INTERNATIONAL JOURNAL OF ENHANCED RESEARCH IN SCIENCE TECHNOLOGY & ENGINEERING
VOL. 2 ISSUE 2, FEB.-2013 ISSN NO: 2319-7463

Future of all technologies - The Cloud and Cyber Physical Systems

Abhishek Gupta[1], Mohit Kumar[2], Siddhartha Hansel[3], Aswini Kumar Saini[4]
[1,3,4]Department of CSE, GBPEC, Pauri Garhwal, Uttarakhand, India
[2]Department of CSE, Jaypee University of Information Technology, Solan, H.P., India
[1]abhi.g2010@gmail.com, [2]meetmohit24@rediffmail.com

Abstract: Modern society relies on a web of physical network infrastructures, such as power stations, telecommunication networks and transportation systems. Thanks to technological advances, these infrastructures have become increasingly dependent on one another and have emerged as interdependent networks. While interdependency enables to build systems that are larger, smarter and more complex, it is also observed that interdependent systems tend to be more fragile against failures, natural hazards and attacks. It is therefore of vital importance to develop the science for interdependent Networks, which serves as the foundation to better understand the interplays among individual networks and propel significant advances therein, such as the Internet, power grid, social networks, the financial system and the economy to name just a few. This paper aims at presenting our future research outlook oriented to the cloud, to mobile device security and to cyber physical systems and some challenges related to cyber physical systems.

Keywords: Cyber Physical Systems, cloud computing.

I. Introduction

As computers and communication bandwidth become ever-faster and ever-cheaper, computing and communication capabilities will be embedded in all types of objects and structures in the physical environment. Applications with enormous societal impact and economic benefit will be created by harnessing these capabilities in time and across space. We refer to systems that bridge the cyber-world of computing and communications with the physical world as cyber-physical systems. Cyber-physical systems (CPSs) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. This intimate coupling between the cyber and physical will be manifested from the nano -world to large-scale wide-area systems of systems. The internet transformed how humans interact and communicate with one another, revolutionized how and where information is accessed, and even changed how people buy and sell in the marketplace. Similarly, CPSs will transform how humans interact with and control the physical world around us.

Examples of CPSs include medical devices and systems, aerospace systems, transportation vehicles and intelligent highways, defense systems, robotic systems, process control, factory automation, building and environmental control and smart spaces. Since CPSs interact with the physical world, they must operate dependably, safely, securely, efficiently and in real-time. Cyber-Physical Systems (CPSs) integrate the dynamics of the physical processes with those of the software and communication, providing abstractions and modeling, design and analysis techniques for the integrated whole[1]. The dynamics among computers, networking and physical systems interact in ways that require fundamentally new design technologies. The technology depends on the multi-disciplines such as embedded systems, computers, communications etc. and the software is embedded in devices whose principle mission is not computation alone, e.g. cars, medical devices, scientific instruments and intelligent transportation systems [2]. Now the project for CPSs engages the related researchers very much.

Since 2006, the National Science Foundation (NSF) has awarded large amounts of funds to a research project for CPSs. Many universities and institutes (e.g. UCB, Vanderbilt, Memphis, Michigan, Notre Dame, Maryland and General Motors Research and Development Center, etc.) join this research project [3,4]. Besides these, the researchers from other countries have started to be aware of significance for CPSs research. In [5-7], the researchers are interested in this domain, including theoretical foundations, design and implementation, real-world applications, as well as education. As a whole, although the researchers have made some progress in modeling, control of energy and security, approach of software design, etc. the CPSs are just in an embryonic stage. The term cyber-physical systems (CPS) refers to a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities. The ability to interact with, and expand the capabilities of the physical world through computation, communication, and control is a key enabler for future technology developments. Opportunities and research challenges include the design and development of next-generation airplanes and space vehicles, hybrid gas-electric vehicles, fully autonomous urban driving, and prostheses that allow brain signals to control physical objects.

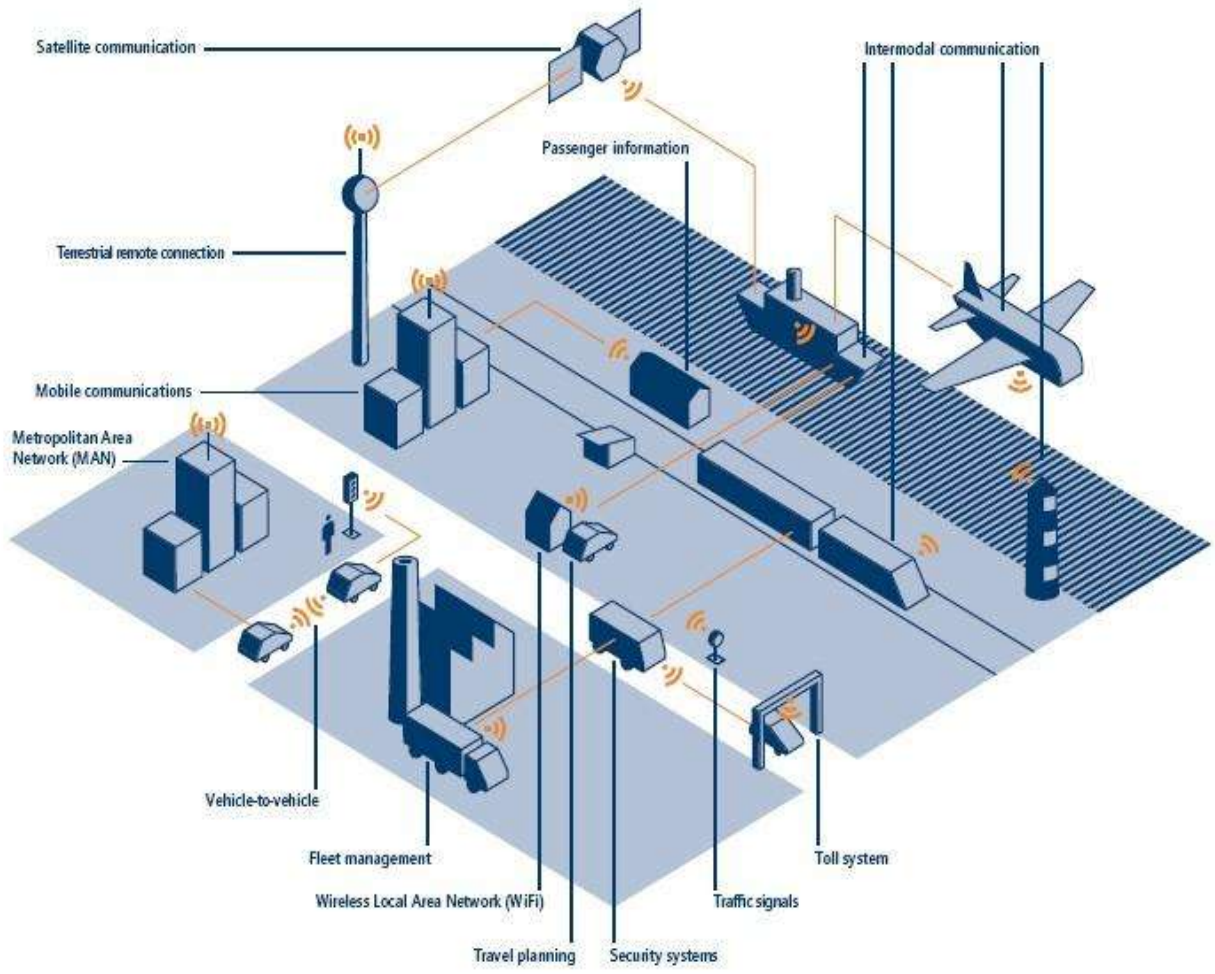

Figure 1: Modern Diagrammatic Layout of CPS

Over the years, systems and control researchers have pioneered the development of powerful system science and engineering methods and tools such as time and frequency domain methods, state space analysis, system identification, filtering, prediction, optimization, robust control and stochastic control. At the same time, computer science researchers have made major breakthroughs in new programming languages, real-time computing techniques, visualization methods, compiler designs embedded systems, architectures and systems software and innovative approaches to ensure computer system reliability cyber security and fault tolerance. Computer science researchers have also developed a variety of powerful modeling formalisms and verification tools. Cyber-physical systems research aims to integrate knowledge and engineering principles across the computational and engineering disciplines (networking, control, software, human interaction, learning theory, as well as electrical, mechanical, chemical, biomedical, material science, and other engineering disciplines) to develop new CPS science and supporting technology.

In industrial practice, many engineering systems have been designed by decoupling the control system design from the hardware/software implementation details. After the control system is designed and verified by extensive simulation, ad hoc tuning methods have been used to address modeling uncertainty and random disturbances. However, the integration of various subsystems, while keeping the system functional and operational, has been time-consuming and costly. For example, in the automotive industry, a vehicle control system relies on system components manufactured by different vendors with their own software and hardware. A major challenge for original equipment manufacturers (OEMs) that provide parts to a supply chain is to hold down costs by developing components that can be integrated into different vehicles. The increasing complexity of components and the use of more advanced technologies for sensors and actuators, wireless communication and multicore processors pose a major challenge

for building next-generation vehicle control systems. Both the supplier and integrator need new systems science that enables reliable and cost-effective integration of independently developed system components.

II. Features of CPSS

Goals of CPSs research program are to deeply integrate physical and cyber design. The diagrammatic layout for CPSs is shown in Figure 1. Obviously, CPSs are different from desktop computing, traditional embedded/real-time systems, today's wireless sensor network (WSN) etc. and they have some defining characteristics as follows [7-10].

- **Closely integrated:** CPSs are the integrations of computation and physical processes.
- **Cyber capability in every physical component and resource-constrained:** The software is embedded in every embedded system or physical component, and the system resources such as computing, network bandwidth, etc. are usually limited.
- **Networked at multiple and extreme scales:** CPSs, the networks of which include wired/wireless network, WLAN, Bluetooth, GSM, etc. are distributed systems. Moreover, the system scales and device categories appear to be highly varied.
- **Complex at multiple temporal and spatial scales.** In CPSs, the different component has probably in equable granularity of time and spatiality, and CPSs are strictly constrained by spatiality and real time.
- **Dynamically reorganizing/reconfiguring:** CPSs as very complicated systems must have adaptive capabilities.
- **High degrees of automation, control loops must close.** CPSs are in favor of convenient man-machine interaction and the advanced feedback control technologies are widely applied to these systems.
- **Operation must be dependable, certified in some cases:** As a large scale/complicated system, the reliability and security are necessary for CPSs.

III. The Future

Smart Devices, The Cloud and Cyber-Physical Systems

Arguably, the future of technology is characterized by a pervasive access to the Internet through smart devices, by the extension of the cloud computing paradigm, and by the increasing interaction between the digital and the physical world. We have already mentioned our work on Bluetooth-enabled smartphones [11],[12]. Building upon this expertise, we are currently working on the vulnerabilities of smartphone user interfaces and input systems. We have some past experience on analyzing the grid computing paradigm [16], arguably one of the ancestors of the upcoming cloud computing revolution. In this area, we are working on the basis of the observation that there is a strong parallel between the emerging paradigm of cloud computing and the traditional time-sharing era [17]. Clouds are the modern reincarnation of mainframes, available on a pay-per-use basis, and equipped with virtual, elastic, disk as-a- Service that replace the old physical disks with quotas. This comparison, beyond being fascinating in its own self, prepares the ground for a constructive critique regarding the security of such a computing paradigm and, especially, of one of its key components: web services. Along this line, we concentrate on a few, critical hypotheses that demand particular attention. Although in this emerging landscape only a minority of threats qualify as novel, they could be difficult to recognize with the current countermeasures, given the change that the new computing paradigm has induced in the use of the network stack.

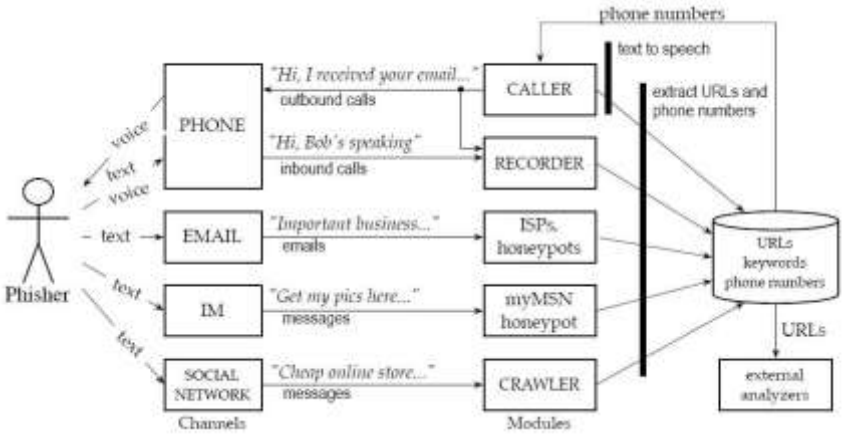

Figure 2: Social-engineering centric data collection architecture.

The final new trend that we wish to study is the emerging class of security issues that arise in the interstitial layer between safety-critical, physical systems and digital, pervasive systems (a typical example is a SCADA-controlled industrial process, but in the near future we can foresee more and more such interactions). The increasing interconnection between such systems creates new attack surfaces that are neither physical nor digital, and which cannot be identified if such systems are studied and secured separately as is customarily done nowadays. As such systems are prevalent in critical infrastructures such as power grids or water-distribution plants, they are primary target for cyber-terrorism and cyber-warfare attacks.

We are beginning to investigate this emerging class of vulnerabilities with an empirical, bottom- up methodology. We will start from devising real-world attacks against both the digital and the physical side of carefully selected target systems, and strive to unveil recurring vulnerability patterns that can be generalized to a (possibly novel) class of vulnerabilities. To ensure their real- world applicability, we will validate, step by step, assumptions, results and countermeasures on replicas, models or simulated systems in controlled environments, with the help of industrial partners. As a first result, we aim to generate actionable assessments of the security of representative, high-profile systems, structured in a series of novel attack papers, and correspondingly produce targeted countermeasures. However, our more ambitious long term goal is to formalize the general problem and its root causes, by attempting to develop a theory, a taxonomy and a methodology for describing, identifying and assessing this novel class of vulnerabilities. Leveraging this general theory, and systematizing our observations, we will also try to produce preemptive secure design patterns and general solutions for this class of problems.

IV. Challenges and Opportunities

Advances in CPS research can be accelerated by identifying needs, challenges, and opportunities in several industrial sectors and by encouraging multidisciplinary collaborative research between academia and industry. The objective is to develop new systems science and engineering methods for building high-confidence systems in which cyber and physical designs are compatible, synergistic, and integrated at all scales. Current and past industry investments in CPS technology research have been significant but focused on shorter-term, quicker-payoff proprietary technologies. Recently, governments and some industry sectors are investing in longer-term, precompetitive technologies and innovative test beds. For example, the European Union has initiated a major joint technology initiative with public-private funding by European nations and industry called Advanced Research and Technology for Embedded Intelligence Systems (ARTEMIS). Similarly, based on recommendations in the August 2007 report of the U.S. President's Council of Advisors on Science and Technology (PCAST), the U.S. National Science Foundation has been funding fundamental CPS research and education [18]. Related initiatives are being pursued in other countries, including Japan, China, South Korea, and Germany. CPS grand challenges are being articulated in many industry sectors. The U.S. National Academy of Engineering has listed 14 grand challenges that relate environmental, health, and societal issues; these issues will clearly benefit from advances achieved in cyber-physical systems. The control engineering research community can play a leading role in the development of cyber-physical systems. Some of the opportunities are described below :

(a) Biomedical and Healthcare Systems

CPS research is revealing numerous opportunities and challenges in medicine and biomedical engineering. These include intelligent operating rooms and hospitals, image-guided surgery and therapy, fluid flow control for medicine and biological assays, and the development of physical and neural prostheses. Healthcare increasingly relies on medical devices and systems that are networked and need to match the needs of patients with special circumstances. Thus, medical devices and systems will beneeded that are dynamically reconfigured, distributed, and can interact with patients and caregivers in complex environments. For example, devices such as infusion pumps for sedation, ventilators and oxygen delivery systems for respiration support, and a variety of sensors for monitoring patient condition are used in many operating rooms. Often, these devices must be assembled into a new system configuration to match specific patient or procedural needs. The challenge is to develop systems and control methodologies for designing and operating these systems that are certifiable, safe, secure, and reliable.

Research challenges in medical technology and healthcare were considered in a series of workshops that are summarized in a U.S. National Information Technology Research and Development (NITRD) report [19]. The report recommends research for new system science and engineering with the following goals:

- Interoperable and open medical systems;
- Distributed monitoring, distributed control, and real-time wireless networks for hospital intensive-care facilities;
- Certification methods for medical device software and systems and networked patient monitoring and assistance;
- Model-based frameworks that support component-based modeling, design, testing, and certification using patient-specific models.

Another challenging area for CPS research is cognition and neuroscience for understanding the fundamental principles of human motor functions and exploiting this understanding in engineered systems. Examples include brain-machine interfaces, therapeutic and entertainment robotics, orthotics and exoskeletons, and prosthetics. Humans and animals seamlessly integrate sensing, computing, and motor control functions. These highly coupled systems do not satisfy simple modularity principles, but are composed of multifunctional elements, computation and feedback loops at different time and length scales, noisy signals, parallel processing, and redundant fault-tolerant architectures. Recent research has suggested that animals use some form of optimal filtering, stochastic control algorithms, and large-scale probabilistic computing structures in dealing with uncertainty. Control researchers working with biologists, neurophysiologists and computer scientists may be able to make further progress.

(b) Next-Generation Air Transportation Systems (NextGen)

Cyber-physical systems research is likely to have an impact on the design of future aircraft and air traffic management systems, as well as on aviation safety. Specific research areas include (1) new functionality to achieve higher capacity, greater safety, and more efficiency, as well as the interplay and tradeoffs among these performance goals; (2) integrated flight deck systems, moving from displays and concepts for pilots to future (semi) autonomous systems; (3) vehicle health monitoring and vehicle health management; and (4) safety research relative to aircraft control systems. One of the key technical challenges to realizing NextGen involves verification and validation of complex flight-critical systems with a focus on promoting reliable, secure, and safe use for NextGen operations. As the complexity of systems increases, costs related to verification and validation and safety assurance will likely increase the cost of designing and building next-generation vehicles. The broader aeronautics community has identified verification and validation methodologies and concepts as a critical research area [20].

The goals of research in verification and validation of aviation flight-critical systems include providing methods for rigorous and systematic high-level validation of system safety properties and requirements from initial design through implementation, maintenance, and modification, as well as understanding tradeoffs between complexity and verification methods for supporting robustness and fault tolerance. Some of the control engineering challenges include:

- Large-scale, real-time, deterministic robust or stochastic optimization algorithms;
- Multiple-objective, multiple-stakeho lder optimization frameworks;
- Design of automation with graceful degradation modes;
- Safety diagnosis/health monitoring methods;
- System architectures that facilitate distributed decision making;
- Data fusion from heterogeneous sensors and assessment of the value of the derived information.

(c) Smart Grid and Renewable Energy

Smart grid and renewable energy research and development has been in the forefront of public interest and is therefore a high priority for policy makers. The goal is to improve energy efficiency by investing in modernization of the energy infrastructure. The geopolitical drivers for renewable energy and smart grids are that (1) electricity demand is expected to increase more than 75% by 2030; (2) generation of electricity contributes to more than 40% of greenhouse gas emissions; (3) the cost of generating 1 KWh is four times greater than the cost of saving 1 KWh. Government funding agencies have partnered with industry, utilities, and local government in technology development and demonstration projects dealing with smart grids. For example: Energy Smart Florida is a groundbreaking public/private alliance of the City of Miami, Florida Power and Light, General Electric, Silver Spring Networks, and Cisco. This project is using federal economic stimulus funds as part of an $800 million investment in smart grid technology and renewable energy over the next two years. An estimated 4.5 million smart meters will be installed in U.S. homes and businesses to develop and demonstrate technology for demand management, distribution automation, substation intelligence, distributed generation and information technology. The goal is to demonstrate the increase in energy efficiency through demand optimization and distributed automation by significantly reducing peak load. Advances in flexible AC transmission devices (FACTS) and phasor measurement units (PMUs) have opened new opportunities for wide-area control of smart grids. The U.S. Department of Energy-sponsored North American SynchroPhasor Initiative (NASPI) has been heavily investing in PMU hardware. Future efforts will be needed to focus on data fusion and analysis for real- time dynamics monitoring, prediction, and system control. With increased reliance on wide-area communications and control to improve system operation, tight coupling is needed between cyber systems and the components of physical systems in smart grids. Critical gaps and shared challenges pertain to advances in system science, particularly hybrid digital-analog systems, complex emergent systems, and advanced software systems for large-scale time-varying, geographically distributed systems. Advances in optimization of multiscale stochastic dynamic systems as well as in distributed control are necessary to improve smart grid performance with respect to security, efficiency, reliability and economics. These issues have been identified by the research community in several workshops dealing with information technology and smart grids.

Conclusion

Cyber-physical systems are expected to play a major role in the design and development of future engineering systems with new capabilities that far exceed today's levels of autonomy, functionality, usability, reliability and cyber security. Advances in CPS research can be accelerated by close collaborations between academic disciplines in computation, communication, control, and other engineering and computer science disciplines, coupled with grand challenge applications. Standardized abstractions and architectures that permit modular design and development of cyber-physical systems are urgently needed. CPS applications involve components that interact through a complex, coupled physical environment. Reliability and security pose particular challenges in this context - new frameworks, algorithms, and tools are required. Future cyber- physical systems will require hardware and software components that are highly dependable, reconfigurable, and in many applications, certifiable and trust-worthiness must also extend to the system level.

References

[1]. F.M. Zhang, K.Szwaykowska, W. Wolf, and V. Mooney, Task scheduling for control oriented requirements for Cyber-Physical Systems, in Proc. of 2008 Real-Time Systems Symposium, 2005, pp. 47-56.
[2]. Available at: http://ne wsinfo. nd.ed u/news/17248-nsf-fund s-cyber-p hysica l-syste ms-projec t/.
[3]. J. Sprinkle, U. Arizona, S. S. Sastry, CHESS: Building a Cyber-Physical Agenda on solid foundations, Presentation Report, Apr 2008.
[4]. Available at: http://cpsc hina.org/.
[5]. Available at: http://www.jia fuwa n. net/gdcps. html.
[6]. J. Z. Li, H. Gao, and B. Yu, Concepts, features, challenges, and research progresses of CPSs, Development Report of China Computer Science in 2009, pp. 1-17. [7] R. Rajkumar, CPS briefing,‖Carnegie Mellon University, May 2007.
[8]. B. H. Krogh, Cyber Physical Systems: the need for new models and design paradigms, Presentation Report, Carnegie Mellon University.
[9]. B. X. Huang, Cyber Physical Systems: A survey, Presentation Report, Jun 2008.
[10]. L. Parolini, N. Toliaz, B. Sinopoli, B. H. Krogh, A Cyber-Physical Systems approach to energy management in data centers, in Proc. of First International Conference on Cyber- Physical Systems, April 2010, Stockholm, Sweden.
[11]. L. Carettoni, C. Merloni and S. Zanero, Studying bluetooth malware propagation: The bluebag project,‖ IEEE Security & Privacy, vol. 5, no. 2, pp. 17–25, 2007.
[12]. A. Galante, A. Kokos and S. Zanero, Bluebat: Towards practical bluetooth honeypots, in Proceedings of IEEE International Conference on Communicatio ns, ICC 2009, Dresden, Germany, 14-18 June 2009. IEEE, 2009, pp. 1–6.
[13]. S. Zanero, Wireless malware propagation: A reality check,‖ IEEE Security & Privacy, vol. 7, no. 5, pp. 70–74, 2009.
[14] P. M. Comparetti, G. Salvaneschi, E. Kirda, C. Kolbitsch, C. Kruegel S. Zanero, Identifying dormant functionality in malware programs, in 31st IEEE Symposium on Security and Privacy, 2010, 16-19 May 2010, Berleley/Oakland, California, USA. IEEE Computer Society, 2010, pp. 61–76.
[15]. D. Antoniades, I Polakis, G. Kontaxis, E. Athanasopoulos, S. Ioannidis, E. Markatos, and T. Karagiannis,web: The web of short URLs in WWW 2011.
[16]. S. Zanero and G. Casale, Gives: integrity validation for grid security,‖ IJCIS, vol. 4, no. 3, pp. 319–333, 2008.
[17]. F. Maggi and S. Zanero, Rethinking security in a cloudy world, Politecnico di Milano, Tech. Rep. TR-2010-11,2010, http://home.dei.polimi.it/fmaggi/downloads/publications/2010 maggi zanero cloud security.pdf.
[18]. President's Council of Advisors on Science and Technology, Leadership Under Challenge: Information Technology R&D in a Competitive World [Online], Aug 2007, Available at http://www.nitrd.gov/Pcast/reports/PCAS T-NIT-FINAL.pdf.
[19]. Networking and Information Technology Research and Development Program. High- Confidence Medical Devices: Cyber-Physical Systems for 21st Century Health Care [Online], Feb. 2009. Available at http://www. nitrd. go v/Abo ut/Med De vic e-FINAL1-web.pdf
[20]. NationalScience and Technology Council., National Aeronautics Research and Development Plan [Online], Feb.2010.