

A large American flag is shown waving in the wind, positioned at the top of the page. The flag features the stars and stripes of the United States flag.

Workshop on Future Directions in Cyber-Physical Systems Security

Final Report

January 2010



**Homeland
Security**

Dr. Nabil Adam
Infrastructure & Geophysical Division
Science and Technology Directorate

Table of Contents

Section	Page
1 Introduction.....	1
1.1 Workshop Objectives.....	1
1.2 Workshop Venue and Program.....	3
2 Energy Sector—Electric.....	5
2.1 Environment.....	5
2.1.1 The Electric Grid Today	5
2.1.2 The Smart Grid	6
2.2 State of the Art	7
2.3 Challenges and Recommendations.....	10
3 Water Sector.....	13
3.1 Environment.....	13
3.2 State of the Art	14
3.3 Challenges and Recommendations.....	15
4 Chemical Sector.....	18
4.1 Environment.....	18
4.2 State of the Art	19
4.3 Challenges and Recommendations.....	20
5 Transportation Sector—Aerospace.....	24
5.1 Environment.....	24
5.1.1 Airplane Assets Distribution Systems (AADSs)	24
5.1.2 Airborne Ad Hoc Networks for Real-time Information Sharing.....	24
5.2 State of the Art	25
5.3 Challenges and Recommendations.....	25
6 Healthcare and Public Health—Medical Devices	30
6.1 Environment.....	30
6.2 State of the Art	31



Section	Page
6.3 Challenges and Recommendations	32
7 Commercial Facilities—Buildings.....	33
7.1 Environment.....	33
7.2 State of the Art.....	34
7.3 Challenges and Recommendations	34
8 Conclusions.....	36
8.1 State of the Art in CPS Security.....	36
8.2 Challenges	37
8.3 Recommendations.....	38
9 Acronyms and Abbreviations.....	42
10 References.....	44
Appendix A. Workshop Announcement and Agenda.....	A-1
Appendix B. Invited Talks	B-1
Appendix C. Panel Presentations.....	C-1
Appendix D. Working Group Presentations.....	D-1
Appendix E. Position Papers	E-1
Appendix F. Biographies of Speakers and Chairs.....	F-1
Appendix G. Workshop Registrants	G-1

Acknowledgments

Thanks to the workshop attendees and to those who served on the workshop's Program Committee, all the workshop speakers, panelists as well as the breakout sessions chairs/co-chairs. Thanks also to the individuals who served as this report's core writing team:

- Dr. K. P. Ananth, Idaho National Laboratory
- Dr. Calvin Jaeger, Sandia National Laboratories
- Dr. Insup Lee, University of Pennsylvania
- Dr. Scott Lintelman, Boeing
- Dr. Raj Rajkumar, Carnegie Mellon University
- Dr. William H. Sanders, University of Illinois at Urbana-Champaign
- Dr. Basit Shafiq, Rutgers University



We would like to acknowledge the support received from three members of the DHS Science and Technology Directorate's (S&T's) Infrastructure and Geophysical Division (IGD): Mr. Christopher Doyle, IGD Director; Mr. Lawrence Skelly, IGD Deputy Director; and Dr. Mary Ellen Hynes, IGD Director of Research, DHS. We would also like to acknowledge the comments and feedback from Mr. Philip Reiting, Deputy Undersecretary of National Protection & Programs Directorate (NPPD), DHS and Director of National Cybersecurity Center; Mr. Gregory Schaffer, Assistant Secretary for Cybersecurity and Communications, DHS; Mr. Norman (Kurt) Fosmire, Senior Program Analyst NPPD/IP, DHS; Ms. Christine Adams, Senior Information Systems Manager, The Dow Chemical Company and Operating Officer, Chemical Information Technology Council; Mr. Clyde Miller, Director Corporate Security, BASF and Chairman of Chemical Sector Coordinating Council; Mr. William Schweigert, Commercial Facilities Sector NPPD/IP, DHS; Ms. Alyssa Marlow, DHS; Dr. Nitin Natarajan, Coordinating Director HHS/ASPR/OPEO; and Ms. Cheryl Santor, Information Security Manager, Metropolitan Water District of Southern California.

Finally, we wish to thank Mr. Ron Bilbrey, Booz | Allen | Hamilton, for helping with all related details, including the logistics of the entire workshop and follow-up meetings; Ms. Kate E. Caballero Horanburg, Booz | Allen | Hamilton, for supporting the workshop, creating the survey, compiling the survey results, writing the survey analysis report, and organizing and assembling this report's various sections; Mr. John Galmiche, Booz | Allen | Hamilton, for his support to the core writing team; Mr. Michael Ciccarello and Mr. Ajmal Aziz, Booz | Allen | Hamilton, for their help with the breakout session report; and Mr. Paul Stregovsky, BayFirst Solutions, LLC, for his technical edit and desktop publishing of this report.

Dr. Nabil R. Adam (Program Chair),
Science and Technology Directorate,
U.S. Department of Homeland Security



1 Introduction

The Department of Homeland Security (DHS)'s Science and Technology Directorate (S&T) hosted a "Future Directions in Cyber-Physical Systems Security" workshop, July 22–24, 2009. The workshop was cosponsored by the National Institute of Standards and Technology; the Department of Energy; the Department of Defense; and the U.S. Air Force (Operations, Plans & Requirements; Logistics, Installations, & Mission Support).

1.1 Workshop Objectives

The objective of the workshop was to provide a forum for researchers, subject matter experts, and practitioners dealing with cyber-physical systems security to assess the current state of the art, identify challenges, and provide input to developing strategies for addressing these challenges. Six specific infrastructure sectors were considered:

- Energy—Electricity
- Chemical
- Transportation—Aerospace
- Water—Drinking Water/Wastewater
- Healthcare and Public Health—Medical Devices
- Commercial Facilities—Buildings.

The focus of the workshop was on the security of cyber-physical systems. A cyber-physical system (CPS) is a system of systems where there is a tight coupling between the computing component of the system and the physical components, underlying processes, and policies governing these systems. "Cyber-Physical Systems" is an evolving area that is an important and distinct part of the cyber infrastructure. Cyber-physical systems are prevalent in almost all infrastructures, including transportation; chemical, water, and wastewater; healthcare; and energy. Given current trends, it is clear that we are moving toward "smart" infrastructures: smart power grid, smart buildings, smart bridges, smart cars, embedded medical devices, and robotic assistance for the elderly. Interconnections created by CPSs form a complex, interdependent system of systems across national and international critical infrastructures. Security threats to CPS pose significant risk to the health and safety of human lives, threaten severe damage to the environment, and could impose an adverse impact on the economy. [24].

An example of CPS is an aircraft, which can be viewed as a CPS whose smart sensor fabrics and on-board networking enable the aircraft to self-monitor its systems and structural health while performing real-time diagnostics and coordination with ground stations. A forward-looking CPS example is that of tele-operational surgical robots that enable a surgeon to remotely perform minimally invasive surgery procedures, using robotic arms.



The most common example of CPS is an industrial control system, which is prevalent in almost every critical infrastructure, including electricity, oil and gas; water; chemical processing; and healthcare. Below is a brief description of industrial control systems.

Industrial Control Systems (ICS)

An industrial control system (ICS) encompasses several types of control system:

- supervisory control and data acquisition (SCADA) systems
- distributed control systems (DCSs)
- programmable logic controllers (PLCs).

SCADA systems are highly distributed systems used for data acquisition and control of geographically dispersed assets. These assets may be scattered over a large area spanning thousands of square kilometers. SCADA systems are used in several critical infrastructures, including electrical power grids, railway transportation systems, water distribution and wastewater collection systems, and oil and natural gas pipelines.

DCSs are used to control manufacturing and production systems that are usually located within the same geographic location. A DCS uses a centralized supervisory control loop to supervise a group of controllers that share the overall tasks of carrying out a localized process, such as water and wastewater treatment, electric power generation, oil refining, chemical processing, food processing, and automotive production.

PLCs are devices used in SCADA and DCS systems to control industrial equipment and processes. In addition, smaller control system configurations for discrete processes such as automobile assembly lines and power plant soot blower controls are accomplished through PLCs.

A key component of both SCADAs and DCSs is a human–machine interface (HMI) that enables operators and engineers to perform such operations as process monitoring, configuring set points, and setting and adjusting controller parameters. For more details on ICS operations and its components, see [24].

Some of the unique characteristics of ICS include [24, 23]:

1. **Physical interaction.** An ICS takes input and possible feedback from the physical environment. Interactions with the physical environment can be complex; consequences can be manifested in physical events.
2. **Distributed management and control.** Large-scale ICSs, as in the case of an electric grid, are interconnected and often managed by multiple autonomous organizations with distributed control.
3. **Real-time performance requirements.** ICS are generally time-critical with real-time requirements for information delivery and system operations.
4. **High availability requirements.** Generally, the processes controlled by ICS are of a continuous nature that cannot tolerate an unexpected system outage.

5. **Legacy systems.** The typical lifecycle of an ICS spans up to several decades, incorporating more legacy systems with proprietary software and communication protocols. In addition, there may not be sufficient computing resources available on such legacy systems. This makes it difficult to retrofit such systems with current security capabilities, and thus makes the overall system more susceptible to security and safety threats.

1.2 Workshop Venue and Program

The workshop was held in Newark, New Jersey on July 22–24, 2009. The New York/New Jersey (NY/NJ) area leads the nation in complex issues affecting certain critical infrastructure facilities, including three sectors: chemical, transportation, and water. New Jersey has one of the highest concentrations of chemical manufacturing plants in the nation. These plants are complex systems that use networks and other information systems to control a physical process. Runaway chemical reactions or incorrectly mixed chemicals can be costly and dangerous, both for operators and for the general public.

Additionally, the NY/NJ region has one of the largest, most advanced transportation systems in the world. This transportation system relies heavily on CPS for the surveillance and control operations of its rails, subways, bridges, and tunnels. The NJ/NY area also represents one of the most complex watersheds in the country and is home to the North American Electric Reliability Corporation (NERC), a New Jersey-based nonprofit corporation whose mission is to ensure the reliability of the bulk power system in North America.

The workshop program comprised a range of sessions:

1. **keynote speeches** by representatives from the DHS, DOD, NSF, DOE, NIST, and the state of New Jersey to discuss their perspectives on cyber-physical systems security.
2. **five panels:** Critical Infrastructure and Key Resources (CIKR) owners/operators and state representatives; industry; sectors, venture capital firms; and NSF/NITRD.
3. **three position-paper sessions**, held in parallel on the 23rd and an additional session on the 24th.
4. **three breakout sessions**, held in parallel on the 23rd and 24th. There were three working groups (WGs) with a diverse group of researchers, practitioners, government agencies' representatives, subject-matter experts, and others from various critical infrastructure sectors, including Electricity; Oil & Gas; the Chemical Industry; Water; Healthcare; and Transportation. Each group had two breakout sessions: one for working groups 1.1, 2.1, and 3.1, the other for working groups 1.2, 2.2, and 3.2. Each workshop participant was assigned to a given breakout session on July 23 and to another breakout session on July 24. The purpose of the group discussions was to help answer six questions:
 - What are the problems/issues/research challenges in the various critical infrastructure sectors related to cyber-physical systems security?
 - Where should the technology and science be in 5 to 10 years?



- Why we are not there now?
- What are some of the challenges that are in the way to be there now?
- Why do we need to be there?
- What legitimate case can be made to justify the needed R&D investments?

The remainder of this report is organized as follows:

Section	Title	Page
2	Energy Sector—Electric	5
3	Water Sector	13
4	Chemical Sector	18
5	Transportation Sector—Aerospace	24
6	Healthcare and Public Health—Medical Devices	30
7	Commercial Facilities—Buildings	33
8	Conclusion	36
9	Acronyms and Abbreviations	42
10	References	44

Finally, a series of appendixes presents the workshop agenda, the main presentations, the panel discussions, the working group sessions reports, and the registered workshop attendees.

We hope these findings and recommendations will help the DHS Science and Technology Directorate formulate sound investment decisions, both near- and long-term, as well as research strategy, plans, and objectives for cyber-physical systems security.

2 Energy Sector—Electric

2.1 Environment

The Energy-Electric sector encompasses the production and distribution of energy in the electric grid and the oil and gas infrastructure. About 90 percent of our electricity is generated primarily from coal, nuclear power, and natural gas; the balance comes from hydroelectric and renewable resources such as solar, wind, and geothermal energy.

The U.S. electric power system is one of the most dependable in the world, serving the vast majority of customers with continuous and uninterrupted supply of electricity with a reliability surpassing 99 percent [38]. High availability and continuous power delivery are crucial for a sustainable economy and a high national standard of living. The Department of Energy (DOE) estimates the annual cost of power outages to be \$25–\$180 billion (10⁹), with approximately 60 percent of the nation’s gross domestic product (GDP) tied to electric power. As shown in Table 2-1, the cost of a power outage for selected commercial customers could range between thousands and millions of dollars.

Business processes/operations affected by power outages	Cost of power outages (per hour)
brokerage	\$6,480,000
credit card	\$2,580,000
airline reservations	\$90,000
telephone ticket sales	\$72,000
cellular communications	\$41,000

2.1.1 The Electric Grid Today

The U.S. electric power grid of today forms one of the largest, most complex systems of systems. It interconnects power generation, transmission, and distribution systems at the local, regional, and national levels. The complexity of the nation’s electric grid is exhibited at the infrastructure level, stakeholder level, and system level.

At the infrastructure level, the U.S. electric grid consists of three interconnected networks. Interconnections are divided into a total of 152 regional “control areas” responsible for the reliable operation of a transmission grid owned by more than 500 independent companies. More than 17,000 generators create electrical power in 10,000 power plants across the country. This power makes its way to homes and business through some 640,000 circuit-miles of North American transmission lines ($\geq 132\text{KV}$), more than 10,000 transmission substations, and more than 2,000 distribution substations. Distributing power through so many nodes is as complex as it sounds.

¹ D. Leiter, “Distributed Energy Resources,” prepared by the U.S. Department of Energy for Fuel Cell Summit IV, May 10, 2000, Washington, DC.



At the stakeholder level, this complexity is illustrated by the fact that power transmission is owned by more than 500 independent companies and generation is supplied by more than 3,000 utilities serving more than 300 million people. Broken down further, 73 percent of customers receive their electric power from 213 stockholder-owned utilities; 15 percent, from 2,000 public utilities run by state, local, or regional government agencies; and the remaining 12 percent, from 930 electric cooperatives. Today’s electric grid has nearly 1,000,000 megawatts (MW) of generating capacity. This power is distributed by more than 250,000 transactions per day on the bulk power market.

At the system level, the electric grid is controlled and operated using energy management systems that rely on SCADA, DCS, PLC, and Remote Terminal Units (RTUs).

Such a complex system of systems is subject to a wide range of vulnerabilities. It is vulnerable to natural disasters (lightning, hurricanes, tornadoes, wind, ice, and fire), to manmade disasters (malicious or accidental), and to aging systems, since many generation and information assets date back to the 1950s and 1960s. As shown in Table 2-2, these vulnerabilities can cause infrastructure failure with consequences ranging from minor to devastating.

Incident	Consequences
Northeast Blackout, August 2003	50 million people were left in the dark, with no power. Cost \$6–\$10 billion to the U.S. economy, including more than \$750 million to New York City.
September 2001	9/11 incident caused a major power outage in Lower Manhattan for 9 days.
Ice storm, January 1998	Left 1.6 million people without power. For some, power was not restored for more than a month.

A deliberate attack could significantly increase the costs listed in Table 2-2, especially an attack against a high-profile target. Several recent reports have called for more robust cyber security for our nation’s electric grid. (See, for example, [39].)

2.1.2 The Smart Grid

With the passage of the Economic Recovery Act and over \$4 billion of funding for “Smart Grid” infrastructure grants, today’s electric grid is evolving into a “Smart Grid.” The Smart Grid, through increased infusion of information technology (IT), makes the electric transmission and distribution network “smart” enough to

- take protective actions to mitigate any local disturbance,
- interact with the control center to generate an accurate state of the system as well as to receive control commands for responding to a global incident, and
- exchange system status information with peer devices, within and across utilities.

By allowing its components to coordinate and interact, the smart grid will make the electric grid vastly more adept. The grid will be

- **smart**, to identify surges, outages, and failure points;
- **resilient**, instantly containing damage and rerouting power around a failure;
- **flexible**, accommodating new off-grid alternative energy sources;
- **reliable**, by providing dynamic load balancing; and
- **secure**, by being less vulnerable to accidental or malicious harms [40, 41, 42].

From the perspectives of consumers, utilities, and operators, benefits will include

- **demand-side load management**. Consumers will have the option to manage their electricity use.
- **savings from reduced interruptions and reduced congestion**. Smart grid upgrades will ease congestion, sending 50 to 300 percent more electricity through existing corridors. Avoided cost savings will be substantial.
- **increased situational awareness** for grid operators.
- **more complete real-time communication** between the utility control centers and the grid.
- **the ability to integrate distributed generation and intermittent renewable generation sources**, such as wind and solar, with storage devices, such as massive electricity storage systems [43].

While the Smart Grid will bring about these extensive benefits, implementing it will not be easy. Its very flexibility will pose significant security challenges due to several factors, including:

- **increased connectivity**, which grants grid access to more entities and the public.
- **sophisticated wireless devices**, such as smartphones, which will be used by nearly everyone, including station workers, delivery vendors, and casual visitors.
- **dynamic interactions** among autonomous systems to support collaborative processes that cut across power generation, transmission, and distribution.

2.2 State of the Art

There has been significant research and development on SCADA systems in the electric sector, and noteworthy progress has been made in identifying and mitigating vulnerabilities under the sponsorship of the Department of Energy (DOE). Examples of such DOE-based initiative are the National SCADA Testbed; funding for research at multiple DOE labs with testbed facilities like the Idaho National Laboratory; modeling and simulation of the grid; phasor (phase vector) measurements; and research and development of the superconducting grid.



NIST is coordinating the development of an interoperability framework for Smart Grid devices and systems. Moreover, NIST has prepared a preliminary list of cybersecurity requirements applicable to the Smart Grid [44]:

- *Recommended Security Controls for Federal Information Systems*, NIST Special Publication (SP) 800-53, provides guidance for Federal agencies on cybersecurity controls. One section specifically addresses industrial control systems.
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Cybersecurity Standards CIP-002 through CIP-009 provide a cybersecurity framework for identifying and protecting Critical Cyber Assets to support reliable operation of Bulk Power System.
- The International Society for Automation (ISA)-99/International Electrotechnical Commission (IEC) 62443 suite of standards addresses Security for Industrial Control Systems.
- A Security task force (AMI-SEC) of the Advanced Metering Infrastructure (AMI) is defining common requirements and produce standardized specifications for securing AMI system elements.

Roadmap to Secure Control Systems in the Energy Sector [45]. Developed in 2006 by an industry, government, and academic group, this roadmap has driven action in the energy sector, guided investments toward a common vision and goals, and accelerated product development to produce tangible results. The roadmap has catalyzed activity that has made the energy sector a model for control systems security and made the sector more resilient and secure. It is now being revised to reflect insights gained from events of the last 3 years.

In addition to the roadmap, three academic research efforts aim to make the power grid more resilient:

- Trustworthy Cyber Infrastructure for Power (TCIP)
- Team for Research in Ubiquitous Secure Technology (TRUST)
- CRITICAL UTILITY InfrastructureAL resilience (CRUTIAL).

They are briefly described below, using material drawn from their Web sites.

Trustworthy Cyber Infrastructure for Power (TCIP) [46]. Researchers from the University of Illinois at Urbana-Champaign, Dartmouth College, Cornell University, and Washington State University are together addressing the challenge of how to protect the nation's power grid by significantly improving the way its infrastructure is built, making it more secure, reliable, and safe. Funded by the National Science Foundation (NSF), with support from the Department of Energy and the Department of Homeland Security, the project recognizes that today's quality of life depends on the continuous functioning of the nation's electric power infrastructure. This continuity, in turn, depends on the health of an underlying computing and communication network infrastructure that is at serious risk from both malicious cyber attacks and accidental failures. Some of these risks may come from cyber hackers who gain access to control networks or create deni-

al-of-service (DOS) attacks on the networks themselves. Other risks arise from accidental causes, such as natural disasters or operator errors.

TCIP's research plan is focused on securing the low-level devices, communications, and data systems that make up the power grid to ensure trustworthy operation during normal conditions, cyber attacks, and power emergencies:

- **At the device level**, new key functionality is being designed into hardware to detect attacks and failures and to restore proper system operation. Likewise, virtual machine technology is being developed and adapted for advanced power meters to permit new power-use scenarios while preserving privacy.
- **At the protocol level**, new techniques are being developed to detect, react to, and recover from cyber attacks that occur while preserving integrity, availability, and real-time requirements. Moreover, lightweight authorization and authentication techniques are being developed that can react quickly in an emergency. Simulation and evaluation techniques are also being used to analyze real power-grid scenarios and validate the effectiveness of the TCIP designs and implementations.
- **In outreach efforts**, TCIP has developed interactive and open-ended applets for middle-school students, along with activity materials and teacher guides, to facilitate the integration of research, education, and knowledge transfer by linking researchers, educators, and students.

Impacts are being made at all levels in the project:

- **At the device level**, attested meters have been developed that provide the advanced features needed for energy control, while ensuring appropriate access control and also preserving customer privacy. Hardware support has been developed to support application-aware detection and recovery mechanisms in power system devices. Likewise, secure coprocessors have been developed to perform efficient cryptographic computations to facilitate communications between substations and control centers on the grid.
- **At the network level**, protocols are being developed to provide efficient, timely, and secure publishing of and subscription to process control system data; to support secure and timely data and resource aggregation in process control systems; and to provide federated identity management, access management, and trust negotiation for the grid. These protocols are being designed with next-generation communication and control requirements in mind, providing the building blocks for a more robust, secure, timely, and adaptive grid infrastructure.
- **To make simulation and testing more realistic**, TCIP researchers have developed a combined simulation/testbed environment that mimics specific aspects of the IT infrastructure of the power grid accurately, while being scalable.

Together, these innovations provide a clear direction toward a next-generation IT infrastructure for the power grid, an IT infrastructure that is reliable, timely, secure, and able to support the continuous functioning of the nation's electric power infrastructure.



Team for Research in Ubiquitous Secure Technology (TRUST) [47] was established as a National Science Foundation Science and Technology Center to develop cybersecurity science and technology that will radically improve the ability of organizations to design, build, and operate trustworthy information systems for the nation's critical infrastructure. The center addresses technical, operational, privacy, and policy challenges through interdisciplinary projects in three infrastructure areas: financial infrastructure, health-care infrastructure, and physical infrastructure.

The TRUST physical infrastructure area focuses on SCADA and other network embedded systems that control critical physical infrastructures (for example, power grid, gas distribution, water distribution, and transportation) and futuristic infrastructures, such as "smart" buildings and structures—for example, active bridges whose structural integrity depends on dynamic control or actuators. For these systems, TRUST researchers are addressing challenges related to ownership and control of the physical infrastructure (whether it is individuals inside their homes or the grid utility provider), availability, integrity, and data privacy.

CRITICAL Utility InfrastructurAL resilience (CRUTIAL) [48] focuses on new networked information and communication technology (ICT) systems for managing the electric power grid. In this context, CRUTIAL project aims to

- develop modeling approaches for understanding the various interdependencies within and across electrical utilities infrastructures,
- investigate distributed architectures that would allow the power grid to be dependably controlled and managed,
- analyze scenarios in which a fault or disruption in the information infrastructure would seriously affect the electric power infrastructure, and
- develop a testbed that integrates the electric power system and information infrastructure.

2.3 Challenges and Recommendations

From a science and technology perspective, the control systems of the future need to be designed, installed, operated, and maintained to survive a natural disaster, human error, or intentional cyber attack with no loss of critical function. This is no small challenge in the energy—electric sector, a sector that is complex and highly networked, presenting a variety of access points. Also, any disruption to the electric sector have cascading effects on other sectors, increasing the premium placed on protection. To make these systems resilient, research must integrate an understanding of cybersecurity, human interaction, and complex network design to address the threats. Among other efforts, this research should include work in data fusion, mixed initiative control, and hierarchical control system design.

Data fusion plays a significant role in tailoring information to the user. It provides a broader state awareness for effects caused by a cyber attack or malicious action. Data fusion technology can also integrate diverse forms of data that allow contrast or variations from normalcy to be recognized. With highly integrated combinations of multiple

control systems, data fusion research is needed to quickly recognize human error or malicious cyber attack that can prevent an unacceptable negative impact cascading to multiple process systems. Mixed initiative control could provide an optimized combination of automation versus human response to achieve the most resilient reaction from both. Humans can be more effective at recalibrating response to changing environments, but must be effectively modeled to ensure the proper integration with automation. A mixed initiative framework is needed that would provide mechanisms to integrate automation and human response in an optimized manner, taking benefit from the inherent resilience in both.

As technologists and policy makers work to create smart grid technologies, a number of challenges need to be addressed. The following three are of particular relevance:

Challenge 1: Cybersecurity aspects in the smart grid are wide and varied. We must develop hardware-based security mechanisms, authentication techniques and protocols, and timely and secure communication and control networks. We must develop detection and response mechanisms and robust cybersecurity protection mechanisms. We must find ways for smart grid components and subsystems to be securely integrated into legacy architectures. Many functions enabled by adding smart grid components have yet to be defined, let alone standardized. For example, access to meters being placed on all residences and in multi-resident complexes could enable cyber-physical attacks even with the traditional barrier protections of fences, gates and surveillance.

Recommendations:

1. Develop and execute a coordinated research program to develop security mechanisms for the electricity-electric sector, one that considers everything from individual hardware and software components to the end-to-end resilience of specific functionality of the smart grid.
2. Appropriately integrate protection, detection, and response mechanisms to construct a grid that is resilient to both accidental failures, malicious attacks or manipulations, and surreptitious monitoring.

Challenge 2: Global vs. local stability. Instead of a regulated utility environment with well-trained support staff, the interactions have now extended down to the individual consumer or local installer. In addition, national versus local priorities may exist between the operation of the bulk power grid and microgrids, which are tailored to support a small region. The outcome of these differences can lead to adjustments in resources to favor individual or regional interests and not resilience of the grid as a whole of the whole.

Recommendations:

1. Develop new economic–technical analysis and control methods that align individual interests with those of the grid as a whole.
2. Develop the science needed to ensure that these methods remain stable and produce desirable control outcomes.

Challenge 3: Distributed power generation. The incorporation of distributed power generation from renewable resources (for example, wind, photovoltaics) into the grid and



the associated control systems is a research area of growing importance. Because most renewable generation sources are non-dispatchable, new controls and complex balancing schemes are required. Moreover, the hierarchy of integrating distributed generation resources with the bulk power grid is ill-defined. Furthermore, grid energy storage technologies have not been deployed in a manner that suggests successful migration to achieve the goal of penetration in the market by renewables up to 20 percent.

In addition to these technology-related challenges, legal and policy issues must be addressed. For example, assuming the “grid” can utilize or draw power from the generating or storage units of individuals or private entities, who will bear the legal liability to the equipment damages? Who will pay the cost associated with operating and maintaining such equipment?

Recommendations:

1. Develop control and load-balancing schemes that are applicable to systems a large fraction of whose power comes from distributed and renewable resources. In doing so, include the predictive modeling and situational awareness beyond information provided by metering data and phasor measurements. To address the inherent variability of renewable energy generation, develop effective grid energy-storage technology.
2. Address the legal liability and policy issues related to receiving power from individuals and private entities.

3 Water Sector

3.1 Environment

The water sector encompasses reservoirs and supply systems for drinking water as well as wastewater utilities. In the United States, there are approximately 160,000 public water systems serving about 250 million people and more than 16,000 wastewater utilities serving more than 225 million people [29, 30]. In addition to providing a safe potable water supply and wastewater treatment, these utilities provide services essential to other sectors during emergency response efforts, including a water supply for fire protection and essential services to recovery areas impacted by natural or manmade disasters.

According to the Water Resource Foundation, the revenues in the U.S. water industry are estimated to exceed \$150 billion a year. The key driving factor to this growth is the aging infrastructure in the water sector, causing failures and disruptions in the water supply system. The U.S. Environmental Protection Agency (EPA) estimates that 240,000 water mains break nationwide every year [31].

Utilities in the water sector rely on both SCADA and DCSs for their operations related to source monitoring, treatment, storage, and subsequent distribution of treated water to consumers. As discussed in Section 1, SCADA is used in the water sector for drinking water distribution and wastewater collection and DCS is used in drinking water and waste water treatment processes [24].

ICSs in water sector utilities often include wireless communication to link the monitoring system and controls for the treatment and distribution systems to a central display and operations room. In addition, the ICS components communicate over short- and long-range paths, including the Internet, public telephone systems, and common wire. And as businesses increasingly demand real-time information to support decisions, ICSs are increasingly connected to a company's enterprise system. This elevated interconnectivity, and the use of shared media for process control and business functions in the water sector, have made ICS increasingly accessible and introduced cyber-physical systems to new security vulnerabilities, including interconnection-caused vulnerabilities (viruses, worms, hackers, and terrorists) [29,30].

In some facilities, systems could be manually operated if the automated system suffers a failure or is compromised. However, the increased automation makes it challenging to have enough personnel to switch to manual operations if there is a cyber-physical security incident [32].

Any exploitation of these vulnerabilities, whether maliciously or inadvertently, can cause a failure or disruption of water system operations, which in turn may result in human health impacts, loss of life, public endangerment, environmental damage, loss of public confidence, or severe economic damage. Two example scenarios illustrate how a vulnerability, if exploited, could seriously affect a water system [29,32]:



- By breaching or disabling a SCADA or DCS system of a water utility, an intruder could introduce either dangerously high (or inadequate) levels of chemicals, to reduce biological treatment levels, to change alarm thresholds, to reduce pressure flows of water into fire hydrants, and/or to discharge of untreated or undertreated sewage.
- Someone could block data or send false information to operators to prevent them from being aware of conditions or to initiate inappropriate actions.

Publicly reported system failures and cyber attacks on the U.S. water sector are illustrated by three examples:

- **Taum Sauk Water Storage Dam failure.** In December 2005, an error in the remote monitoring of the water level in the Taum Sauk Water Storage Dam resulted in the release of a billion (10^9) gallons of water [24].
- **Hacking of the California canal management system.** A former employee of a small California canal system installed unauthorized software, damaging the computer used to divert water from the Sacramento River [33].
- **Malicious software implanted in a water treatment system in Harrisburg, PA.** A hacker broke into a water filtering plant through the Internet and planted malicious software that was capable of affecting the plant's water treatment operations [34].

3.2 State of the Art

Cyber-security self-assessment tool. In 2007, DHS and Idaho National Laboratory (INL) completed the development of a control systems cybersecurity self-assessment tool for use by water sector utilities in collaboration with the Water Environment Research Foundation and American Water Works Association (AWWA) Research Foundation. The plan is to use this tool along with the national, recommended roadmap implementation efforts to increase cyber-security awareness among utilities' owners and operators.

Risk Assessment Tools. A set of risk assessment guidelines and tools have been developed for the water sector and supported by EPA funding or by others. These risk assessment guidelines and tools include [30]

- Risk Assessment Methodology for Water Utilities
- Risk Assessment Methodology for small and medium utilities
- Vulnerability Self-Assessment Tool for water, wastewater, and water/wastewater systems
- Security and Emergency Management Systems
- Security Vulnerability Self-Assessment Guide for small drinking-water systems serving populations of 3,300 to 10,000

- *Security Vulnerability Self-Assessment Guide* for very small drinking-water systems—those serving populations smaller than 3,300
- *Automated Security Survey and Evaluation Tool* for small drinking water systems
- *Protecting Your Community’s Assets: A Guide for Small Wastewater Systems*.

Water/Wastewater Agency Response Network. Mutual aid and assistance agreements have been established among utilities under the Water/Wastewater Agency Response Network (WARN) initiative [35]. This initiative is spearheaded by the water sector’s professional associations, state primacy agencies, and EPA. WARN aims at enabling utilities to collaborate when dealing with damages from natural or manmade incidents. Through this network, water sector utilities can receive temporary aid for rapid restoration of critical operations. This aid can be in the form of personnel, equipment, materials, and other associated services.

SCADA Guidelines and Standards. Recent efforts [35] provide guidelines for SCADA-specific security policies. However, the recommendations address control system problems of a general nature; there is a need for local, state, and federal laws and regulations to be reviewed for each particular industry and control systems.

3.3 Challenges and Recommendations

Challenge 1: Increased automation, connectivity, and accessibility. Many of the current water-sector systems are being operated in new ways that were never intended when the systems were designed and built. For example, these systems have increased connectivity and increased levels of automation and remote access to users for equipment maintenance and software updates (by manufacturers and suppliers) and for system operations. In addition, these systems are increasingly connected to a company’s enterprise system because of increasing demands for real-time business information. Additionally, as water sector systems continue to be built and modified, they are becoming increasing more complex, with more operating systems and equipment and increased opportunities for security issues. Consequently, they are more prone to fail from cyber attacks, unanticipated interactions among the components, and vulnerabilities in the operating systems and application software.

Recommendations:

1. **Develop self-healing architectures and methodologies** to enable fully automated security-state monitoring with real-time remediation that minimizes the adverse impact on the overall system reliability, availability, and safety.
2. **Develop components and architectures** with built-in, end-to-end security
3. **Develop automatic contingency and remedial actions** that would “kick in” in response to attempted intrusions.

Challenge 2: Verification and validation of interconnected and interacting ICS components for the overall process. As the automation, connectivity, and accessibility of the control process increase, it becomes more and more difficult to verify the interactions among the different ICS components with respect to the operational, safety, and security prop-



erties of the overall process. These interacting ICS components encompass cyber components and physical components with different models for safety and security verification.

Recommendations: Develop models, theories, and tools that account for a system's cyber and physical components in an integrated, unified way. By considering both the continuous and discrete aspects such models and tools, developers would enable:

- the analysis and design of the ICS
- consequence analyses of interdependencies and potential cascading effects across related processes (for example, source water monitoring, raw water treatment, water distribution, and wastewater treatment).

Challenge 3: Consequence analysis of cyber-physical attacks. In the water sector, underlying processes are complex; systems span a wide geographical region; and facilities are owned and managed by multiple autonomous operators/stakeholders. There needs to be a deep, detailed understanding of the consequences of physical or cyber attacks on the drinking water supply sources and infrastructure.

Recommendations:

1. Create a testbed, similar to the Electric Grid testbed at Idaho National Laboratory, to provide a controlled environment where we have access to the ground truth (for example, stress level, risk, interdependency, component interactions). This testbed would enable the vulnerability of SCADA systems to be assessed by replicating a multitude of control system specifications and running simultaneous cyber-physical attacks on multiple systems.
2. Model and simulate the underlying processes and systems; collect data about these processes and systems and manage them.

Challenge 4: Risk management. Currently, risk management for the water system, including the ICS, is generally performed at the component level. No integrated cyber-physical systems approach exists. Furthermore, there are no common metrics for benchmarking ICS risk.

Recommendation: Develop a cross-disciplinary, enhanced risk-assessment tool for owners and operators. Tools are also needed for security management for an ICS event. Additionally, there is a need for the establishment of performance metrics and tools to evaluate the systems.

Challenge 5: Overall system resilience.

Recommendations:

1. In the near term, making the water system more resilient will require immediate response or timely remediation. Development of adaptive CPS architectures that can ensure resilience in an environment of multiple, dynamic threats is also needed. ICSs should be capable of self-diagnosis coupled with real-time monitoring and alerting and self-configuration/healing, as applicable. If any ICS patching is required, the time to perform these activities must be significantly reduced.

2. Future water systems and ICSs should be designed and installed such that critical functions can continue to be performed during and after a cyber-physical event. This approach will require a comprehensive understanding of the total system (for example, physical, cyber, operations) and identification of critical components, critical systems, connectivity, and impacts from cyber events. The establishment of performance metrics and tools to evaluate the systems are needed.



4 Chemical Sector

4.1 Environment

Chemical facilities manufacture a host of products and represent a very diverse sector with regards to process types and facility sizes. The sector can be divided into five major segments:

1. basic chemicals
2. specialty chemicals
3. agricultural chemicals
4. pharmaceuticals
5. consumer products.

Overall, these segments convert various raw materials into more than 70,000 diverse products, many of which are critical to the health and well-being of the nation's citizenry, security, and economy [6].

The chemical sector generates revenues of more than \$637 billion per year and employs nearly 1 million people [4].

Cyber-security requirements within the chemical sector encompass both information and process control security. The industrial control systems (ICSs) perform various functions and exist at different stages of evolution throughout the chemical sector. In the chemical sector, mainly distributed control systems (DCSs) are used to control chemical manufacturing and production systems. These systems are usually located within a more confined factory or plant-centric area [24]. SCADA systems are likewise used for monitoring and supervisory control in the pharmaceutical and petrochemical industries. However, unlike power grid or water distribution systems, monitoring and supervisory control in the chemical industry is limited to a relatively small area, usually within the physical boundaries of a chemical plant. Moreover, the industrial control systems across chemical plants or facilities are not interconnected. Therefore, an incident in a chemical plant is more likely to affect the site alone, rather than trigger cascading failures across multiple sites [6]. The public and environmental impact may extend beyond the plant to wider geographical areas. For example, the 1984 Bhopal (India) gas tragedy exposed more than 500,000 people to methyl isocyanate gas and other chemicals [50].

Such a lack of interconnectivity, however, does not reduce the danger of accidental or malicious exploitation of the ICS vulnerabilities in the chemical sector. Like controls systems used in other sectors, ICSs in the chemical sector have increased remote connectivity capability over the Internet, public telephone lines, or wireless channels, opening up new vulnerabilities. Remote connectivity is not limited to the control system's operators: It extends to business managers, vendors, engineers, and maintenance personnel [7]. There are connections between older and newer systems. And the chemical

sector's increasing use of commercial off-the-shelf technologies creates potential vulnerabilities at system gaps and interface points.

The chemical sector offers cybersecurity guidance that encourages the separation of ICS from the Internet and corporate information systems to reduce the potential of infiltration from the Internet.

The accidental or malicious exploitation of such vulnerabilities may have a severe impact on the safe operations of the system. For example, an intruder capable of injecting network traffic into the communications stream of a chemical plant ICS might increase the reflux rate and or the steam flow rate of a distillation column, possibly causing the column to flood. Alternatively, the intruder could simply disrupt the normal flow of control traffic through a denial-of-service attack, and thus confuse and easily overload end devices such as remote terminal units (RTUs). Without control, the process might easily become toxic, become explosive, or simply overheat and melt down, resulting in major economic and environmental costs.

The threats to ICSs in the chemical sector are exacerbated by the fact that the raw or finished chemical products may be hazardous. Any incident affecting the processes that uses or produces a hazardous material may have serious consequences to human life, public health, and the environment.

It is important to recognize that the chemical sector uses a defense-in-depth approach to securing the industrial automation and control systems environment. Where the use or production of hazardous materials is involved in a chemical manufacturing process, safety instrumented systems (SISs) are widely used across the sector. When a manufacturing process unexpectedly exceeds its control parameters, the SIS is designed to either safely shut the process down or stabilize the process until it can be brought back into proper operation. These SISs are part of a layered defense approach in the chemical sector. In the event that an SIS fails, the plants also have secondary containment systems designed to trap an unplanned release of product.

4.2 State of the Art

Security Vulnerability Assessment. The chemical sector has a long commitment to safety and hazard analysis. It was one of the leaders in developing security vulnerability assessment (SVA) tools for its facilities. These SVAs considered both physical and cyber threats. These threats could result in a range of undesired events, including the release of a hazardous chemical, the theft of a chemical, and facility sabotage. Under the Chemical Facility Anti-Terrorism Standard (CFATS), a process has been developed to receive information from facilities having hazardous chemicals, placing the facilities into tiers and eventually performing assessments of the most critical facilities. Other SVA tools are being used within the sector against both physical and cyber threats.

Guidelines and best practices. The Chemical Sector Cybersecurity Program has developed a set of guidance documents and white papers by which chemical companies can assess and improve the security of their facilities, plants, and production systems [5]. In addition, several industry organizations and Government organizations have initiated



collaborative programs for developing guidelines, best practices, and standards for industrial control systems security. These collaborative programs include

- the Department of Homeland Security (DHS)-sponsored Industrial Control Systems Joint Working Group (ICSJWG)
- the INL Control Systems Security Center, located at the Idaho National Laboratory (INL) and funded by DHS-Control Systems Security Program
- the National Institute of Standards and Technology (NIST) Process Control Security Requirements Forum (PCSRF)
- the Automation Federation ISA.

Information sharing. The Cybersecurity Program aims to provide a trusted environment for sharing information within the chemical sector about cybersecurity incidents, security vulnerabilities, and security guidelines. Chemical companies can avail themselves of a variety of information-sharing tools and portals, including Business Roundtable’s CEO ComLink, the Homeland Security Information Network–Critical Sectors (HSIN-CS), the United States Computer Emergency Readiness Team (US-CERT), and the Government Emergency Telecommunications Service (GETS). Information-sharing initiatives currently underway include an initiative to establish a cyber crisis communication capability within the chemical sector and a DHS-initiated information-sharing pilot to make it easier for the chemical sector and DHS to exchange information about the impact of cyber vulnerabilities and cyber incidents [5].

National exercises. The chemical sector actively participates in national exercises, including Cyber Storm II, an exercise that enhances the learning of individual companies and reveals the value of a sector-level crisis communication process [5]. The chemical sector is planning to test its cyber crisis communication process and its link to the National Cyber Incident Response Plan during the Cyber Storm III exercise in 2010.

4.3 Challenges and Recommendations

Challenge 1: Risk assessment. Assessment tools that can be easily used by operators to evaluate risks to ICSs and physical systems are not widely available. Some cyber assessment tools provide self-assessment capabilities for cyber systems, but they don’t show how cyber threats relate to the overall system operations and mission. Furthermore, there are no generally agreed-upon metrics for chemical-sector ICSs.

Recommendations:

1. Develop a comprehensive risk assessment tool is needed that looks at the entire chemical facility, all the different systems, and how these systems bear upon system operations, support, and business functions. The DHS-initiated Chemical Facility Anti-Terrorism Standards (CFATS) is a step in this direction [51].
2. Improve risk-assessment tools and provide quantifiable return-on-investment figures for decision makers in security and plant management. These tools must bring together repeatable information, based on scientific and engineering principles, and provide it to decision makers to help them protect system effective-

ness, identify vulnerabilities, and identify possible measures to mitigate the consequences. The assessment tool should be able to address multiple hazards and demonstrate protection strategies and solutions that may apply to both malevolent and natural events.

3. Create risk metrics, together with a means to measure and compare degrees of risk. Risk assessment criteria should be able to evaluate not just the ICS but the overall protection effectiveness of the process or system and its effect on one or more sectors or areas. A study is needed to evaluate how accurately these criteria indicate a plant's "state of security health."

Challenge 2: Design and evaluation of ICS security measures. One risk challenge is somewhat peculiar to the chemical sector: Potential risk is strongly tied to potential hazards of the material and the aggregate value of the material and systems. Thus, for similar ICS functions, grading of the security requirements may need to be based on the potential risk. Risk and consequence should also take into account the potential harm to surrounding ecosystem: the air, water, soil, and wildlife.

Many current ICS security measures were performed after-the-fact to address specific threat tactics or meet other requirements. A limited number of design requirements exist or are in development. ICS developers and owner/operators need more guidelines to help them design security measures into an ICS. The desired end state would have systems and components that are secure-by-design.

Recommendation:

1. Develop approaches for measuring how effectively security mechanisms prevent accidental or malicious exploitation of ICS vulnerabilities and reduce the potential hazards of the underlying chemical products. Given that most ICSs oversee numerous chemicals and compounds, the effectiveness of ICS security mechanisms may need to be evaluated for processes involving selected individual and combined materials with differing hazard levels.
2. Create a testbed, such as the CSSP Control System Analysis Center (CSAC²), for evaluating cyber-physical security. Using this testbed, researchers could
 - replicate the control system specifications and outcomes for a given process,
 - configure and enforce the specified security policies and mechanisms,
 - run simultaneous cyber-physical attacks, and
 - safely analyze the impact of the individual or combined material used in the process that could be stalled, disrupted, or rendered hazardous or contaminated by a cyber-physical attack.

Challenge 3: Security and safety analysis. ICS safety and security analyses have been carried out independently; safety analysis has focused mainly on protecting the technical functions of the system and meeting physical and cyber protection requirements. Current cybersecurity analysis deals mainly with cyber intrusion detection, access control

² not to be confused with DHS S&T's Chemical Security Analysis Center at the Aberdeen Proving Ground, Maryland



enforcement, and network security. For safe ICS operations, a key requirement is to ensure that security policies and mechanisms are properly designed, configured, and enforced to satisfy the system safety and requirements. Currently, there is a lack of unified models and approaches for analyzing security and safety together.

Recommendations:

1. Develop a unified framework for combined analysis of safety and security of ICS. This framework will be useful to
 - identify any possible violation of safety and security properties due to the interplay of system dynamics/control logic and security policies
 - detect incompleteness and vagueness in security policy specifications, and identify security holes
 - detect when a security mechanism has sustained a misconfiguration that may lead the process to an undesirable state.
2. Develop methods to verify, validate, and test security mechanisms in the context of safety verifiability and system functionality.

Challenge 4: The human in the loop. As chemical plant owners and operators strive to safeguard their ICSs, insider threats remain an imposing challenge. As reported by USSS/CERT [8], 87 percent of insider incidents are caused by privileged or technical users. Some of these insider incidents are due to accidental exploitation of ICS vulnerabilities; others are deliberate, planned actions motivated by revenge from disgruntled employees. In the chemical sector, this is a more serious concern: Armed with knowledge of potential hazardous materials, combinations of materials, and the processes in which they are created or used, a malicious insider could attack or disrupt ICS operations. The resulting impact could be grave.

Recommendations:

1. Develop methods and approaches for verifying whether access control policies and mechanisms are properly designed and configured to guarantee that the system is operating safely. In particular, if an action taken by a privileged user could make a system less safe, either accidentally or intentionally, that action must be monitored. Develop methods to identify the times and conditions under which authorized actions are needed or not needed for process control and system operations.
2. Develop methods and approaches by which a user's credentials can be automatically and promptly updated or revoked when his job status changes—for example, when he's hired, reassigned, placed on leave, or terminated.
3. Develop approaches for monitoring the actions of legitimate ICS users and operators and detecting anomalies in their actions.
4. Conduct social science research to better understand work ethics, loyalty, social norms, and motivation for not doing harm. Researchers could start by pulling together behavioral indicators that predict workplace violence.

Challenge 5: Secure information sharing. At the sector and government levels, there are many programs for sharing information about cyber-physical systems vulnerabilities and incidents. But often, plant owners and ICS vendors are reluctant to share such sensitive information with government agencies, competitors, and customers because of security and business concerns.

Recommendation: Develop approaches for security and privacy while fostering an information-sharing environment [9, 10, 11, 12, 13].

Challenge 6: Trusted systems. With the increased reliance on commercial off-the-shelf products for the ICS, there may be cases where the ICS hardware and software may not be developed and built within the United States.

Recommendations:

1. Conduct research to address the development of trusted systems from untrusted components.
2. Develop approaches and methods for testing and evaluation of systems that are made of untrusted components or interact with other systems in an untrusted environment.



5 Transportation Sector—Aerospace

5.1 Environment

Cyber-physical systems (CPSs) in the aerospace domain leverage new networking and information technologies to sense properties of the physical world and to tightly control physical assets. For example, under next-generation Air Traffic Management (ATM) systems, each airplane could compute its real-time location using Global Positioning System (GPS) sensors and transmit this information to ATM ground stations [26]. The airplane itself can be viewed as a CPS where smart-sensor fabrics and on-board networking enable the airplane to self-monitor its systems and structural health and to perform real-time diagnostics and coordination with ground stations [21, 26].

To illustrate the issues and challenges related to CPS security in the aerospace environment, let us consider two related applications:

- airplane assets distribution system (AADS)
- airborne ad hoc networks for real-time information sharing.

5.1.1 Airplane Assets Distribution Systems (AADSs)

AADSs deals with the electronic distribution of airplane information assets such as loadable software and airplane health data [21]. Such information asset distribution takes place throughout the airplane's lifecycle, including development, assembly, testing, use, and resale. It is the responsibility of the AADS to securely distribute the information assets from source to destination in the presence of an adversary. In the course of this asset distribution, the AADS interacts with several entities, including suppliers, manufacturers, airlines, servicers, and airplanes. The nature of this interaction, the distribution path, and the underlying asset to be distributed all vary with the airplane's lifecycle state. Typically, the software distribution process relies on the supplier to distribute the software to the airframe manufacturer or to the airline. The deployed airplane interacts with the ground systems of the airline or its contracted services to receive the software, which is then installed into a destination line replaceable unit by maintenance personnel.

During the software and data distribution phase, an adversary could attack the AADS, causing significant safety hazards and unwarranted flight delays. An attack may be come in the form of software tampering, software misconfiguration, software diversion to unsuitable recipient, unnecessary software updates, or delaying of a critical software update [21].

5.1.2 Airborne Ad Hoc Networks for Real-time Information Sharing

Aircraft-to-ground infrastructure (A2I) and aircraft-to-airplane (A2A) communications allow airplanes to form an airborne ad hoc network [26]. This airborne network can be used for real-time sensing and sharing of onboard health diagnostics with aerospace engineers and equipment suppliers for enabling proactive airplane maintenance and

airplane health management. In addition, this capability can significantly improve air traffic management, specifically airborne navigation and ground surveillance of air traffic.

With open networked systems, the threats for data and onboard system security remain real and raise several concerns about aircraft safety and airline business disruptions.

5.2 State of the Art

The state of the art in the CPS security in aerospace consists of the following:

1. **protocols and standards** for low-level data transfer and network security
2. **safety standards and regulations for development and delivery of software** (for example, RTCA DO-178B). However, safety and security must be considered together throughout the software development and delivery process to improve the safety of the overall system. In this context, safety implies functional software correctness; whereas, security analysis deals with non-functional properties, such as authorization, authentication, and the integrity of information assets.
3. **ongoing development of a data format in ARINC 827** for the electronic delivery of signed loadable software and related information exchanged between ground systems and aircraft
4. **guidance material**, developed by the International Civil Aviation Organization (ICAO), for an aeronautical telecommunication network which includes air-to-ground infrastructure communications [20]. The current network is based on the Internet Protocol (IP) networking standard. IPv6 security issues are being considered as an integral part of the guidance.
5. **participation by the CPS community in a recent workshop** by NSF HCSS, University of Washington, Boeing, and Ford. The resulting report outlined CPS research directions unique to aerospace as well as directions common to the aerospace and automotive sectors [2]. Their report identified CPS security as a “grand challenge.”
6. **guidance and regulations for continued airworthiness** that have begun to cover security threats to the aircraft onboard systems and information assets. Two FAA regulations serve as examples:
 - Federal Aviation Administration, 14 CFR Part 25, *Special Conditions: Boeing Model 787–8 Airplane; Systems and Data Networks Security—Protection of Airplane Systems and Data Networks From Unauthorized External Access*.
 - Federal Aviation Administration, *Airworthiness approval and operational allowance of RFID systems*, FAA Advisory Circular AC No: 20-162.

5.3 Challenges and Recommendations

Challenge 1: Security and safety interplay. An emerging concern in aerospace CPS is that security concerns affect system safety, especially in emerging network applications on which future CPS will depend for safe operation—for example, electronic safety-assured



software distribution. But it is not clear how to relate the two fields. For instance, what level of security assurance is needed for an AADS subsystem that handles safety-critical information assets such as DO-178B Level A avionics software updates?

- Currently, there is a lack of unified models and approaches for analyzing security and safety in aerospace. Traditional safety analysis used in design, development and certification of aircraft and avionics software is quantitative and probabilistic; it considers both process operations, which are continuous, and control dynamics, which are discrete. In contrast, traditional security analysis in the cyber world lies squarely in the discrete domain.
- Security threats are not bounded; their impact can change over time. For example, the discovery of an exploit can threaten the integrity of distributed aircraft software.

Recommendations:

1. Develop a unified framework to formalize the relationship between cybersecurity and system safety for aerospace CPS. Such a framework would allow us to express relevant security considerations as well as accommodate security risks and mitigations in a safety analysis. The unified framework would require advances such as:
 - Integrate the mainly discrete methods of traditional cybersecurity analysis into the quantitative probabilistic approaches of safety analysis used in aerospace.
 - Combine security analysis, which refers to non-functional properties, with the functional software correctness analysis to achieve an overall system safety level.
2. Develop methods to perform verification, validation, and testing of security technologies in the context of safety verifiability. These methods could enable the future design and development of certifiable security mechanisms for protecting safety-critical onboard systems and information assets.
 - Evaluation the onboard software and systems used to encrypt and authenticate systems and information assets that can affect system safety.
3. Develop certifiable information and network technologies for safety-critical or regulated functions of aerospace CPS. These technologies would enable aircraft to increasingly use advanced networking and IT technologies—for example, integrated modular avionics, which lighten an aircraft by lowering the number of physical systems onboard.
4. Design, develop, and evaluate onboard RFID and advanced sensing architectures to perform real-time, critical functions during flight, which can meet the current and future regulatory constraints and safety standards of aircraft.

- Develop methods to assess security assurance levels of open-source software and platforms, to gain the benefits of these cost-effective technologies in aerospace CPS and supporting applications.
 - Effective assessment methodologies for evaluating real-world open-source software design and development practices.
 - Develop metrics for determining assurance levels of open-source products.
5. Quantify the impact of cyber-world threats on the physical world.
- Evaluate the trustworthiness of sensed information of the physical world.
 - Evaluate the effect of cybersecurity vulnerabilities on the accuracy and performance of physical-world properties, such as aircraft delays and airline costs.

Challenge 2: Mixed criticality is inherent to CPS in the aerospace domain. In the context of an airborne network as an aerospace CPS, there is a mix of safety-critical and non-safety-critical data on the shared network. This network will be used by air vehicles and additionally by ground systems to distribute large volumes of potentially non-safety-critical data—for example, traffic information and weather updates.

For in-flight operations, each aircraft has a shared network with multiple logical domains separated by security mechanisms, such as firewalls. The most critical layer involves flight-control communications. The least critical layer includes passenger entertainment systems.

Recommendations:

1. Ensure that the architectures for controlling an aircraft’s integrated modular systems are safe and secure.
 - Evaluate the potential impact of software at different safety-assurance levels residing on the same hardware platform on an aircraft. For example, if DO-178B Level E software undergoes a cybersecurity-induced failure, how will that failure affect the safety-critical DO-178B Level A software?
2. Assess how potential security vulnerabilities of future decentralized airspace will affect various classes of air vehicles.
 - Conduct a security assessment of future communications, navigation, and surveillance technologies, such as Asynchronous Dependent Surveillance, before they are used for air traffic control and management.
 - Secure operation, control, and coordination of unmanned aerial systems for civilian applications in airspace.
3. Formally specify and validate the correct real-time interactions between mixed / critical system components in a CPS.
 - In the context of an airborne network, design a standard global policy specifying correct interactions between the airborne ad hoc network nodes for air



traffic control—that is, between aircraft as well as between aircraft and ground control centers. Apart from policy specification, the policy must be enforced to prevent violation by a compromised onboard or ground controller. A major weakness with the use of a centralized solution for enforcing policy among the network nodes is the risk of creating a single point of failure. Hence, a distributed policy enforcement technique is needed to regulate the behavior of the mobile aircraft.

- In the context of a multilayer shared network for in-flight operations, develop a verified and validated system architecture to assure that all layers remain separated and to verify that the interactions of components within and across layers do not interfere.

Challenge 3: An aerospace CPS can be a large-scale complex system or can rely on a large-scale system, with multiple stakeholders involved with manufacturing, operation, and maintenance of cyber and physical assets. In such an environment, individual entities may not have a complete view of the overall system and may not be aware of all the components and their interactions. Consequently, the safety and security requirements for the entire system may not be well-established at the global level even though these requirements are known, verified, and tested for individual components. For example, consider how loadable software from the onboard equipment suppliers is distributed to the aircraft. The end-to-end distribution is highly complex, involving multiple suppliers, airframe manufacturer, and airlines, all working together to deliver safety-assured software to a fleet of aircraft.

Recommendations:

1. Provide high assurance of systems of systems.
 - Develop interoperable domain standards and policies for security.
 - Design scalable pervasive solution for establishing trust in aviation applications such as commercial airplane software distribution.
 - Develop security models for multidisciplinary global collaboration.
 - Develop inexpensive, efficient, scalable methodologies for end-to-end assurance assessment.
2. Develop user-friendly verification and validation tools for CPS community.
3. Develop tools to visualize high-assurance methods and analysis in order to facilitate communication of high-assurance evaluation benefits to business management.
 - Create high-assurance system design and development tools that software architects/developers can use without substantial training, and that customers can easily understand so they can contribute to the specification.

Challenge 4: An aerospace CPS has physical-world properties that impose constraints arising from the lifespans of various subsystems. These properties and constraints must be considered in CPS design and evaluation. The typical lifecycle of an aircraft can span several decades, posing a unique design constraint on solutions. For example, the flight

control and communication systems are designed for the lifespan of the airplane. Passenger entertainment systems, on the other hand, need to keep pace with the latest advances in the entertainment systems, which require far more frequent replacements/updates. Because of these updates, the overall system may be more prone to security and safety threats.

Recommendation: Develop long-term security mechanisms for protecting information assets that are required by the aircraft till the end of its service.

Challenge 5: The human in the loop. Incorporating human-in-the-loop considerations into the design and operation of the CPS is critical to CPS dependability and predictability. CPS stakeholders must answer some very human questions: How will the user influence cyber-physical security guarantees and properties? How can the user be leveraged to make cyber-physical security functions more robust?

Recommendations:

1. Understand, define, and establish high-confidence human–computer interaction for physical asset operators from different backgrounds.
 - For example, in aerospace, the introduction of onboard networks and security technologies will warrant data representation and network monitoring tools to ease the cognitive load of pilots, aircraft maintenance, and air traffic control personnel. Because many aspects of global airline operation are safety-critical, software tools must support high-confidence designs and assessments as well as usability for a heterogeneous group of operators.
2. Develop privacy enhancement technologies for CPS users.
 - Assess concerns about user privacy. For example, how can a passenger be assured that an onboard RFID system used to trace his checked baggage won't be used to record what he bought, where? How can a passenger be assured that an airline's logistics or surveillance system designed to know the whereabouts of an airplane won't be used to report the comings and goings of its passengers?
3. Define and establish cybersecurity processes and procedures for CPS stakeholders.
 - Define and establish a cybersecurity management policy for physical asset operators.
 - Define and establish a cybersecurity incident-response policy for physical asset operators.



6 Healthcare and Public Health— Medical Devices

6.1 Environment

The domain of medical devices includes hospital care, pre-hospital advanced medical and trauma care, home care, electronic health records (EHRs) systems, and ambulatory and implanted devices. These devices may work in a standalone configuration or be interconnected with other devices. For a single standalone medical device, the most obvious danger is tampering of the device because the device's firmware could be reprogrammed, maliciously or accidentally. Since medical devices are increasingly being connected to the Internet, their firmware could even be altered remotely. For example, a patient may need to upgrade software that detects pacemaker arrhythmias using methods based on EMF (electric and magnetic fields) but that is impervious to EMF-based attacks. If the device undergoes tampering, the pacemaker may malfunction if the patient passes near an electromagnetic field.

Internet-enabled medical devices are often used to communicate patient information to a central location. This happens most commonly with home health-care devices, but is also common in remote clinics and telemedicine such as electronic Intensive Care Units (eICUs). Home healthcare devices gather patient data such as weight, blood glucose level, and blood pressure, transmitting the data to a server. The data may be copied in transmission, or a malicious attacker could replace the real data with a fake data stream, causing clinicians to miss a real problem or see a problem when none exists. Home devices also relay instructions from caregiver to patient. These instructions, too, are vulnerable to interception and replacement. For example, a device may be triggered to deliver medicine or interfere with implanted device.

A healthcare delivery process may also involve interaction between two or more devices. An example is the automatic synchronization of the X-ray exposure with an anesthesia ventilator that eliminates the need to manually switch off the ventilator to obtain an X-ray, then switch it back on after the X-ray has been taken [1]. Such manual switching of the ventilator for patients under anesthesia is prone to human errors, as reported in a case study by the Anesthesia Patient Safety Foundation in 2004 [22]. However, interoperability and interaction among devices create an unanticipated environment in contrast to the validated and verified usage of each device in stand-alone mode.

To prevent someone from tripping over a cable, a wireless infrastructure is often used to transmit information from device to display. Interconnected healthcare systems have many benefits. For example, emergency personnel may access private data on-demand anywhere and anytime, especially in wireless environments. For example, emergency personnel may access private data on demand anywhere and anytime, especially in wireless environments. Increasingly networked healthcare systems, however, pose new challenges in security and privacy. For example, as healthcare systems are interconnected, they are increasingly being subjected to malicious attacks:

- In 2008, healthcare devices in the National Health Service in England were infected by more than 8,000 computer viruses. In 12 instances, the e-infection directly affected patient care. In one well-publicized event, an instance of the Mytob cyber worm overloaded systems at several hospitals, limiting access to X-rays, blood tests, and patient administration systems.
- In an Idaho hospital, computer systems were severely handicapped when an employee opened an attachment from a celebrity-related email.
- In March 2009, the Conficker worm showed up on medical imaging devices. Most embedded systems on medical devices are not designed to upgrade or patch themselves. Many manufacturers state that such devices should not be connected to an open network.

For network-enabled and interconnected devices, dangers also include remote attacks as well as unexpected interference with other devices and external phenomena. For example, RFID readers can interfere with other medical devices, such as external pacemakers, dialysis machines, and defibrillators [27].

6.2 State of the Art

The state of the art in the security of medical devices and medical system integration consists of two key components:

- low-level data transfer and network security protocols and standards, and
- standards and regulations specifying best practices for device development. Some of these exist today (for example, IEEE 60601 governing electrical safety of connected devices); others are in progress—for example, Integrated Clinical Environment (ICE).

Current protection schemes operate at the network level and, for protecting important assets, at the host level. Intrusion prevention systems include firewalls; intrusion detection systems (statistical-, anomaly-, and behavior-based); and intrusion tolerance systems.

Existing medical devices, particularly embedded ones, commonly have unusual proprietary interfaces. In many cases, the devices are secured only by the obscurity of the interface and the difficulty of building the hardware necessary to communicate with the device. Open-source hardware tools like GNU Radio radically simplify the reverse engineering of these interfaces. While open source tools have been a boon for developers, they have opened devices to attack. An example of this can be seen in [16] on attacking pacemakers and implantable cardiac defibrillators with a GNU radio. The attacks need not be malicious. As the numbers of communicating devices increase, the likelihood of unintended interactions and interference rises significantly [27].



6.3 Challenges and Recommendations

Challenge 1: Security violation detection. In many ways, EHR systems are similar to distributed database systems in other domains, and security solutions used elsewhere will likely apply in the medical domain, as well. However, detecting security violations in medical systems is substantially different, and the task presents unique challenges. In order to detect tampering with a medical device in primary care, we will need to observe abnormal behavior in the device. But defining what is normal is a challenge in and of itself, given the tremendous amount of variability in human body. Thus what may be a normal development for one patient may be completely abnormal for another, regardless of whether the abnormality is caused by the patient’s condition, a device malfunction, or a security breach.

Recommendation: Develop improved patient and caregiver models that will help perform dynamic adjustment for the detection algorithms and improve fidelity of alarm generation.

Challenge 2: Verification and validation of interconnected and interacting devices. As the number of interacting devices in the healthcare delivery process increases, it becomes more and more difficult to anticipate the possible scenarios that need to be verified and validated.

Recommendation: Develop tools and techniques, such as those based on static analysis and lightweight theorem proving, that can help verify that implementations of medical systems satisfy security and safety specifications.

Challenge 3: Proprietary interfaces and protocols. Most large computer-based medical systems today are built (and billed) as “integrated solutions” by a single vendor. Interfaces to the components of such systems and communication protocols they use are often proprietary, making it difficult to independently validate the system, particularly from the standpoint of security.

Recommendations:

1. Develop open-API interoperability techniques and standards with provable security guarantees.
2. Develop open device implementations and virtual devices for testing.

7 Commercial Facilities—Buildings

7.1 Environment

Building automation systems (BASs) monitor, control, and administer building attributes and interactions among devices within and across building systems. A typical building system includes BASs for lighting heating, ventilation, and air conditioning (HVAC); power; building access control; elevator controls; and fire alarm and life safety.

Traditionally, these systems were dedicated and worked in stand-alone configurations. However, they are now being tightly integrated to allow improvement in building control and cost reductions [21, 26, 20]. For example, lighting systems use considerable energy and generate cooling loads that, in turn, overload the HVAC systems. By more closely coordinating the HVAC system and lighting system, a building operator can significantly reduce energy usage. Similarly, fire alarm systems are being interfaced to HVAC so that an alarm signal can trigger shutting down of the air handling systems. Additionally, controlling of the HVAC functions by the fire alarm/life safety system allows air duct systems to be used for smoke control and removal. Also, fire alarm/life safety systems can control elevator systems. Other interoperation examples of BAS include the activation of lighting for safe exit and automatic triggering of CCTV events enabling remote operators to view/capture live video from an area of interest [28].

With the emerging Smart Grid applications, BASs are being designed for remote monitoring and control of power usage for efficient power management in a given area. Remote users, including the electric power companies and other authorized users, may access the building automation system for energy service management, system configuration, and fault handling [19, 21].

Communication networks in BASs are typically implemented using a two-tiered hierarchical model [25], including a control network and a backbone network. The control network includes intelligent sensors and actuators that exchange process data, such as sensor values, or receive control commands and system configuration parameters. Several control networks are connected through a backbone network for central monitoring and control, remote maintenance, and diagnostics. The backbone network also supports remote monitoring and management functions to users through the Internet.

Unfortunately, this increased connectivity and Internet-based access to control networks make BASs vulnerable to cyber-physical attacks. Though the BAS controllers run only dedicated software applications, their device-to-device network may be compromised. Moreover, the security vulnerabilities in the BAS data communication protocols (for example, BACNet, LonWorks/LonTalk, KNX/EIB) can be exploited for compromising BAS [20, 3, 17, 18]. A compromised device can be used to disrupt other BAS devices or subsystems by spoofing or by launching a denial-of-service attack [17, 18]. For example, a compromised fire alarm/safety system may trigger the HVAC system to shut down power; it may even activate sprinkler system. This may have disastrous effects on the building operations as well as the lives and safety of the building's occupants. Consider, for example, a hospital where patients with highly contagious diseases such as



H1N1 are quarantined in separate, designated wards. A malicious or unintended change in the HVAC settings may endanger the safety of patients and staff members in other wards [15]. Recently, in Dallas, a hacker gained access to a hospital's HVAC system [49].

In addition to the IT vulnerabilities, BASs are susceptible to other CPS threats [17]. For example:

- Through human error, a subsystem or device can be misconfigured, causing other BAS devices to malfunction.
- A BAS component can fail, affecting other BAS components in the shared network.
- An insider can perform an unauthorized action.

7.2 State of the Art

The state of the art for countering security threats in BAS and BAS networked systems include these tools and measures:

- **Encryption-based protocols** for secure data communication and network security addressing [3]:
 - BAS device and user authentication
 - Integrity and confidentiality of data when exchanging process data such as sensor values or device configuration and control data
 - Encryption key management, including key distribution, revocation, and lifecycle.
- **Intrusion prevention systems**, including firewalls
- **vulnerability assessment of BAS data communication protocols**—for example, a BACnet wide-area network security threat assessment [18]
- **best practices and guidelines for BAS network design** and tamper-resistant measures that can be implemented in a BAS network [14, 36].

7.3 Challenges and Recommendations

As the conventional electric grid is evolving into a smart grid, there is a parallel trend toward zero-energy smart buildings. These smart buildings will have more infusion of IT and more closely coupled integration of BAS, providing more connectivity and remote accessibility for efficient energy management and support for smart metering, distributed generation, and distributed aggregation of power generation resources. Support for distributed resource aggregation may require shutting off some of the building operations; that decision will depend on the supply capability of the off-grid resources. This increase in complexity in smart and energy-efficient buildings due to increased interdependency and connectivity creates more potential vulnerabilities and challenges.

Challenge 1: Verification and validation of interconnected and interacting BAS components and subsystems. As the number of interacting BAS components and subsystems increases in smart buildings, it becomes more and more difficult to anticipate the possible scenarios that need to be verified and validated, especially in buildings such as hospitals and chemical plants, where the vulnerability exploitation could directly threaten human health or safety.

Recommendation: Develop tools and techniques, such as those based on static analysis and theorem proving, that can help verify that implementations of integrated BAS systems conform to the security specifications of the relevant building automation and control operations and can ensure that the interplay of these operations does not pose a security or safety threat.

Challenge 2: Safety and security analysis. A key requirement for safety of building automation and control operations is to ensure that security policies and mechanisms are properly designed, configured, and enforced. Safety analysis mainly focuses on the functional correctness of the system as well as meeting the protection requirements. By contrast, security analysis mainly deals with intrusion detection, access control enforcement, and network security. Currently, there is a lack of unified models and approaches for analyzing security and safety together.

Recommendations:

1. Develop a unified framework for conducting a combined analysis of BAS safety and security. This framework will be useful for
 - identifying any possible violation of safety and security properties arising from the interplay of BAS dynamics/control logic and security policies
 - detecting incompleteness and vagueness in security policy specifications, as well as identifying security holes
 - detecting when a security mechanism is misconfigured in a way that can cause a process to enter an undesirable state.
2. Develop methods to functionally test security mechanisms and verify and validate that they are safe from intentional attack and inadvertent misconfiguration.



8 Conclusions

In this section, we present the general state of the art, common challenges, needed capabilities, and pending challenges that are common across multiple cyber-physical system (CPS) sectors. We also offer specific recommendations to target these issues.

8.1 State of the Art in CPS Security

In this subsection, we summarize the state of the art in securing cyber-physical systems.

For securing individual CPS components, we can count on reasonably good capabilities, such as firewalls, gateways and individual controllers. However, a complete understanding and comprehensive security are sorely missing at the integrated system level and the system-of-systems level. A sophisticated attacker, for example, could exploit relatively minor loopholes in different components and subsystems, and, by combining these exploitations, launch a sophisticated attack that causes major damage. In the water sector, for example, a hacker might cause minor leaks at a large number of control valves: each leak by itself can be minor and acceptable, but together the leaks can cause a substantial loss in water pressure. Should the hacker target a chemical plant, he might cause different gases to leak from different valves, creating a gaseous mixture that, sooner or later, will explode. The threat vectors from such cumulative attacks are many. In brief, the composite effects of small security breaches are not understood.

The problem of securing cyber-physical systems is currently treated as a cyber-security problem. Yet solutions for cyber-security problems do not always translate to securing cyber-physical systems. For instance, the physical dynamics and impact of a successful attack on chemical plants, sewage systems, dam controls, and electricity can be substantial and immediate. In information systems, backward compensation can be carried out. For example, if a credit card is stolen, the corresponding account can be canceled and a new card issued. However, once a dam is breached, or toxic chemicals and fumes are released, compensation is rather difficult (if not impossible) and substantial damage to lives and property can be all but inevitable.

The lack of solutions has several causes:

- There is a distinct lack of integrated approaches for securing both cyber and physical aspects of cyber-physical systems.
- Typically, cyber-physical systems use embedded real-time operating systems and executives, but vendors of such software typically do not build safety and security mechanisms into their software infrastructure, in order to keep cost low and performance high.
- The design, construction, and operation of cyber-physical systems require a multitude of skills, while security experts often tend to be information experts, not specialists or engineers in the cyber-physical system domain of interest.

8.2 Challenges

In this subsection, we will identify a host of challenges that need to be addressed to secure cyber-physical systems and the critical infrastructure of the nation.

Sound scientific foundations that bridge the cyber world of information security and the security of the physical world are currently lacking. This situation is partly due to the multidisciplinary nature of cyber-physical systems that exploit not only cross-domain principles but also domain-specific optimizations.

Verification and validation (V&V) techniques that can deal with both the continuous dynamics of the physical world and the discrete logical transitions of the cyber-world do not yet exist. While hybrid model checking techniques offer potentially promising solutions, they need to be scaled substantially to deal with real-life situations.

Cyber-physical systems can be extremely complex since they must **simultaneously satisfy requirements for dependability, real-time safety, and security**. Researchers and practitioners are typically experts in one (or at most two) of these areas. These constraints can also lead to conflicts among design goals. For example, dependability may require lots of redundancy, but coordinating replicas in real-time is made more difficult. Good security may call for frequent authentication and security checks, which in turn can work against user-friendliness or real-time performance.

A common understanding of risk is lacking in today's cyber-physical systems. Risk is often estimated in ad hoc fashion on a sector-by-sector basis; coherent solutions to quantify and manage risk are not available. For example, is the electric grid, with its distributed footprint but much wider customer base, more risky—or less risky—than a centrally located chemical plant with a smaller population in the neighborhood?

Coherent security performance metrics do not exist in cyber-physical systems in different sectors. While productivity and output metrics are available in industry sectors, metrics that integrate network connectivity and system-level security are not available. **Performance and risk assessment testbeds** that can span multiple CPS sectors are also not present. Creating multiple sector-specific testbeds can be prohibitively expensive.

Real-time datasets that can be used for validating hypotheses and interesting conjectures are not available for research and experimentation purposes.

A worrisome aspect is the modern trend of **outsourcing and off shoring** development with the objective of cost-cutting. However, the security loopholes that may be opened up by code developed in other countries are not fully understood. While unintended bugs may always exist, errors and trapdoors that were maliciously introduced can exist and cause problems at the most inopportune times.

The scale and complexity of cyber-physical systems across multiple large sectors that span the entire economy is daunting. The social benefits of these systems must be appreciated in policy planning. For example, the loss of electricity for only a few days can cause major inconvenience to large geographical regions and acute problems in life-critical scenarios. The extended loss of water supply or extensive environmental pollution can lead to the suffering of millions of people. At the same time, continuous monitoring of such systems, when abused, can legitimately lead to concerns about the loss of



privacy. These social costs, too, must be taken into account in the design of cyber-physical systems, and corresponding cost–benefit analyses must be carried out. Both the limits and power of connectivity as they relate to cyber-physical systems must be fully understood. As cyber-physical systems interface with the physical world in real-time, environmental and systems data can be collected in enormous volumes very rapidly. We don't yet understand the point at which one has "too much" data.

There is limited dialogue among the stakeholders of cyber-physical systems and the stakeholders of nation's critical infrastructure assets. On one side is the federal government, represented by the Department of Homeland Security, responsible for the safety of the homeland, its infrastructure, and its people. On another side are for-profit companies, such as electrical utilities and plant owners, whose interest could be to maximize their overall profits and profit margins. A service (such as electricity) may be generated and delivered by entities that span multiple states and different owners.

Finally, consumers may get quite agitated if their privacy is compromised and their individual data are exported for all to see. Mechanisms and modalities for dialogue among stakeholders are not easy to design and to execute in practice.

8.3 Recommendations

In this subsection, we identify specific capabilities and recommendations that will be required to secure our cyber-physical systems infrastructure.

New security strategies must be developed for integrated cyber-physical systems where the physical impact of attacks is explicitly taken into account. Such strategies require a clear understanding of the threat models, the resources being defended, and the physical impact of successful attacks. Novel analytical techniques will be required to explore the space of possible attacks and inoculating cyber-physical systems from such attacks. Innovative synthesis techniques will be needed to compose and integrate different components, subsystems, and systems, building them both from scratch and in incremental fashion, and to prove and demonstrate that the resulting system of systems will be safe under day-to-day operations. Also needed are the development and availability of robust performance models and metrics that can unambiguously distinguish attacks from normal variations in the process being controlled. Run-time mechanisms are also required to provide graduated failure containment in case of breaches.

Given the increased connectivity and accessibility of cyber-physical systems, it becomes more and more difficult to verify and validate their interactions with respect to the functional correctness as well as the safety and security properties. Methods and approaches are needed to support verification and validation of interconnected and interacting cyber-physical systems at different granularity levels, including the component level, the system level, and the system-of-systems level. These methods and approaches should be scalable and support detailed design time verification and validation as well as runtime analysis for monitoring and control.

As mobile and portable devices such as smartphones and netbooks with network connectivity proliferate, they will increasingly be used by CPS personnel to access and per-

haps even control cyber-physical processes. **New techniques are required to authenticate millions of devices** as they continue to grow in popularity.

Innovative architectures with pluggable yet secure interfaces are necessary to integrate legacy systems with newer systems and designs that include the interconnectivity across the physical domain due to physical coupling, and networks, including the Internet and the mobile communications network, comprising WiFi, WiMax, and 3G and 4G broadband technologies. To support these requirements, we will need new operating system services, protocol stacks, and hardware devices, as well as smart sensors and actuators that can distinguish between an action, command, or setting that is benign and one that is malevolent or simply unsafe.

The unique security needs of cyber-physical systems must be documented by formal **requirements capture tools that can track both the discrete and continuous aspects** of cyber-physical systems. In essence, what is not understood well cannot be built and verified correctly. Since facilities such as nuclear power plants, utilities, and air traffic control systems must also satisfy government regulations, modeling of these policies and regulations is also required. For example, if a nuclear power plant stops operating for any reason, regulatory agencies must be notified and need to clear the plant before it can restart operations, leading to expensive and inconvenient delays. Security hooks must, therefore, be aware of such constraints. They cannot, however, be either over-aggressive or over-conservative.

As cyber-physical systems such as automated manufacturing plants become sophisticated, the **security for increasingly autonomous systems with dynamic behaviors** requires new feasible solutions. One can easily imagine robots and other automated sentries keeping an ever-watchful eye to secure physical premises. Since such autonomous systems may occasionally enter states that they may have never been in before (such as “high alert”), defining and validating their security properties must be done at relatively high levels of abstraction (such as safe states and recoverable states).

New techniques for securing networks with self-configuring and self-healing capabilities are needed. For example, consider a smart grid that detects that an electrical substation is being attacked, and in response reroutes power around the substation to its many destinations. It may be that the attacker intended that response as the desirable outcome of the original attack, and subsequent attacks may exploit the dynamic reconfigurations of the network to cause even more havoc down the road. Similarly, as more wireless sensor-actuator networks get deployed to monitor bridges, dams, and other structures, the inherent security deficiencies of wireless communications must be balanced against the lower costs enabled by the absence of wiring.

As cyber-physical systems grow more sophisticated, they must be able to **provide appropriate feedback to operators** in human-friendly terms to explain why specific actions are (or are not) being taken.

Either intentional or unintentional misbehavior of human operators of cyber-physical systems can lead to partial or complete system failures. Extensive studies of many man-made disasters, such as failures of nuclear power plants, spacecraft failure, rocket failures, and aircraft accidents attributed to pilot error, indicate that a chain of errors, each of which might individually be small, often leads to serious safety lapses. Statistical, yet



detailed, **models for humans in the loop** need to be developed for cyber-physical systems. There is a related, yet complex, question: What role, if any, should humans play in securing cyber-physical systems? A likely answer is that humans can neither be completely out of the loop nor be heavily involved in every operational step in such systems. In fact, humans may need to be more (or less) involved, depending upon the current state(s) of the cyber-physical system being secured.

The construction of cyber-physical systems requires skills and expertise from multiple disciplines, such as operating systems, networking, security, control systems, sensors, physics, chemistry, and mechanical or structural engineering. **Cross-disciplinary and cross-sector training** are critical. A common vocabulary must be adopted by both engineers and cyber-scientists. This is especially crucial since the same terms—such as “signals” and “sockets,” or acronyms, such as IP³—can have very different meanings to different specialists. New terms may also need to be introduced for new concepts. Just as the complexity and difficulty of writing and testing good software led to the new domain of software engineering, the inherent cross-disciplinary nature of cyber-physical systems must lead to the domain of **CPS engineering**.

While many innovations are required to make cyber-physical systems secure, **solutions must follow the KISS principle** (Keep It Simple, Stupid). Unnecessary complexity can lead to more hiding places for attackers and latent bugs. As more features are added and more complexity is added, interactions among subsystems and components only become more complex and, therefore, less easy to secure/protect.

Most cyber-physical systems may need to adapt in practice. Operating conditions, workloads, available resources, and environmental attributes may change, forcing the cyber-physical system to change its mission or lower its efficiency. For example, if the workload on the electrical grid goes past a threshold during a hot summer day, brown-outs may be initiated in an attempt to prevent the widespread blackouts and the resulting damages. Such adaptability must be controlled such that it does **not induce any cascading failures**. In chemical plants and reactors, any faults (such as processor, communication and valve failures) that occur must be contained using appropriate fault-containment boundaries both in the cyber and physical domains. Fault-tolerance strategies that jointly deal with these failures need to be designed and their effectiveness demonstrated in practical systems. As faults occur, even techniques like **online model checking** could be utilized and enable dynamic validation of the safety and security properties of the system under its current operating conditions. Hybrid systems checking can also be extended significantly to treat safety not as a binary state (safe or unsafe) but as a continuum (safe, mostly safe, acceptably safe, ..., to unsafe).

Realistic testbeds that can be used to validate the security of cyber-physical systems are needed. For example, honeypots used for securing cyber systems must be extended significantly to support cyber-physical systems. These **CPS honeypots** must emulate the behavior of the physical side of the CPS to provide the attacker with the illusion of a successful attack. Physical dynamics and impact must therefore be emulated convincingly.

³ *Signals* represent useful information in continuous data for electrical engineers, and asynchronous notifications of events for operating system experts. *Sockets* represent consumer electric power outlets for electrical engineers, and communication endpoints for networking experts. *IP* denotes the Internet Protocol for computer scientists but Intellectual Property for inventors.

ly, in real-time. These testbeds must also support multiple domains and disciplines that constitute a complete CPS.

While techniques to react to ongoing attacks on cyber-physical systems are needed, **solutions that deter attacks** can more be effective defensive weapons for keeping cyber-physical systems secure. In other words, both proactive and protective measures must be identified, implemented, and tested. The effectiveness of such preventive approaches must also be quantified; any tradeoffs (such as the lack of flexibility and convenience for the users) must be made explicitly. Even if it's not 100 percent effective, an emphasis on deterring attacks can minimize the impact of failures or delay its effects such that more time is available to identify and repel the attack.

New techniques must be developed to deal with privacy in the context of cyber-physical systems. Medical devices and health-care equipment are cyber-physical components, attacks on which can compromise private data quickly to the detriment of many unsuspecting victims. Anonymization techniques with multiple levels of indirection and hashing could be developed to mitigate or even eliminate concerns about leakage of medical information. Similar concerns apply to the consumption of electricity, water, and gas. Aggregation techniques that remove consumer identification could be one solution to deal with such situations, but billing and remote control (as part of a smart infrastructure like a smart grid) will still require private information to be treated with the utmost care. Innovative solutions based on the physical properties of these entities can be developed.

If **outsourcing and offshoring** trends cannot easily be reversed, technological solutions must be brought to bear to ensure that code developed elsewhere does not hide Trojan horses and trapdoors that may be exploited in the future. Emulators, testbeds, and new abstractions that extend honeypots can be used to validate the behaviors of externally produced code under a vast range of operating conditions. Testing theory can be developed that introduces, for example, finite test vectors, which can be verified rapidly but with extremely high fault coverage. Another possible approach is to express design and security intent that runs as wrappers around suspected code, trapping any violations of intent before they manifest as negative effects in the environment. The physical dynamics of the system must be explicitly considered to support such behaviors safely and securely. Errors from these code modules should be constrained so that they cannot leak into other modules and subsystems. These concerns and prospective concerns can be generalized as follows:

Given (partially) untrusted components, how can one build trusted systems?

Practical and cost-effective solutions to secure cyber-physical systems must be found. Theories that study the optimal and best-possible schemes may serve as comparison points, but approximations that are affordable and usable in practice will be highly desirable.

Cross-disciplinary and cross-sector initiatives are required to address the multitude and scale of cyber-physical systems in the nation's critical infrastructure. Substantial and sustained investments will be needed to maintain innovation and competitive advantage at the national level.



9 Acronyms and Abbreviations

AADS	Airplane Assets Distribution Systems	ICS	industrial control system
AC	Advisory Circular	ICSJWG	Industrial Control Systems Joint Working Group
AMI	Advanced Metering Infrastructure	IEC	International Electrotechnical Commission
AMI-SEC	Advanced Metering Infrastructure Security	IEEE	Institute of Electrical and Electronics Engineers
API	application programming interface	IGD	Infrastructure and Geophysical Division (of DHS S&T)
ATM	air traffic management	INL	Idaho National Laboratory
A2A	aircraft-to-airplane	IP	Office of Infrastructure Protection (of DHS)
A2I	aircraft-to-ground infrastructure	ISA	International Society for Automation
AWWA	American Water Works Association	IT	information technology
BAS	building automation systems	KISS	Keep It Simple, Stupid
CCTV	closed-circuit television	kV	kilovolt
CEO	Chief Executive Officer	M&S	modeling and simulation
CFATS	Chemical Facility Anti-Terrorism Standard	MW	megawatt
CIKR	critical infrastructure and key resources	NERC	North American Electric Reliability Corporation
CIP	Critical Infrastructure Protection	NIST	National Institute of Science and Technology
CPS	cyber-physical system(s)	NITRD	Networking and Information Technology Research and Development
CRUTIAL	CRITICAL UTILITY InfrastructureAL	NJ	New Jersey
DCS	distributed control systems	NSF	National Science Foundation
DHS	Department of Homeland Security	NY	New York
DOD	Department of Defense	PCSRF	Process Control Security Requirements Forum
DOE	Department of Energy	PLC	programmable logic controller
EHS	electronic health records	R&D	research and development
eICU	electronic intensive care unit	RFID	Radio-frequency identification
EMF	electric and magnetic fields	RTU	remote terminal unit
EPA	Environmental Protection Agency	S&T	Science and Technology Directorate (of DHS)
FAA	Federal Aviation Administration	SCADA	supervisory control and data acquisition
FOUO	For Official Use Only	SP	Special Publication
GDP	Gross Domestic Product	SVA	security vulnerability assessment
GETS	Government Emergency Telecommunications Service	TCIP	Trustworthy Cyber Infrastructure for Power
GNU	GNU's Not Unix	TRUST	Team for Research in Ubiquitous Secure Technology
GPS	Global Positioning System	US	United States
HMI	human-machine interface		
H1N1	Hemagglutinin Type 1 and Neuraminidase Type 1 ("swine flu")		
HQs	headquarters		
HSIN-CS	Homeland Security Information Network—Critical Sectors		
HVAC	heating, ventilation, and air conditioning		
ICAO	International Civil Aviation Organization		
ICE	Integrated Clinical Environment		

USAF	U.S. Air Force
US-CERT	United States Computer Emergency Readiness Team
USSS	U.S. Secret Service
V&V	verification and validation
WARN	Water/Wastewater Agency Response Network
WG	working group



10 References

- [1] D. Arney, J. M. Goldman, I. Lee, E. Llukacej, and S. Whitehead. Use Case Demonstration: X-Ray/Ventilator, *Joint Workshop on High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability*, p. 160, 2007.
- [2] R. Poovendran et al. *A Community Report of the 2008 High-Confidence Transportation CPS Workshop*, June 2009.
- [3] W. Kastner, G. Neugschwandtner, S. Soucek, and H. M. Newman. Communication Systems for Building Automation and Control, *Proceedings of the IEEE*, Vol. 93, No. 6, pp. 1178–1203, 2005.
- [4] Chemical Sector, *National Infrastructure Protection Plan*. Department of Homeland Security. http://www.dhs.gov/xlibrary/assets/nipp_snapshot_chemical.pdf
- [5] American Chemistry Council. *Making Strides to Improve Cybersecurity in the Chemical Sector*, 2009 Update.
- [6] Chemical Sector Cybersecurity Program Steering Team, *US Chemical Sector Cybersecurity Strategy*, American Chemistry Council, September 2006.
- [7] US-CERT, *Control Systems Cybersecurity Awareness Information*, July 2005.
- [8] USSS/CERT, *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, May 2005.
- [9] X. He, J. Vaidya, B. Shafiq, N. Adam, and V. Atluri. *Preserving Privacy in Social Networks: A Structure-Aware Approach*, to be published in *Proceedings of the 2009 IEEE/WIC/ACM International Conference on Web Intelligence*.
- [10] X. He, J. Vaidya, B. Shafiq, and N. Adam. *Efficient Privacy-Preserving Link Discovery*, 13th Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD-09).
- [11] X. He, B. Shafiq, J. Vaidya, and N. Adam, *Privacy-Preserving Link Discovery*. *Proceedings of the 23rd Annual ACM Symposium on Applied Computing, Data Mining Track*, March 16–20, 2008, Fortaleza, Ceara, Brazil.
- [12] N. Zhang and W. Zhao. *Distributed Privacy Preserving Information Sharing*, *Proceedings of the 31st international Conference on Very Large Data Bases*, Trondheim, Norway, 2005.
- [13] R. Agrawal, A. Evfimievski, and R. Srikant. *Information Sharing Across Private Databases*, *Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data*, San Diego, California, June 09–12, 2003.
- [14] B. Eisenstein, T. A. Reddy, A. Woldu, and R. Wagle. *Investigation into Computer Network Security for Integrated Building Automation and Control Systems*, Drexel University contractor report, NIST GCR 03-845, 2003.
- [15] B. Eisenstein, T. A. Reddy, A. Woldu, and R. Wagle. *Security of Life Safety and Access Control Systems in an Integrated Building System Environment*, Drexel University contractor report, NIST GCR 03-850.

- [16] D. Halperin, T.S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses, *IEEE Symposium on Security and Privacy*, May 2008.
- [17] David G. Holmberg. Enemies at the Gates: Securing the BACNet Building, *ASHRAE Journal (BACnet Today)*, Vol. 45, No. 11, B/24-28, November 2003.
- [18] David G. Holmberg. *BACnet Wide area network Security Threat Assessment*, NIST Internal Report 7009, 2009.
- [19] Hsiao-Yi Huang, Jia-Yush Yen, Sih-Li Chen, and Feng-Chu Ou. Development of an Intelligent Energy Management Network for Building Automation, *IEEE Transactions on Automation Science and Engineering*, Vol. 1, No. 1, pp. 14–25, July 2004.
- [20] ICAO, *Draft Manual of Detailed Technical Specification for IPS/ATN*, June 2006.
- [21] Scott A. Lintelman, Krishna Sampigethaya, Mingyan Li, Radha Poovendran, and Richard V. Robinson, High Assurance Aerospace CPS & Implications for the Automotive Industry, *Proceedings of the National Workshop on High Confidence Automotive Cyber-Physical Systems (CPS)*, April 2008.
- [22] A. S. Lofsky. Turn Your Alarms On! *APSF Newsletter: The Official Journal of the Anesthesia Patient Safety Foundation*, 19(4):43, 2005.
- [23] Clifford Neuman. Challenges in Security for Cyber-Physical Systems, *DHS:S&T Workshop on Future Directions in Cyber-physical Systems Security*, July 2009.
- [24] *Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). Recommendations of the National Institute of Standards and Technology.*
- [25] Timothy Salisbury. A Survey of Control Technologies in the Building Automation Industry, *16th IFAC World Congress*, July 2005.
- [26] Krishna Sampigethaya, Sudhakar Shetty, Terry Davis, Mingyan Li, Scott Lintelman, Richard Robinson, and Linda Bushnell. Networked CPS View of a Future Airspace, *Proceedings of the National Workshop on High Confidence Transportation Cyber-Physical Systems (CPS)*, November 2008.
- [27] R. Togt, E. Lieshout, R. Hensbroek, E. Beinat, J. Binnekade, and P. Bakker. Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment, *JAMA* 2008;299(24):2884–2890.
- [28] Joanna R. Turpin. Integrating BAS with life safety: Part II. *Engineered Systems*, March 2005.
- [29] Water Sector Coordinating Council Cybersecurity Working Group. *Roadmap to Secure Control Systems in the Water Sector Roadmap to Secure Control Systems in the Water Sector*, March 2008.



- [30] Water Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan, May 2007, http://cfpub.epa.gov/safewater/watersecurity/publications.cfm?sort=name&view=doctype_results&document_type_id=2
- [31] As Inspections Dwindled, Water Main Breaks Rose, *Washington Post*, May 7, 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/05/06/AR2009050604214.html?sid=ST2009052002320>
- [32] Wastewater Facilities Experts' Views on How Federal Funds Should Be Spent to Improve Security. *United States Government Accountability Office Report to the Committee on Environment and Public Works*, U.S. Senate, January 2005.
- [33] R. McMillan. California Canal Management System Hacked. *PC World*, December 1, 2007, <http://www.pcworld.com/article/id,140190-page,1/article.html>
- [34] Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain. *Government Accountability Office Report*, 2007 (GAO-07-1036).
- [35] Catalog of Control Systems Security: Recommendations for Standards Developers. *National Cybersecurity Division, Control Systems Security Program*, DHS, January 2008.
- [36] J. Zachary, R. Brooks, and D. Thompson. Secure Integration of Building Networks into the Global Internet, *The Pennsylvania State University contractor report*, NIST GCR 02-837, 2002.
- [37] D. Leiter. *Distributed Energy Resources*, prepared by the U.S. Department of Energy for Fuel Cell Summit IV, May 10, 2000, Washington DC.
- [38] *America's Electric Utilities: Committed to Reliable Service*, www.eei.org, May 2000.
- [39] Electricity Grid in U.S. Penetrated By Spies, *The Wall Street Journal*, Tech, Wednesday, April 8, 2009, <http://online.wsj.com/article/SB123914805204099085.html>
- [40] S. M. Amin and J. Stringer. The Electric Power Grid: Today and Tomorrow, *MRS Bulletin*, Vol. 33(4):399–407, April 2008.
- [41] S. M. Amin and B. F. Wollenberg. Toward a Smart Grid, *IEEE Power and Energy Magazine*, Vol. 3, No. 5, September 2005
- [42] H. C. Richards. The “Smarts” of an Intelligent Grid: Analytics for Intelligent Grid Initiatives, *Energy Insights #EI212029*, May 2008.
- [43] IEEE-USA Policy Position Statement, *National Energy Policy Recommendations*. January 2009.
- [44] Cybersecurity Coordination Task Group. *Smart Grid Cybersecurity Requirements*, NIST Working Draft Version 1.0, August 2009.
- [45] *Roadmap to Secure Control Systems in the Energy Sector*. Developed by Energetics Inc., and sponsored by U.S. DOE and U.S. DHS.

- [46] Trustworthy Cyber Infrastructure for Power (TCIP), <http://tcip.iti.illinois.edu>
- [47] Team for Research in Ubiquitous Secure Technology (TRUST),
<http://www.truststc.org>
- [48] CRITICAL UTILITY InfrastructurAL resilience (CRUTIAL),
<http://crutial.cesiricerca.it/>
- [49] Emily Tsao. Arlington Man Accused of Hacking into Carrell Clinic Computers,
The Dallas Morning News, June 30, 2009.
- [50] E. Broughton, The Bhopal Disaster and its Aftermath: a Review, *Environmental Health*, 2005; 4(1):6.
- [51] Chemical Facility Anti-Terrorism Standards: Facility Inspections.
http://www.dhs.gov/files/programs/gc_1177001576714.shtm.



Appendix A. Workshop Announcement and Agenda

Science & Technology Directorate, US DHS
National Cybersecurity Division, US DHS
Office of the Secretary of Defense, US DOD
National Institute of Standards and Technology
US Department of Energy
Operations, Plans & Requirements (A3/5), HQ USAF
Logistics, Installations, & Mission Support (A4/7), HQ USAF
In Collaboration with the following states: Delaware, District of Columbia, Maryland, New Jersey, New York, Pennsylvania, Virginia, West Virginia (members of the All Hazards Consortium)

Workshop on
Future Directions in Cyber-Physical Systems Security
July 22–24, 2009
Gateway Hilton Newark Penn Station
Gateway Center, Newark, NJ 07102

Overview

Cyber-physical systems (CPS) are characterized by the tight coupling and coordination among sensing, communications, computational and physical resources and are exhibited in many application areas including industrial control systems (ICS). ICS encompass several types of control systems including: supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). CPS are prevalent in almost every critical infrastructure sector such as: electricity, water, gas, transportation, chemical, and healthcare. Interconnections of cyber-physical systems form complex systems with interdependencies within a given sector as well as across sectors. For example, the electric power grid of today forms one of the largest and most complex systems of power generation, transmission, and distribution systems at local, regional, and national level. It is envisioned that the complexity of the cyber-physical systems of the future will far exceed that of today's. Such a complexity poses several research challenges related to resiliency, vulnerability, threat, and recovery assessment. There is a need for models, theories, methods, and tools to address the security of cyber-physical systems taking into account the cyber and physical components of a system in an Inte-

Program Committee

- Nabil R. Adam, DHS-S&T (Program Chair)
nabil.adam@dhs.gov
- Michael Aimone, U.S. Air Force
- S. Massoud Amin, U of Minnesota
- Elisa Bertino, Purdue U
- Alvaro Cardenas, UC Berkeley
- Peter Chen, Louisiana State U
- Lydia Duckworth, The MITRE Corporation
- Ronda Dunfee, U.S. DOE
- George Gross, UIUC
- Mark Hadley, Pacific Northwest NL
- Steve Hawkins, Raytheon Intelligence and Information Systems
- Clas A. Jacobson, United Technologies
- Sushil Jajodia, GMU
- Antwane Johnson, Office of the Secretary of Defense
- Bruce Larson, American Water Works, Inc. and Water Sector Coordinating Council
- Insup Lee, U of Pennsylvania
- Chung-Sheng Li, IBM
- Marija D. Ilic, CMU
- Sean P. McGurk, National Cyber Security Division, DHS
- Frank Mueller, NCSU
- Raj Rajkumar, CMU
- Riley Repko, US Air Force
- William H. Sanders, UIUC
- Ronald M. Sega, Colorado State U
- Kang G. Shin, The Univ. of Michigan
- Lawrence Skelly, DHS-S&T (General Chair)
- James A. St. Pierre, NIST
- John A. Stankovic, U of Virginia
- Kevin Sullivan, Microsoft
- Bhavani Thuraisingham, U Texas at Dallas
- Bill Woodward, DHS/TSA
- Yelena Yesha, UMBC



**Homeland
Security**

Science and Technology

grated and unified way and realizing the discrete and continuous aspects of the system.

Workshop Goals and Objectives

The objective of the workshop is to provide a forum for

- i) representatives from various government agencies to briefly present their strategic vision of securing the cyber-physical systems as it relates to the nation's critical infrastructures;
- ii) researchers from academia, industry and national laboratories to assess the state of the art, identify related R&D challenges, and propose solutions to address these challenges;
- iii) subject matter experts, practitioners and state and local representatives to discuss their perspectives on the current state of the security of cyber-physical systems; where should the technology and science be in 5–10 years from now; why we are not there now – What are some of the challenges that are in the way of to be there now?; and why do we need to be there? That is, what legitimate case can be made to justify the needed R&D investments?

The results of the workshop will help DHS-S&T formulate near and long term investment decisions as well as research strategies, plans and objectives for cyber-physical systems security.

Classification

The workshop will be conducted as **Unclassified**.

Workshop Structure and Format

Format for the workshop:

- Keynote Speakers
- Presentations, Panels, posters—The presentations and panels will be discussing background useful for the breakout sessions
- Breakout sessions and reports

Submission Requirements

Presentations at the workshop will be by invitation. If interested, please submit a 3-page position paper (excluding references).

Papers not selected for presentations at the workshop will be considered for a poster session.

Workshop discussions will focus on identifying detailed research challenges and promising avenues for satisfying the unique security needs in cyber-physical systems. Infrastructure sectors of special interest include Electricity, Chemical, Transportation, Drinking Water/Wastewater, and Healthcare.

A position paper should address one or more of the following questions. Authors should feel free to add more questions as they see fit.

- What makes CPS security different from traditional IT security?
- What is the current state-of-the-art in CPS security?
- What are some grand challenges for CPS security?

- Can different degrees of security be applied to CPS?
- Can security and hard real-time constraints co-exist?
- What physical properties of CPS influence security/cryptography and vice-versa?
- How does network infrastructure need to change in order to support security in large-scale distributed CPS?
- What new scientific foundations (e.g. temporal security, dynamics-based cryptography, location-based encryption/decryption) need to be explored for security in CPS?
- Does the distributed nature of ICS and critical infrastructure help or hinder security? How can any hindrances be removed?
- What are good architectures and programming paradigms for secure CPS?
- What new operating systems, components and services are suited for securing CPS?
- What human factors challenges that are unique to CPS security?
- What are possible appropriate analytical frameworks for the assessment of CPS reliability, security, and risk?
- What are the viable approaches for addressing economics of security measures so as to justify related expenditures?
- How can we address the formulation of appropriate policy for security measures?

Poster Submission

Inviting one page submission for Posters. The deadline for submitting the poster description is July 6, 2009. Please email a pdf copy of the description to Basit Shafiq at basit@andromeda.rutgers.edu .

Paper Submission

Submission site: <http://www.easychair.org/conferences/?conf=cpssw09>

Important Dates

- **July 6, 2009**—Deadline for submitting poster description.
- **June 8, 2009**—Deadline for submitting position paper.
- **June 29, 2009**—Author notification
- **July 22–24, 2009**—Workshop

Travel and Lodging Support for Students

PhD students are encouraged to apply for Travel & Lodging support - the first 6 students will receive such a support. To apply for travel & lodging support, Please send a copy of your resume including a description of your research work to “Mr. Ron Bilbrey” at Ron.Bilbrey@associates.dhs.gov. Also copy Dr. Nabil Adam (Nabil.Adam@dhs.gov) in the email. For more information, please visit <http://civic.rutgers.edu/> .



Registration

Workshop attendance is open subject to space availability, with July 10 as the cut-off date. Workshop registration is free. For registration detail and for an up-to-date copy of this workshop write up, please visit:

<https://www.enstg.com/signup/passthru.cfm?ConferenceCode=WOR89068>

Workshop Venue

This workshop is scheduled for July 22–24, 2009 at the Hilton Newark Penn Station, Newark, NJ.

Hotel Accommodation

Hilton Newark Penn Station

Gateway Center–Raymond Blvd, Newark, New Jersey, United States 07102-5107
Tel: 1-973-622-5000 Fax: 1-973-824-2188. The hotel offers a block of rooms at the government rate of \$133.00 per night, with July 6 as the cut-off date.

Workshop on Future Directions in Cyber-Physical Systems Security

AGENDA Wednesday July 22, 2009

12:00–1:00 pm	Registration (Outside Garden State Ball Room)
1:00–1:10 pm	Workshop Kickoff Nabil Adam , DHS-Science and Technology Directorate (Garden State Ball Room)
1:10–1:25 pm	Welcome Address by Christopher Doyle , DHS-Science and Technology Directorate (Garden State Ball Room)
1:25–1:55 pm	DHS Perspective Speaker- Philip Reiting , Deputy Undersecretary of National Protection & Programs Directorate, DHS (Garden State Ball Room)
1:55–2:25 pm	NSF Perspective Speaker- Jeannette Wing , Asst. Director, National Science Foundation (Garden State Ball Room)
2:25–2:40 pm	Break
2:40–3:10 pm	DOE Perspective Speaker- Thomas Malec , Department of Energy (Garden State Ball Room)
3:10–3:40 pm	NIST Perspective, Speaker- George Arnold , National Coordinator for Smart Grid Interoperability (Garden State Ball Room)
3:40–4:00 pm	NJHSP Perspective, Speaker- Richard L. Cañas , NJ Office of Homeland Security and Preparedness (Garden State Ball Room)
4:00–4:15 pm	Break
4:15–5:45 pm	Owners/Operators and State Representatives Panel (Garden State Ball Room)
	Speaker—Representatives from Valero, Verizon, Bank of America and American Water State Representatives: K. Wood (MD), S. Popat (DC), R. Dixon (WV), R. Keener , M. McAllister (VA), J. Conrey (NJ), TBA (NY), TBA (PA), and E. Starkey (DE). (members of the All Hazards Consortium) Chair – Joe Conrey
6:00–7:30 pm	Reception (Essex Room)



Workshop on Future Directions in Cyber-Physical Systems Security

AGENDA

Thursday July 23, 2009

7:00–8:00 am	Continental Breakfast (Bergen Room)		
8:00–8:10 am	Welcome Back, Christopher Doyle , DHS-S&T (Garden State Ball Room)		
8:10–8:30 am	Welcome Remarks by Mildred Crump , City Council President, Newark, NJ (Garden State Ball Room)		
8:30–9:00 am	DOD Perspective Speaker- Robert F. Lentz , Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance, DOD (Garden State Ball Room)		
9:00–10:30 am	Industry Panel (Garden State Ball Room)		
	Microsoft (Kevin Sullivan), IBM (Chung-Sheng Li) Raytheon (Steve Hawkins), United Technologies (Claas Jacobson), Cisco Systems (Dave Dalva), Siemens (Yan Lu) Chair – Riley Repko, USAF		
10:30–10:45 am	Break		
10:45–12:15 pm	Position Paper Sessions (parallel sessions) See below for list of papers in each session		
	Session 1 Chair – Raj Rajkumar (Monmouth Room)	Session 2 Chair – Peter Chen (Seth Boyden Room)	Session 3 Chair – Insup Lee (Menlo Park Room)
12:15–1:15 pm	Lunch (on your own)		
1:15–2:45 pm	Sectors Panel (Garden State Ball Room)		
	Lydia Duckworth (Healthcare); Walter Heimerdinger (Process Con) Scott Lintelman (Air Transportation); Paul Myrda (Electricity) Chair – Dr. William Sanders, UIUC		
2:45–3:00 pm	Break		
3:00–4:15 pm	Breakout Sessions (Working Groups 1 – 3)		
	WG1.1 Chair– Riley Repko Co-chairs– Lydia Duckworth; Scott Lintelman; (Monmouth Room)	WG2.1 Chair– James St. Pierre Co-chairs– Stephen Curren; Mark Hadley; Cherrie Black (Seth Boyden Room)	WG3.1 Chair– Norman Fosmire Co-chairs– Richard Andres; Michael Mason; Cal Jaeger (Menlo Park Room)
4:15–4:30 pm	Break		
4:30–5:30 pm	Breakout Reports (Garden State Ball Room)		
	WG1.1 Report, Speaker: Riley Repko ; WG2.1 Report, Speaker: James St. Pierre ; WG3.1 Report, Speaker: Norman Fosmire ;		
5:30–6:45 pm	Poster Session (Garden State Ball Room)		

Workshop on Future Directions in Cyber-Physical Systems Security

AGENDA Friday July 24, 2009

6:45–7:45 am	Continental Breakfast (Bergen Room)		
7:45–8:30 am	Venture Capital Firms Panel (Garden State Ball Room)		
	Speaker – Jack Biddle, Novak Biddle Elad Yoran, Security Growth Partners LLC Edward Merrill, Granite Gate Corp. Chair – Riley Repko, USAF		
8:30–9:15 am	Position Paper (Garden State Ball Room) See below for list of papers in this session		
	Session 4 Chair – Yelena Yesha		
9:15–10:30 am	NSF/NITRD Panel (Garden State Ball Room)		
	Ty Znati (NSF) Helen Gill (NSF) Lenore Zuck (NSF) Frankie King (NITRD) Chair– Raj Rajkumar (CMU)		
10:30–10:45 am	Break		
10:45–12:00 pm	Breakout Sessions (Working Groups 1 – 3)		
	WG 1.2 Chair– George Gross Co-chairs– Craig Rieger; Clas Jacobson (Monmouth Room)	WG 2.2 Chair– Raj Rajkumar Co-chairs– Cal Jaeger; Dave Dalva (Seth Boyden Room)	WG 3.2 Chair– Peter Chen Co-chairs– Steven Fernandez; Walter Heimerdinger (Menlo Park Room)
12:00–1:00 pm	Breakout Reports (Garden State Ball Room)		
	WG1.2 Report, Speakers: George Gross WG2.2 Report, Speakers: Raj Rajkumar WG3.2 Report, Speakers: Peter Chen		
1:00–1:10 pm	Closing Remarks by Nabil Adam (Garden State Ball Room)		
1:10 pm	Adjourn		

