and systems technologies – NSF, FDA, NIST, NSA

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

Seventh Annual HCSS Conference: Showcasing promising research to improve system confidence – NSA, NSF

Static Analysis Methods/Tools Summit: Software security, for vendors, users, academics – NIST, NSA, NSF

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

High-confidence RTOS technology needs assessments: Series of non-disclosure briefings by technology development and systems integration vendors – All HCSS agencies and other agencies

Advancing Software Producibility: NA study and workshop series – OSD, NSF

Sufficient Evidence? Building Certifiably Dependable Systems: National Academies study – NSA, NSF, ONR, with ARO, DARPA, FAA, FDA, NASA, NIST

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

Additional 2007 and 2008 Activities by Agency

NSF: Formal methods (composition, verification); rigorous computation models; compositional software methods

OSD (DDR&E): Software Engineering Institute – quality attribute reasoning; principles, methods, techniques for integration and interoperation and assurance across software components, systems, systems of systems; model-based software engineering for real-time systems; methods for evidence-based assurance

AFRL: Methods, techniques, and tools to enable development of flight-critical systems

NASA: Aeronautics research – enabling V&V technologies for NGATS; integrated vehicle health management, integrated intelligent flight deck, and integrated resilient aircraft control; Exploration – terminate (end of FY 2007) R&D in reliable software technologies

NIST: Security, integrity, usability, and accessibility of voting systems; software diagnostic and conformance testing including cross-enterprise document sharing; computer forensics tool testing; software assurance metrics, tools, and evaluation; vulnerability databases

FAA: Certifiably dependable systems, including incremental certification in traditional safety-critical systems; improved continuous external monitoring of a system's internal vital signs

FDA: Formal methods-based design and assured verification (medical device software/system certification; safety/security/regulatory policy models; forensics analysis, engineering tool foundations); assured platform, middleware, resource management ("black box" data recording, plug-n-play); cyber-physical systems