Winning the Future with
Science and Technology for 21st Century Smart Systems

America, the singular leader in the Industrial Age, made groundbreaking advances in transportation, mining, manufacturing, food processing, and agriculture. The result was a thriving economy that sustained the American Dream for more than a century. A second revolution, based on technology for computing and networks, revolutionized the white-collar workplace and yielded an Information Economy that has propelled global economic growth over the past three decades.

Now these two forces are converging. Inexorably, future advances in the capability of engineered systems will derive in major part from flexibility purchased by embedding "cyber" components -- components that can compute, communicate, and control -- into the physical world. The U.S. transportation system, medical technology, energy systems, and manufacturing capacity all depend on this fusion of cyber and physical engineering. At the same time, global competition in cyber-enabled systems is escalating exponentially. If the US is to continue to lead as an economic power, long-term R&D and education investments are needed. This is essential to guarantee a future in which a productive, educated, and innovative workforce and a robust industrial base can compete successfully in the global milieu. A "leap-ahead" national effort is required to assure US competitiveness for the 21st century.

What is the Problem?

Cyber-physical systems—smart systems that have cyber technologies, both hardware and software, deeply embedded in and interacting with physical components, sensing and changing the state of the real world—represent a core opportunity area and source of competitive advantage for the U.S. innovation economy in the 21st century. Examples of cyber-physical systems (CPS)-based initiatives include smart transportation systems, smart medical devices and technologies, smart buildings, next-generation air transportation systems, and the Smart Grid. The President's Council of Advisors on Science and Technology (PCAST) in a 2007 report[1] found that cyber-physical systems "are now a national priority for Federal R&D. Improved methods are needed for the efficient development of these systems. These methods must assure high levels of reliability, safety, security, and usability." This is because cyber-physical systems have stringent requirements above and beyond—and different from—those in home and office automation systems. CPS must support real-time behavior, with ultra-high reliability: "While the occasional "Blue Screen" may be only an annoyance in the office environment, it can have extreme consequences in the air."[2]

The PCAST recommended that Federal R&D agencies should "strengthen existing programs or create new ones that cross disciplinary boundaries to accelerate work in this area. The agencies should also place greater priority on devising mechanisms that enable industry and universities to collaborate on pre-competitive research in these systems." The December 2010 PCAST report reinforces and expands the emphasis on networking and IT systems integrated with and acting upon the physical world, particularly as applied to energy, transportation, health care, and homeland security.[3] The report

> *"We know what it takes to compete for the jobs and industries of our time. We need to out-innovate, out-educate, and out-build the rest of the world."*
>
> - President Barack Obama

[1] *Leadership Under Challenge: Information Technology R&D in a Competitive World*, PCAST report, August 2007 http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-07-nitrd-review.pdf

[2] Statement of Mr. Don C. Winter, Vice President, Engineering & Information Technology, Boeing Phantom Works, Before a hearing on: Networking and Information Technology Research and Development (NITRD) Program, Committee on Science and Technology, U.S. House of Representatives, July 31, 2008, http://lazowska.cs.washington.edu/initiatives/Winter.pdf

[3] *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*, PCAST Report, December 2010 http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf

recommends that the Federal Government invest in a national, long-term, multi-agency, multi-faceted research initiative in these areas. The Office of Science and Technology Policy (OSTP) and Office of Management and Budget (OMB) have also called for focused support of R&D in advanced manufacturing to "strengthen U.S. leadership in the areas of robotics, cyber-physical systems, and flexible manufacturing" as a means to promote sustainable economic growth and job creation."[4]

These recommendations arise from recognition of 1) the growing importance of CPS to the economic future of the country, national and homeland security, and the mission success of federal agencies, and 2) the increasing technical challenges resulting from rapidly growing demand for new capabilities and applications such as the Smart Grid, the Next Generation Air Transportation System, Intelligent [surface] Transportation Systems, Smart Medical Technologies, Smart Buildings, and Smart Manufacturing.

The ability to effectively engineer high-confidence cyber-physical systems is critical to success in government Smart Technology initiatives and private sector next generation products and systems that will *win the future*. A broad consensus has emerged, both among federal agencies and in the private sector, that current approaches to engineering these systems are too costly, too error prone, and take too long. According to the PCAST report:

> Such systems can be difficult and costly to design, build, test, and maintain. They often involve the intricate integration of myriad networked software and hardware components, including multiple subsystems. In monitoring and controlling the functioning of complex, fast-acting physical systems (such as medical devices, weapons systems, manufacturing processes, and power-distribution facilities), they must operate reliably in real time under strict constraints on computing, memory, power, speed, weight, and cost. Moreover, most uses of cyber-physical systems are safety-critical: they must continue to function even when under attack or stress.

Amplifying this last point, it is also exceedingly difficult to produce an evidence-based case to serve as the basis for approving or disapproving use of these systems for life-, health-, or safety-critical applications.

We are starting to be able to envision the day when robotic assist technologies extend independent living for seniors, when health care follow-ups can be done at home and clothing and devices worn or embedded in the home can report adverse health events, when your car will be able to drive you safely and securely to your destination, when your home and car both consume energy from—and provide energy to—the electricity grid, and when real-life bionics integrate seamlessly with human physiological systems to replace lost functionality. But what will give us confidence that these future automation technologies will predictably perform as desired in a wide variety of situations and environments? Who will have the multidisciplinary skills to build these systems?

The risk to U.S. innovative capacity and industrial competitiveness of not addressing these questions is a problem of National proportions, one with consequences that will extend far into America's future. Key challenges cut across industrial sectors and mission agencies; companies and agencies cannot individually overcome the crosscutting CPS R&D challenges that need to be solved. Isolated efforts by mission agencies are simply not sufficient to address the underlying issues in a holistic manner. Trying to address them agency-by-agency or sector-by-sector would result in inefficiencies and insufficient progress relative to system development timetables, and we might never get to where we need to be. The introduction and increasingly critical role of computational, communications, and software

[4] OMB-OSTP Science and Technology Priorities memo, July 21, 2010
http://www.whitehouse.gov/sites/default/files/microsites/ostp/fy12-budget-guidance-memo.pdf

elements in regulated cyber-physical products and mission-critical systems is outstripping national and agency capabilities to specify, review, build, integrate, test, approve, procure, operate, investigate, and upgrade and maintain these systems. Performance measures and standards to support these activities are also lacking.

An Evolving Cyber-Physical Systems Landscape

Cyber-physical systems are becoming ubiquitous, pervading every sector of the critical national infrastructure and every aspect of an individual's daily life, including the following examples:

	Current	Future
Medical care and health	Pacemakers, infusion pumps, medical delivery devices, connected to the patient for life-critical functions	Life-supporting micro-devices, embedded in the human body; wireless connectivity enabling body area sensor nets; mass customization of heterogeneous, configurable personalized medical devices, and natural, wearable sensors (clothing, jewelry) and benignly implantable devices
Energy	Centralized generation, Supervisory Control and Data Acquisition Systems for transmission and distribution	Systems for more efficient, effective, safe and secure generation, transmission, and distribution of electric power, integrated through the smart grid; smart ("net-zero energy") buildings for energy savings; systems to keep nuclear reactors safe
Transportation and Mobility	Vehicle-based safety systems, ABS, traction and stability control, powertrain management; precision GPS-enabled agriculture;	Vehicle-to-vehicle communications for enhanced safety and convenience ("zero fatality" highways), drive-by-wire, autonomous vehicles; next generation air transportation system (NextGen); autonomous vehicles for off-road and military mobility applications
Manufacturing	Computer controlled machine tools and equipment; robots performing repetitive tasks, fenced off from people	Smarter, more connected processes for agile and efficient production; manufacturing robotics that work safely with people in shared spaces; computer-guided printing or casting of composites
Materials and other sectors	Relatively few, highly specialized applications of smart materials – predominantly passive materials and structures	Sustainable mass production of "smart" fabrics and other "wearables" with applications in many areas; Actively controlled buildings and structures to improve safety by avoiding or mitigating accidents; electronics provide versatility without recourse to a silicon foundry; emerging materials such as carbon fiber and polymers offer the potential to combine capability for electrical and/or optical (hence NIT) functionality with important physical properties (strength, durability, disposability)

Where we are now

Critical functions, applications, and assets are becoming so CPS-dependent that, often, there are no effective fallback alternatives. CPS are "systems-of-systems" whose interactions are exponentially complex. For example, electricity production, transmission, distribution, and consumption in the U.S. is a single large-scale integrated system, rapidly growing in size, complexity, and vulnerability. It is necessary to ask, who is going to build our future systems? The requisite skills for building CPS are cross-disciplinary, but today's educational pipeline does not yield an adequately prepared workforce.

With increasing complexity, safety issues become increasingly difficult to recognize, understand, and analyze. Testing will not get us to correctness. Safety-critical CPS are typically too complex to be completely verified and validated. Remaining uncertainties are significant, but not well understood. A single defect can make logic wrong, potentially leading to serious consequences, but the capability to engineer defect-free systems does not exist. Networking (wired or wireless) introduces new vulnerabilities that are not well understood, such as hidden dependencies and couplings. Latent defects can combine in many scenarios, with potential to cause high consequence failure. The more complex a system is the more is the exposure to defects. Verification of a high-integrity system or component, e.g. operating system, takes more effort and time than its initial development. To take an example from the aviation sector, "in the 70's and 80's aerodynamics and structures accounted for nearly 90 percent of the development cost of a transport aircraft, with cyber-physical system development accounting for less than 10 percent. The trend has reversed, and cyber-physical system design, development, validation and certification account for nearly half of development costs for current generation system, and for next generation systems this percentage is expected to rise to 50% or more."[5] Similarly, the following experience reported from the automotive sector exemplifies an issue common to all sectors. USCAR has indicated that "the most difficult issues lie not in the design of the software in individual modules, but in the interactions between different modules and components – i.e., integration of embedded systems composed of heterogeneous components designed and implemented by different suppliers."[6]

As a result, safety assurance becomes increasingly dependent upon expert judgment. Safety analysis and evaluation require high competence and judgment, but these capabilities are very scarce. In particular, hazard analysis requires extremely high (but scarce) competence in many disciplines, and is challenging because system failure modes may not be well understood or fully communicated.

CPS systems must be protected from cyberattack. Because of their central role in critical infrastructures and safety-critical applications, CPS may represent attractive targets for adversaries. For example, in 2010 Stuxnet malware was found, specifically designed to exploit Supervisory Control and Data Acquisition (SCADA) systems in the energy sector. Because of the strict performance and safety requirements of many CPS, security measures must be designed in as an integral part of the system, and security products and approaches developed for office automation applications may not be directly applicable. Still, there are strong points of leverage with the broader National strategy and portfolio of cybersecurity R&D.

The question, "What is adequate?" arises in every safety-critical CPS. Examples of the difficulties can be seen in failures of medical devices, automobile recalls, and delays in delivery of new aircraft. Comparing

[5] Statement of Mr. Don C. Winter, ibid.
[6] Statement of Mr. Don C. Winter, ibid.

experiences from various sectors of the economy,[7] it is clear that similar problems exist in most safety-critical, mission-critical application domains, but to date there has been little synergy toward developing a common core set of underlying solution capabilities. Fragmented efforts limit progress. We lack the tools and science to understand and mitigate the effects that are showing up more and more often in huge development, schedule, and cost overruns, as well as unpredictable operational behaviors. Better means are needed to:

- Transform abstract goals, objectives, and requirements into unambiguous specifications,
- Transform specifications through design into implementations in a way that satisfaction of the original requirements is inherently assured, and
- Assess and verify the applicability of commercially available tools, developed for non-critical consumer applications, to safety-critical system development.

Overcoming this barrier to understanding will open the way to a whole new era of opportunities.

What is the vision?

The U.S. has an opportunity to gain competitive leadership through the ability to develop new cyber-physical systems with built-in assurance of their critical properties, e.g. safety and security, and correct, timely performance of their intended functions. Such capability does not exist anywhere in the world. However, Europe is relatively ahead in moving toward it, following large investments in public-private initiatives.[8] A major R&D investment is needed to capture this opportunity. While Europe already has a well-established infrastructure for education and research in the science and technology needed for cyber-physical systems, now China, S. Korea and other Asian countries are making tremendous investments to build the requisite infrastructure. Timing is urgent, as many non-critical IT software and systems development projects and capabilities have already gone offshore.

Our future is with the convergence of industrial technology and information technology. Information technology can bestow intelligence and its advantages on mechanical, chemical, energy, and other systems in the physical world. This is the convergence of the cyber with the physical that will next transform our economy.

Succinctly stated, the vision of the desired future state for all application sectors is that *cyber-physical systems are routinely developed with built-in assurance*[9] *of safety and security.* "Do it right the first time" becomes the cheapest and fastest way to both realize a system and manage upgrades over the system lifecycle. System development tools are certified. Accredited third party services are commercially available for verification and validation, review, attestation, and certification. Trustworthy accreditation services are readily available. System integrity is cost-effectively preserved as these critical systems evolve in response to changes in environment, requirements, threats. Requisite competence (knowledge, skills) is certified, and certified people with the requisite competence are readily available. The requisite body of knowledge is mature and readily accessible. Educational and training institutions have mature curricula to produce and certify the requisite competence.

---

[7] See the *CPS Executive Summary*, CPS Steering Group, March 2008, http://precise.seas.upenn.edu/events/iccps11/_doc/CPS-Executive-Summary.pdf

[8] The Embedded Computing Systems Initiative (ARTEMIS), ftp://ftp.cordis.europa.eu/pub/fp7/docs/factsheet_artemis_en.pdf

[9] To reach such a level of assurance for digital instrumentation and control systems in the nuclear navy, verification and validation effort is 9 times the rest of the development effort.

Objectives of an Initiative

The initiative seeks to address the challenge set out in the PCAST 2007 report, which asserted: "Among the goals of a program to improve development methods should be:

- Establishing a scientific basis, a codified knowledge base, and shared principles for designing, building, evolving, and operating NIT systems connected with the physical world
- Synthesizing knowledge from the physical sciences, mathematics, engineering, biological sciences, computer science, and other fields to model and simulate such systems in their full complexity and dynamics, including the interactions among potentially many dynamic systems and components in uncertain environments
- Developing a modern NIT systems technology framework to support the real-time computational control requirements of complex, networked, engineered physical systems
- Establishing rigorous, systematic, scalable, and repeatable design, development, verification, and validation methods, particularly to integrate design, evolution, and certification and thereby accelerate the approval process and reduce the cost of including (or modifying) new NIT-based capabilities in products for public use
- Building a variety of research testbeds that can be used to test, refine, validate, and approve system designs and development methods
- Developing, documenting, and disseminating research-based standards that are integrated throughout the R&D process to achieve best practices for designing systems cost-effectively to function dependably in their environment, with the necessary assurances of reliability, safety, security, and usability"

Challenges in moving from the current state to the desired state

Progress will not occur spontaneously. Both natural inertia and more deeply institutionalized barriers must be overcome. Among these, some of the most important and difficult are:

High effort threshold: The effort threshold to reach the desired state is too large for any individual organization or group or application domain to overcome by itself. Market and societal forces for the transformation do not exist. Cross-sector cooperation is needed to develop the common CPS science and technology foundation.

Reactive behavior: Societal behavior is reactive (e.g., deaths from infusion pumps; unwanted acceleration in automobiles; 2003 Great Lakes Blackout) – not proactive. The CPS problem space is growing exponentially. Concerted effort is needed to develop the CPS science and technology infrastructure to avoid such tragic and disruptive mishaps, which can arise due to accidental or malicious causes.

Education and Training: The educational and research infrastructure is organized around single-discipline oriented "chimneys" – not teaching, training, and exploring the integration of knowledge from diverse disciplines.

To overcome the challenges, we propose jump start activity that leads into a long-range plan. The activities build on research already underway and related science and technology initiatives other than CPS R&D. There are two key elements in the proposed strategy:

1. Define and exercise an iterative, evolutionary process to progress from the current state to the desired state.
2. Identify and model a representative challenge problem in at least one application sector (e.g. medical), embodying the key cross-sector challenges experienced in the current state. Generalize the solution approaches and apply to other application sectors for validation.

Common cross-cutting themes arise in the perspectives of the participating agencies. (The Annex to this document summarizes current state and future vision in different sectors from representative agency perspectives.) These are:

- Innovation, competitiveness, workforce productivity
- Safety, security, reliability
- Autonomy
- Interaction, Coordination, Interoperability
- Complexity
- Usability
- Cost of certification, cost of recalls and delayed time-to-market
- Cost of system evolution and change

To jump start research to address these themes, a call for "leap-ahead" technology is required that will create new opportunities for multidisciplinary research, causing the computing and engineering research communities to move from narrowly focused, separated research activities to more a connected, interactive research forum ("a marketplace of ideas"). Such a forum can accelerate the development of knowledge and technology and can provide a productivity and innovation multiplier for future systems. Mechanisms such as Open Source development, challenge competitions, and reference implementations of groundbreaking ideas would be sought to spur the research community towards transformative approaches that can apply to real systems. Such an effort would require engagement of both research and mission agencies towards their shared needs. Success will depend upon progress in three dimensions: (1) strategic science and engineering research thrusts, (2) technology capacity building, and (3) programmatic cooperation among agencies to provide interaction and leverage on hard problems of importance to US economic sectors.

"Leap Ahead" Systems Technology: Research Thrusts

Systems you can bet your life on

This thrust tackles core problems in achieving certifiably dependable systems and software.[10,11] A fundamental transformation of system design and implementation approaches is required; the current state of the art will not suffice. Relevant research would take a cyber-physical perspective in devising innovative methods and mechanisms to achieve dependable functionality, safety, security, and privacy end-to-end: from design to implementation to operation. A key focus of this thrust is on cyber-physical design for resiliency, fault tolerance, and guaranteed recovery. The span includes topics such as: methods for assuring non-interference of potentially conflicting system actions, new concepts for monitoring and management of both cyber and physical system condition ("health"), and new methods

[10] Sufficient Evidence? Building Certifiably Dependable Systems, http://sites.nationalacademies.org/CSTB/CompletedProjects/CSTB_042247
[11] Critical Code: Software Producibility for Defense, http://www.nap.edu/catalog.php?record_id=12979

for detecting failure modes that may have cyber and physical causes and assessing criticality of their consequences. The resulting assurance technology would be used not only during the design phase, but also to guide safe adaptation. Certification approaches would be pursued that logically relate design and verification evidence to safety and security claims. This research thrust seeks an assurance capability that can mesh with and enable technology developed under the research thrusts that follow.

Connected, capable, cooperating, controlled

This research thrust pursues new capability for easily orchestrating actions taken by multiple interacting systems (or subsystems) through cooperative, high-performance, cyber-physical control. This is the arena in which ad hoc approaches are most visibly failing today. Instead of pursuing traditional approaches that count on highly-centralized information to enable centralized decision and control – this thrust would explore new control architectures that may be networked over wired and (increasingly) wireless infrastructure. New theory, tools, and systems technology are needed to support "live" coordination and cooperation of systems. To accomplish this, innovations are needed in distributed real-time supervisory control. New approaches must accommodate a dramatic shift from traditional closed-loop control systems -- designed using wide safety margins and generally commanded by cooperating human operators -- to highly automated, even autonomous, systems that must cooperate to achieve overall system objectives in challenging environments. The configuration of interacting systems may change, as may the underlying infrastructure (for example, a wireless network may be supported by the participating systems, as in wireless networks formed opportunistically based on vehicle proximity). To achieve "cooperative autonomy" in this setting entails innovation in several contributing areas: real-time supervisory control; real-time networking for physical systems; security and privacy mechanisms suitable to protect real-time control processes in physical system timeframes; improved foundations for human interaction with autonomous systems (e.g., robots and humans working in shared space). The cyber-physical perspective adopted in this thrust demands control mechanisms that can operate over a much wider range of physical interaction and uncertainty requirements than is accommodated in traditional systems. To increase technology leverage, this thrust also would seek to raise the level of assured support provided by control system hardware and software platforms.

Open systems revisited: the digital-physical interface

Cyber-physical systems comprise multiple inter-operating software and physical components. Physical and cyber components have historically been developed by teams with different engineering cultures. On the physical side, concepts are expressed in terms of continuous-valued functions and components are defined as physical objects. On the cyber side, concepts are expressed in terms of digital logic and components are defined as software objects. Building successful integrated systems requires meshing of these physical and logical engineering views. It is time to take a new look at the margins of design, with attention to defining and verifying the requirements for inter-operability between physical and cyber components. This requires foundational research on models and abstractions that bridge the digital/physical divide.

The new clockwork

To control or react to events in the real world, cyber components need to maintain current information about the state of the world, analyze that information, and act on it before the world moves on. The closer the cyber and physical are required to co-operate, the more time-critical become their interactions. Software must not only be trusted to do the right thing; it must be trusted to do it at the right time, reliably, like clockwork. Core research challenges include meshing time and event-based system requirements, and improving the receptiveness and responsiveness of systems. These

challenges are magnified when components are required to interact at a distance. Real-time networking is at a very primitive level. Much of the prior art in real-time systems has become ineffective as advances in hardware and software technology have increasingly abstracted away the ability to manage the execution timing of software, by introducing layers of virtualization. A serious instance of such regression in our ability to build time-critical systems has been the introduction of multi-core processors, which provide the appearance of multiple computers capable of doing computations in parallel, but exhibit unpredictable timing interactions between the cores. This transformative change in technology has rendered obsolete a very large part of the theory and the software infrastructure developed for real-time systems for time critical systems.

Technology for a competitive U.S. industrial base

This thrust explores the development of well-founded cyber-physical tools and technologies that can empower competitive production of components and integration of future systems. Research under this thrust would focus on issues in managing modularity for open engineered systems to enable principled integration of components (e.g., from possibly-volatile supply chains). Areas of effort include design for "plug and play" without succumbing to the tyranny of overdesign, maintaining needed safety margins, and managing complexity of engineered systems as they scale both up and down. To dramatically multiply workforce productivity will require: new tool chains for both rapid and assured development of engineered physical systems; new technologies and architectures for networks, computing, and software platforms embedded in, and linking cyber-physical systems; and principles of design and programming languages that close the cyber-physical software gap and improve productivity.

Technology Capacity Building

Research infrastructure

A corresponding effort is needed to provide research infrastructure that can support the wide range of research activities envisioned. Translation from basic research to applicable technologies is greatly aided by open experimental platforms that provide validation of theories and comparison of alternate solutions. Research infrastructure creation will be enabled by multi-agency "virtual" research centers, in which government-supported and even privately-funded or public-private contributions of experimental platforms can be hosted. Ultimately, a mechanism is needed to actively foster transition of the research for use in government and industry. One possible longer-horizon mechanism is a multi-agency research evaluation and transition center.

Programmatic jump start

A translational research pipeline is needed, comprising long-term basic research, experimental applied research, prototyping and early development, phased deployment, and adoption in mission systems. Both research and mission agency participation and industry-university engagement are essential in each stage.

There is strong interest from mission agencies, and their representative problems offer model opportunities for strategic early action using "virtual centers" to jump-start topics that address transition from the current state to the desired vision. In all actions outlined below (and future actions), a pervasive and cross-cutting interaction with NSA and DHS is intended, through a cyber-security initiative that parallels this proposed initiative. Cooperation can address issues in design (building in cybersecurity), system evaluation, and scientific underpinnings for cybersecurity in cyber-physical systems. Today, clear candidates for interagency participation in jump start activities include:

- Medical Devices and Systems (NSF, NIH, FDA, NIST): Such an effort can build on parallel investments: NSF supports research in open medical systems technology and NIH investments in infrastructure to enable open, interoperable medical devices and systems, on the existing NSF-FDA "scholar-in-residence" interaction in this area, on the FDA's infusion pump initiative, and on NIST's mission to support innovation-promoting standards and high-confidence manufacturing.
- Ground Transportation (NSF, FHWA, NIST, DOE): Such an effort can explore a "virtual center" concept, linking projects funded by the NSF and the DOT/FHWA and supported by NIST intramural research. The initial projects to be included are related to vehicle autonomy, passenger safety, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communication, and safety-enabling highway infrastructure. This "virtual center" would include NIST participation in innovation-enabling automotive standards, manufacturing, and (with DOE) green transportation. The effort would build on prior HCSS agency interactions with the USCAR consortium regarding research needs and vehicle reliability. The objective is to create potential opportunities for public-private efforts to advance U.S. competitiveness in automotive transportation.
- Air Transportation (NSF, NASA, FAA JPDO for NextGen, AFRL, NIST): Such an effort can initiate research on the real-time cooperative networked control concepts and in the system and software verification strategies that are essential to overcome barriers to increased autonomy in U.S. airspace. These include strategies for including unmanned air systems (UAS) flight in the continental U.S. NIST involvement would guide manufacturing considerations and innovation-enabling standards.
- Energy (DOE, ARPA-E, NSF, NIST, NRC, DHS, NSA): Such an effort can support research exploring architectures and hierarchical real-time networked control concepts for complex, configurable, management of interacting electrical grids and system load (e.g. smart building) designs. Innovation-enabling standards and cybersecurity are key elements of this effort.

This list is intended to illustrate, rather than to serve as an exclusive list of options. Manufacturing is a critical activity that cross-cuts all of these sectors. Agriculture, mining, and environmental protection are concerns notably omitted from the list that ultimately should be included.

Key action: Without a strong, central focus on innovation and the common issues in translational research for innovation in cyber-physical systems, including standardization, manufacture, and deployment, each of the jump start activities above runs the risk of devolving into an isolated, marginally-effective effort. At the outset, these actions can take advantage of NSF-initiated Virtual Organization (CPS VO) support, the purpose of which is to enable a multi-disciplinary CPS research community and support industry-university interaction. The CPS VO is in the first year of its 5-year funding and has received supplemental funding from HCSS agencies. However, an expanded and stabilized cross-agency entity needs to be established, whose mission is to foster long-term translational research and persistent interaction between academia and industry. We urge, at this earliest stage, steps be taken towards such an entity, with mission to foster US industrial innovation in cyber-physical systems.

Long range action plan

The central research thrusts outlined above would be pursued and adapted cooperatively by the agencies as the CPS discipline matures. To achieve persistent interaction among industry, academia, and government we recommend that the above "key action" lead to the creation of a Joint Institute for

Cyber-Physical Systems that will develop pre-competitive, generic solutions that remove those barriers and create testbeds for demonstrating both the effectiveness and synthesis of those solutions. This also will facilitate the path to commercialization and minimize the risk of early adoption of new cyber-physical systems technology. The activities of the Joint Institute can enable translational research for both research and mission agencies under a broad charter to foster US innovation and US industrial competitiveness across all sectors.

The Joint Institute for Cyber-Physical Systems will have four major benefits. First, it will bring together complimentary R&D assets from government, universities, and industry. This will change the traditional sequential approach to innovation to a more productive parallel approach in which basic science and applied engineering are addressed concurrently. Second, having industry as a vital partner from the beginning ensures that the right pre-competitive solutions are being developed and facilitates the technology transfer needed to go from prototype to commercialization. Third, the institute solves a common problem that arises in the development of infrastructural solutions – risk pooling. This occurs because no one company is willing to invest the time or resources to develop the public-good solutions necessary for commercialization. Fourth, and most importantly, the institute provides a foundation for compressing the entire innovation life cycle. This compression is critical in today's economic environment where time-to-market is becoming the decisive factor in success.

ANNEX – Assessment of Current Status and Future Vision, by Industrial Sector

Many barriers and gaps are echoed across sectors. The following brief subsections illustrate issues that crosscut the future visions, technology needs, and research gaps for US industrial sectors and mission agencies.

Determining barriers to US productivity and future technology R&D needs could be attempted sector-by-sector. Addressing them in isolation would multiply cost and waste redundant effort. It also would discard an opportunity for valuable cross-fertilization.

Engineering and Manufacturing

Where we are now: Today's manufacturing is done on in traditional factory-situated shop floors, focused on fabricating physical components in mass production. System integration floor setup takes days, rather than hours and minutes. Robotic automation has improved productivity of some tasks, yet major technology investment and maintenance costs restrict such workflow automation to relatively high-volume manufacturing operations. Increasingly labor is outsourced, with flight of design, manufacturing, and supply chains to cheap, highly leveraged, and increasingly well-educated labor markets overseas.[12] Huge investments by China, South Korea, Indonesia, India, Europe (both Western and Eastern) in research and innovation multiply their industrial capacity and access to technology and accelerate training of skilled workers. In the US are seen shuttered factories, workforce displacement, and decline of private investment in US industrial capacity. Low technology investments in the US increasingly detract from the productivity multiplier for, and investment in, a skilled US workforce capable of producing value and earning a living wage. For these reasons, the decline in US manufacturing competitiveness is being studied as a possible national security risk.[13]

Vision: Cyber-physical systems science and technology will accelerate US invention and innovation in both products and manufacturing processes: smart products, smart production, and lifecycle design for product safety, security, and sustainability. Global demand is increasing for tailored smart products that have active control and communicate easily with people and other devices. Homes, automotive and air vehicles, healthcare, clothing, agriculture, food processing and preparation, military logistics and weapons systems, all benefit from cyber-physical engineering concepts, infrastructure, and tools to reduce time-to-market for smart products and automation-enabled systems. Emerging fabrication technologies such as additive manufacturing make possible agile, even on-site, fabrication and repair. Increased innovation in materials such carbon-fiber composites, conductive polymers, super-strength and active conformable and shape-holding materials, synthetic muscles, metal-ceramic compounds, and agriculturally-based polymers both enable these smart products and simultaneously increase opportunities for local sourcing and production of many products. Recycling and remanufacturing are mainstream elements of manufacturing. Certifiably safe, secure, and dependable "plug and play" integration of both cyber (computing, communication, control) and physical components increase opportunities for product specialization and customization. Research-, innovation-, and integration-enabling standards promote innovation, competition, and resilience in flexible supply chains. New 3D

[12] See, for example: Frugal Healing: Inexpensive Asian innovation will transform the market for medical devices, The Economist, Jan. 20, 2011.
[13] Intelligence Director Will Look At National Security Implications of U.S. Manufacturing Decline, Manufacturing & Technology News, Feb. 3, 2011.

printing[14] and other additive manufacturing technologies (for, e.g., machine parts, aircraft wings), "WikiFAB", and similar concepts for IP-based design and manufacturing enable new entrants into US industry and can enhance local and regional productivity. These advances enable production activities to be flexibly located near sources of materials, technology skill centers, or consumers of end products -- enabling more flexible optimization of cost and markets and control of environmental impact. Not least, American children can look forward to safe, interesting, creative, and well-compensated occupations, leveraging highly versatile core knowledge and skills, in which they can actively contribute to the Nations' growth and productive capacity.

Medical Technology

Where we are now: Cost and quality of health care delivery have become central issues for the U.S. Economy. Alternatives are needed to the use of hospital-based care, particularly emergency room care, in circumstances that do not require it. However, large technology gaps currently exist between current and future needs for clinical care technology and between hospital-based, doctor's office, outpatient, and home healthcare delivery. The transition from paper to the electronic health record (EHR) is expected to contribute progress in healthcare delivery, but the integration of biomedical technology with EHR use lags. We are at the verge of a transition from individual, stand-alone medical instruments and devices to increasingly automated, networked, and mobile medical technologies. Yet neither wireless device technology nor device designs are ready for interoperation in either clinical or alternative settings. Devices currently are moving from wired to wireless interfaces, without full consideration of the safety and security implications. Validation and verification of engineered medical technology remains extremely time consuming and expensive, slowing time-to-market, inhibiting innovation, and complicating regulatory approval required for safety, and still the need to remove defective designs from the market is not always avoided. Current device architectures are highly proprietary, not interoperable and rely heavily on skilled medical professionals to provide inputs and assess outputs. Skilled technicians are needed to configure, calibrate, and maintain hospital-based systems. As a result, the spiraling costs of these systems are economically feasible only on the hospital scale (and perhaps not even there). As in other sectors, the flight of industry to Asia and Europe is also seen in medical technology, at severe cost to U.S. innovative capacity for biomedical advances, to U.S. medical researchers who lose the opportunity to participate in new device design, and to patients with urgent need for early access to technology-based therapies.

Vision: U.S. research investment in medical cyber-physical systems will spur innovation at the patient/technology interface. It will enable low-cost, continuous, real-time monitoring of patients with chronic disease. It will exploit and unlock the potential of wireless communications for safe and secure health care delivery. The goal is to enable hospital-quality (or better) care to be delivered at home or alternative care settings. An important subgoal is the interoperation of integrated therapeutic devices with electronic health care records. This will vastly improve access, quality, and cost-benefit through remote and mobile health care delivery. Investment in underpinning methods for engineering medical cyber-physical systems will enable the development of non- and minimally-invasive medical technologies that can reduce recovery times, risks, and health care costs. It also can provide support for care delivery that is safer and increasingly aware of the patient and his/her medical context (for example, the patient whose infusion pump may have a nearly-exhausted supply of insulin, or the pacemaker wearer who should not be subjected to MRI). Cyber-physical medical research will

[14] Print me a Stradivarius – How a new manufacturing technology will change the world, The Economist, Feb. 10, 2011.

accelerate innovation in medical robotics, advanced prosthetics, and biotech-enabled health solutions[15]. A trend will be seen towards the mass customization of heterogeneous, configurable personalized medical devices, and towards natural, wearable sensors (clothing, jewelry) and benignly implantable devices[16]. With the advance of understanding of human physiological processes and associated algorithms, it possible to imagine real-time pervasive health interventions that duplicate cyber (computing) functions in biology and permit therapy at a functional or even cellular level.

In this, as in other sectors, CPS engineering science and technology will bolster U.S. medical technology competitiveness by providing both, design and engineering capability for highly-innovative and capable, as well safe and secure, medical products and systems, together with the means to safely manufacture, implement, and approve them. Strengthening technological competitiveness in CPS will create new opportunities for US innovation in biomedical technology; expand opportunities for an American workforce skilled in designing, manufacturing, and using these new technologies; and deliver safer, more accessible, and cost-effective healthcare to U.S. citizens.

Energy

Everything from our finances and transportation to our health, water supply, and emergency responses depends on reliable energy. Energy delivery systems—networks of physical processes that produce, transfer, and distribute electricity, oil, and natural gas—are the backbone of the energy sector. These physical systems rely fundamentally on control systems—the interconnected electronic and communication devices that monitor and control these processes. Control systems include the sensors and actuators that physically monitor and control the energy processes, the computer-based systems that analyze and store data, and the communication networks that interconnect the process and computer systems. Today's highly reliable and flexible energy infrastructure is possible due to the control systems' ability to provide timely information to system operators and automated control over a large, dispersed network of assets and components. A resilient, reliable, and secure electric transmission and distribution grid is paramount to the success of the economy and the public health and safety of citizens and businesses.

Where we are now: With population increases and economic growth comes increasing consumer demand for electricity. Today's electric grid is demand driven: electricity is generated as it is used, with minimal storage capability. Instead, the grid relies on control systems, high-speed computer and communication systems that constantly balance the stable generation and flow of electricity. Managing generation with requisite responsiveness to demand is inefficient for many of today's generation systems (especially coal-based) that are difficult and slow to switch on- or off-line in the face of load changes. Disturbances in the control can destroy critical process components and cause failures capable of stopping the generation and flow of electricity to end users across the nation. Excessive peak loads, overheated transmission lines, and natural accidents such as falling tree limbs cause brownouts and blackouts, sometimes triggering cascading power system failures affecting large regions of the country. The power grid also is vulnerable to intentional disruption: a shift from closed to extensively networked (including Internet) control and communication, and from proprietary to widely-accessible commercial software, has increased vulnerability to cybersecurity attacks. This was seen recently in the 2010 discovery of Stuxnet malware, specifically designed to exploit Supervisory Control and Data Acquisition (SCADA) systems.

[15] High Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care, http://www.nitrd.gov/About/MedDevice-FINAL1-web.pdf

[16]

In a first step to abate congestion, the widespread deployment of smart meters and an advanced metering infrastructure (AMI) seeks to involve consumers in attempts to reduce peak and overall electricity use. ARRA-funded Smart Grid projects are expected to add 18 million meters to the 8 million currently installed; the Federal Energy Regulatory Commission (FERC) estimates that 80 million meters may be installed by 2019. However, this does not fully resolve the overall structural issues confronting today's power system. Environmental issues have moved to the forefront of the electric power business. Currently, over two-thirds of electricity generation in the United States comes from the burning of fossil fuels (both natural gas and coal); however, generation from renewable resources is increasing, and is expected to reach 772.99 billion kilowatt-hours (kWh) by 2030. The growth rate of renewable energy sources such as wind, solar, and hydropower is increasing at both the bulk transmission system and at the distribution system levels. The mix is likely to change substantially over the next several decades as the nation seeks cleaner sources of power supply. Although renewable energy sources have immense potential for the future, the power they can supply is intermittent or at best variable. In today's grid this highly variable generation can compromise grid reliability.

Vision: Flexibility and resilience will be engineered into the power grid, providing real-time automated response, real-time pricing, dramatically reduced numbers and extent of outages and power quality disturbances, improved control of transmission and distribution capacity, better resource utilization and reduced congestion. The future grid must include control architectures that enable new and clean power supplies to be taken on- or off-line, readily and flexibly to meet requirements. New methods will be needed to incorporate vastly increased electricity storage capacity (batteries, PHEVs), that can buffer supply and demand, providing improved capacity to handle peak loads. The future grid control architecture will be required to integrate both centralized and distributed energy resources, exploiting new technologies for solar, thermal, wind, and water based generators, small modular reactors for smaller-scale nuclear power generation, and systems fired by alternative fuels. Smart buildings will include co-generation of heat and power. The previous lines dividing energy market components into generation, bulk energy transmission, and distribution are shifting, as plants and homes provide generation directly into what previously was considered the distribution network, at or near the point of consumption. CPS engineering will enable an end-to-end integrated control system view that allows optimization from generation to consumption. For example, the advanced metering infrastructure can be extended to enable more comprehensive management of industrial energy consumption, "smart load", to schedule power utilization. Advances in cyber-physical systems technology -- with cybersecurity built-in -- will provide next-generation platforms for resilient, secure, real-time networked control of these diverse elements. The scope of these long-needed changes will create diverse new opportunities for growth of this sector through innovation in highly flexible and dependable (resilient, safe, and secure) energy technologies. The vision is of a robust 21st century US energy technology sector that depends on, and provides jobs for, a skilled workforce that can build and operate this dynamic new landscape of U.S. energy systems and infrastructure.

Transportation

Advances in cyber-physical systems are critical for the entire U.S. transportation industry to meet increasing complex and difficult goals from increasing safety, to reducing energy dependence and environmental impacts, to supporting sustainable economic growth and increased quality of life. Travel is a near universal daily activity whether going to work, to school, or to visit a neighbor. An efficient multi-modal network also is critical in supporting the national flow of goods and services across oceans and continents or to the corner store.

Air Transportation

Where we are now: Today's aircraft operate with procedures that are very similar to those created over 30 years ago. Although the national airspace system (NAS) is the safest in the world, it is a large, complex, distributed, and loosely integrated network of systems, procedures, and infrastructure, much of it decades old. Air traffic control is operator-centric, performed primarily through the use of surveillance radars, voice radio systems, limited computer support systems, and numerous complex procedures. The NAS's operating procedures were originally designed around technologies now considered antiquated, yet these procedures remain largely unchanged despite new concepts of operation afforded by current and near-term technologies. The resulting inefficiencies pose severe cost and capacity limitations on aviation growth. Uncertainties in the total flight environment negatively affect system throughput. Uncertainty is managed by queuing traffic to be serviced, and demand is managed by restricting access to the airspace to avoid straining capacity. Under capacity stress, it is becoming increasingly difficult to maintain aviation safety. On the airport surface, runway incursions and missed taxi clearances result from a lack of situational awareness and communication limitations for operators or traffic controllers. The use of unmanned aircraft in the NAS remains limited despite the growing demand in both the military and civil aviation sectors. Existing Federal regulations and procedures do not allow routine unmanned aircraft system access to the NAS. Furthermore, existing access methods are not sufficiently scalable to address current mission needs or commercial demand.

Vision: The FAA's Next Generation Air Transportation System (NextGen) [17] is a future system concept for substantial and long-term change in the management and operation of the national air transportation system. In the future, it is envisioned that all airports and aircraft in the US airspace will be connected to NextGen's advanced infrastructure and will continually share information in real-time. This "Net Centric" framework has the potential to improve air transportation's safety, speed, efficiency, and environmental impacts, while enabling increased capacity levels and convenience for passengers. NextGen represents a comprehensive vision that involves not only the development of new technology, but also the leveraging of existing technologies. It includes satellite navigation and control of aircraft, advanced digital communications, and enhanced connectivity between all components of the national air transportation system. Progress in cyber-physical systems research will address key risks of the NextGen concept and aviation safety in general: how to design and build highly functional, yet verified and validated complex systems. These NextGen challenges include: a changing balance of human vs. automated operation, a shift in authority between (hence new architectures for) air and ground control, the potential for failure modes arising from poorly-understood interaction of cyber and physical components, and growing need for automated flight control systems to cooperate and adapt to adverse conditions. In addition, aviation safety compels us to find new ways to improve effectiveness of safety and security certification, and to create new capabilities for in-flight management of system health and air-worthiness that can assure safe flight under increasingly complex conditions. NextGen-capable innovation in autonomous as well as human-piloted but highly-automated air vehicles and the infrastructure systems that support them will require advances to unify digital and physical (cyber-physical) engineering capability. No single entity – industry sector or government agency -- can accomplish this. A shared investment is needed to obtain the core high-confidence system architecture, design, and hardware/software/system implementation technology that will be required to produce and operate safe, secure, energy-efficient, and dependable systems for the 21st century. The future competitiveness of the US aviation industry, including aircraft manufacturers, commercial aviation, and general aviation companies (including many small businesses), is a central element of this puzzle. With a

[17] http://www.faa.gov/nextgen/

skilled cyber-physical systems workforce capable to build, maintain, and operate these systems, America can keep these crucial value-producing (hence high-value) jobs to sustain a robust, productive, and competitive U.S. aviation sector.

Ground transportation

Where we are now: With aging infrastructure, limited funding, and increasing demand, it is inescapable that we must enlist new approaches and technology so U.S. transportation systems can continue to support the economic well-being of the nation, states, regions, and communities. Even with dramatic decreases in traffic fatalities due to investment in new automotive systems, roadway designs, and enforcement strategies, the Centers for Disease Control and Prevention (CDC) cite a cost of over $70 billion in 2005 from preventable injuries and deaths from motor vehicle crashes. In addition, congestion in U.S. urban areas is estimated to cost $115 billion in 2009.

Vision: Surpassing what the U.S. created in the 20th century with infrastructure investment, research and development of cyber-physical systems can lead to dramatic changes in system safety, energy efficiency, and improved quality of life for the people travel, rely on, or live near the nation's surface transportation networks. With the integration of cyber-physical systems into both vehicle and infrastructure systems, we can aim towards a future where traffic fatalities are uncommon rather than daily events (no avoidable collisions, mitigation of collisions that do occur), where travelers and freight can arrive at destinations reliably and without fear of unexpected delays, and where advanced controls can provide substantial energy savings that can decouple the economic benefits of transportation from regional and global environmental impacts. From the vehicle perspective, the issues and opportunities discussed above under air transportation (increased automation; requirement for verification and validation; and simultaneous design for new capability, safety, and security) increasingly are concerns in the automotive industry. New concepts for extreme-efficiency plug-in electric and hybrid-electric vehicles already are being explored for their potential to reduce transportation dependence on foreign energy resources. The integration of vehicles into the power grid as both "smart load" (electrical charging behavior) and "smart storage" (discharging behavior) opens new horizons for U.S. engineering -- opportunities and challenges that will test American inventiveness in both transportation and power systems. The challenges of simultaneous, integrative, cyber and physical design of vehicle, roadway, and energy infrastructure control open tremendous opportunities for innovation in function and capability for both transportation and energy systems. Success in this vision will both depend upon and provide highly skilled jobs in the transportation industry as well as bolstering the efficiency of the overall economy by surmounting barriers to travel and trade. The path to success, however, is complex, requiring coordinated investment and leadership.

Defense

Where we are now: Defense systems for air, land, sea, and space are engineered systems that are increasingly cyber-physical systems. These are systems that monitor a tactical environment, operate and cooperate in that environment, alter it, adapt to it, and provide a common operational picture into its operations. The technology, operational environment, and mission change but these processes do not. These are complex, highly-integrated, and highly automated "smart" engineered systems: cyber-physical systems subject to requirements for extreme survivability, performance, robustness, interoperability, and security. These are highly engineered systems that operate in extreme environments. These systems are called upon to protect and defend our country and provide humanitarian assistance and disaster relief in times of international crisis. However, development and acquisition costs are escalating. Our inability to routinely build these systems at predictable and reasonable cost is a

recurring problem, affecting our capacity to provide reliable and cost-effective technologies to our own armed forces and those of our allies.

Vision: The need for agile development of cyber-physical systems in defense will accelerate, driven by changing defense needs. Systems will become smarter, more autonomous, highly coordinated, and remotely operated in shared physical spaces. New real-time networked control platforms will support rapid, safe, and secure integration of "smart" (cyber) technology that can exploit and manage innovative system physical capabilities and limitations. This will achieve unprecedented access to defense system automation, creating opportunities for new capability and innovation in operations. The trend will continue for smart unmanned platforms that increasingly can assume the roles that put personnel at risk, saving lives. Systems will be engineered to be more resilient to disruptive change without compromise of integrity. Systems will be more attuned to their environments, receiving and processing massive amounts of data, to determine courses of action. The goal of a strategic technology is to prevent technology surprise in the face of globally- emerging conflict situations, while offering new technological opportunities and options for defense and humanitarian assistance in this new space. The future defense landscape is one of expanding cyber-physical systems capability. Investment in the foundations, engineering design tools, and implementation platforms for such systems is an essential ingredient to make the technology affordable and maintain US leadership in defense systems.