Integrating Cyber-Physical Research and Thinking in College Education

Georgios Varsamopoulos[1], Sandeep Gupta[1], Ayan Banerjee, Krishna K. Venkatasubramanian[2]
{georgios.varsamopoulos,sandeep.gupta,abanerje}@asu.edu, vkris@cis.upenn.edu
[1] Arizona State University, Tempe, Arizona
[2] University of Pennsylvania, Philadelphia, Pennsylvania

Abstract

Cyber-physical system (CPS) research has been a recent yet strongly supported area by NSF. CPS is any computing system which has significant and tight interdependence among its cyber part (i.e., computing functionality), its physical part and the environment (i.e., behavior). A large issue with teaching CPS (and even researching about them) is that they break out from current disciplinary conventions: although we can argue and reason about the separate aspects of a CPS—its physics, its mechanics, its computing—there is no single theory or set of principles that govern the tight coupling of these aspects. In teaching about CPS at Arizona State University, we focus on cultivating *cyber-physical thinking*, a spin-off of *computational thinking*.

1. Introduction (What is CPS and why teach CPS?)

The notion of *cyber-physical system* (CPS) was keyed by James Truchard from National Instruments in 2006. He demonstrated the concept of a CPS by use of a LEGO® MINDSTORMS® NXT robot and stressed on the "deeply integrated, real-time interaction between computer and physical components." [1]. It rapidly caught on with NSF and expanded its application domain beyond robotics into smart power grids (the 2003 northeast blackout memories were fresh back then), avionics, automobiles, medical devices, and homeland security. Now, when we talk about a cyber-physical system, we talk about any system whose physical interaction with the environment has a tight, two-way interdependence with its computing functions.

2. CPS education at Impact Lab, ASU

The Impact lab has been working on CPS research for several years. Research projects include: i) the profiling of wireless sensing node operation on human tissue, with the objective to adjust the node's operation to minimize the adverse health effects on the tissue; ii) providing cyber-physical security on embedded computing systems; iii) improving the sustainability of large scale data centers. On applying the results of that research into teaching, we devise material and assignments that promote ***cyber-physical thinking*** *and* ***design***, i.e. when designing a system one should consider both the computing and physical behaviors. This concept relates to *co-design*, with the difference that co-design has to do with designing two separate system components with the same objective, while cyber-physical design is about designing one system component for two objectives: a computing objective and a physical objective.

To that extend, research at the Impact Lab has set forth a terminology for cyberphysical systems and their interactions with their environment as follows.

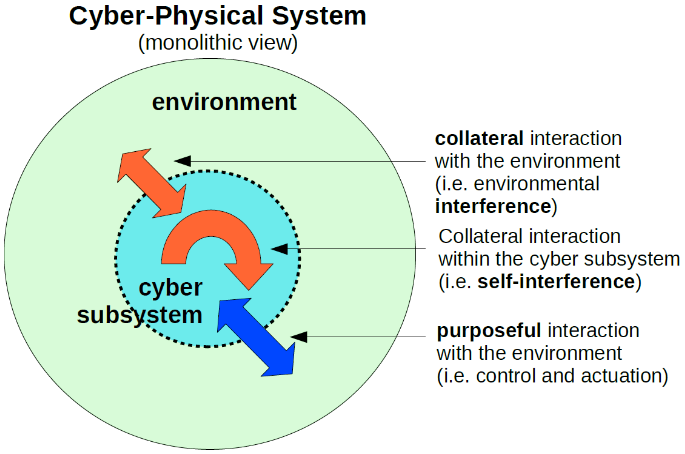
Cyber-Physical System
(monolithic view)
environment
cyber subsystem
collateral interaction with the environment (i.e. environmental interference)
Collateral interaction within the cyber subsystem (i.e. self-interference)
purposeful interaction with the environment (i.e. control and actuation)

Figure 1: Conceptual view of a CPS

Hosting environment (in short, ***environment***) is defined as the physical place where a CPS is installed and operating, as well as the natural pattern of activities conducted in the environment. The environment can be a natural or a constructed area. ***Control volume*** is the three-dimensional space of the environment which the interference can impact, including the contained objects. CPS may be a system whose operation may casually or collaterally affect or be affected by the environment. Distributed CPSs (i.e., DCPSs) consist of distinct and autonomous computing nodes. ***Interference*** is the casual1 exchange of some form of energy among the nodes and the environment, which has the potential to affect the operation of the DCPS or the conditions of the environment. Considering the structural decomposition of an DCPS, the interference can be classified to the following types:

- ***Cross-interference***: this is defined as the interference among nodes of a DCPS. One example of interference is the increased probability of failure of an overheated caused by heat arriving from other servers. Another example, mentioned in [2] [3], is that radio transmission can cause interference in circuitry. A third example is from [4], where sensors with different modalities are deployed to sense magnetic, acoustic, seismic, and optical data. The existence and operation of one optical sensor may influence the reading of another magnetic sensor.
- ***Self-interference***: the cross-interference of a node onto itself. The operation of a node may degrade its own performance or lead to a loss of functionality. In monolithic, centralized CPSs, the cross-interference reduces to self-interference only, as there is only one component.
- ***Environment interference***: the interference of the systealm to the environment and vice versa. Environment interference is distinguished into interference ***to*** the environment and interference ***from*** the environment.

Condition variable is an observable, and desirably predictable, quantity that describes one aspect of the system's or environment's condition. Examples of condition variables are temperature, pressure or sound level. Condition variables are associated with a spatial point in the control volume. A model that describes how a condition variable's values are affected with respect to the distributed energy consumption of the DCPS is referred to as ***interference mode***l, and a condition variable is then referred to as interference effect variable. Also, there are certain safety constraints that are associated with a condition variable (usually expressed as upper or lower value limits).

The following section provides three examples of what results where produced at the Impact Lab in CPS research and how they can be introduced in academic curricula.

3. Examples of integrating cyber-physical research into teaching courses

3.1. Safety in medical devices

In this example, we consider medical device cyber-physical systems and their networks called Body Area Networks (BANs) used for critical health care applications such as patient monitoring and drug diffusion. Safety is essential given the mission critical deployments of medical devices. ISO 60601 defines safety as the avoidance of hazards to the physical environment due to the operation of a medical device under normal or single fault condition. We believe that this definition of safety can also be applied to CPSes in non-medical domains by broadening the scope of hazards considered, including faulty operation of the computing unit, radiation leaks, thermal effects, bio-compatibility issues, software failures, mechanical, and electrical hazards. However, in case of medical devices patient safety due to hazardous effects of the dynamic cyber-physical interactions with the medical device is essential.

Traditionally, researchers have focused on bypassing this dynamic interaction and transforming the safety assurance problem into a well understood problem in computer science such as formal model reachability analysis. In this regard, several static assumptions on the interaction has been considered, which abstract out the dynamic nature of the physical environment. For example, in works such as [5], [6], infusion pump software has been modeled using a timed automata. The diffusion process is simplified so that the drug concentration in the blood is incremented by the infusion rate instantaneously. The problem of safety assurance is consequently reduced to developing bug free software or a control system analysis problem. Such simplified notion of safety, however, may not entirely capture the hazards resulting from the dynamic cyber-physical interactions. For example, infusion pumps for chemotherapy require characterization of the spatial extent to which the drug diffuses. In case of pumps used for anesthesia [7], the safety analysis requires the time taken for the drug to reach a particular concentration. Hence in order to guarantee safety of CPS software it is necessary to accurately characterize the spatio temporal dynamics of the physical environment and its tight coupling with the computing units. In essence more focus is needed on the *interference safety*.

Interference safety hazards can occur due to different kinds of cyber-physical interactions, i.e. cross-interference (e.g. headphones are reported to interfere with pacemakers of heart patients, see http://www.medicaldevicesafety.org/), interference to the environment, and interference from the environment (e.g. tissue growth around the implanted sensors can hamper sensing and communication capabilities).

Addressing interference safety is a challenging task. Principally, it requires exact understanding of the physical processes of the environment and the properties of the computing unit that affect the physical processes. This usually also means considering the *spatio-temporal* nature of cyber-physical interference.

3.1.1. Solution

CPSes leverage information from their physical environment for their effective operation. Hence, any solution to safety, security or sustainability of a CPS should consider the physical environment as an important component of the entire CPS. Such considerations necessitate characterization of the cyber-physical interactions and their incorporation in the design of CPSes. Characterization of cyber-physical interactions includes determining: i) the effects of computing operation on the interaction parameters, ii) the effects of the physical processes in the environment on the interaction parameters, and iii) the effects of the interaction parameters on the computing unit and physical environment. Well defined theories in the domain of computer science can effectively characterize the computing operation of a CPS. Similarly, well defined techniques in domains such as thermodynamics, mechanical engineering, and chemical fluid dynamics can be used to characterize physical processes. The interaction parameters however, should be coupled with both the computing and physical processes for a cyber physical interaction to exist. Their characterization should involve unification of theories from different disciplines.

For instance a model predictive infusion controller can be designed, which decides on the future infusion rate, in order to maintain unconsciousness of the patient without causing respiratory distress [8]. In this regard, a mathematical representation of the drug diffusion process is required, which can be obtained from the theories of fluid dynamics. Subsequently the techniques of control theory can be employed with this model to design the controller. *We hypothesize that any cyber-physically oriented solution to safety would involve synergistic employment of various approaches and techniques from different domains of science.*

Some recent research endeavors in solutions for CPS problems have concentrated on this unification. The need for computer scientists to understand the operation of the physical environment has been stressed in [9]. The authors in [9] propose a methodology to consider the operation of the physical environment in any given domain. The idea is to consider the physical system as a black box and study its behavior. Then mathematical abstractions can be developed that represents the behavior of the physical system, also called *behavioral models*. Such a *model based approach* to the unification of different disciplines is essential for designing safer CPSes.

Research efforts in this regard have resulted in modeling frameworks [10], which can be used for medical devices to model them as cyber-physical systems. Abstract models of the computing system and the human body can be developed to represent critical medical scenarios. Given these models two types of analysis are performed: a) simulation on a given set of test cases and b) formal model checking analysis. In this regard, BAND-Aide, a modeling and analysis framework for BANs, is proposed, which uses abstract behavioral models and a generic simulation analysis algorithm [10] to evaluate safety of BANs.

For model checking purposes, hybrid automata based formal models has been recently considered, for modeling medical devices. However, a Spatio-Temporal Hybrid Automata (STHA) [11] that captures the spatio-temporal cyber-physical interactions is necessary. Figure 2 shows the variation of skin temperature over space for the operation of two sensors on the human body. A formal model generally represent a system as a collection of states and a set of dynamic equations that define the evolution of the states. Traditionally a state is defined as a collection of variables (called state variables), which vary over time and a set of ordinary differential equations, which govern this variation over time. However, in STHA, a state should represent the system properties and their variations at a particular time and space. As shown in Figure 2, depending on the magnitude of temperature rise the spatial region, at a particular time, can be partitioned into states. These partitions vary over time resulting in spatio temporal variation of the state variables. Such variations are often characterized by spatio-temporal partial differential equations. In a traditional formal model, the temporal variation of the variables result in events, which causes transition of the system from one state to another. However, in STHA since the state variables vary over both space and time the events causing state transitions can be spatio-temporal in nature.

A STHA model can be used for model checking purposes for a CPS. One of the main analysis techniques for model checking is the reachability analysis [12]. The reachability analysis can be used to perform safety analysis by marking a subset of states as *unsafe*. While performing reachability analysis if those states are reached then the system operation can be concluded as *unsafe*. Current techniques to analyze hybrid automata [12] support system evolution in only one dimension (time). However, STHAs require evolution in four dimensions. This not only renders the current available analysis tools inapplicable but also increases the analysis complexity. Reachability analysis technique for STHA model can be performed by discretization of space and time dimensions. In this analysis, the continuous dynamics of the hybrid automata is evaluated by performing fixed point computations of the specified equations. Then the discrete state transitions are simulated based on the transition conditions to determine the states that can be reached from an initial state [12]. This can be done by setting an initial state, incrementing time and checking the reachable states as the continuous dynamics evolves.

3.1.2. Educational Outcomes

The impact lab over the years have incorporated research findings in the area of cyber-physical system safety verification into graduate and undergraduate courses. Currently, there is a lack of training of new graduates in theories, formal methods and tools for both cyber-physical system analysis and synthesis. The tools that are developed in this research such as BAND-AiDe [10], spatio-temporal formal models [13] are incorporated in courses such as green computing (http://impact.asu.edu/cse591gc.html) and mobile computing (http://impact.asu.edu/cse598fa11.html). Courses like these will serve as vessels to introduce the concepts, theory and tools of STHA, which we predict that they will be crucial educational asset for future “CPS engineers”. Also impact lab has been actively involved in teaching engineering courses to 8th and 9th graders and are introducing the basic concepts of automata and cyber-physicality in those curricula.sdf

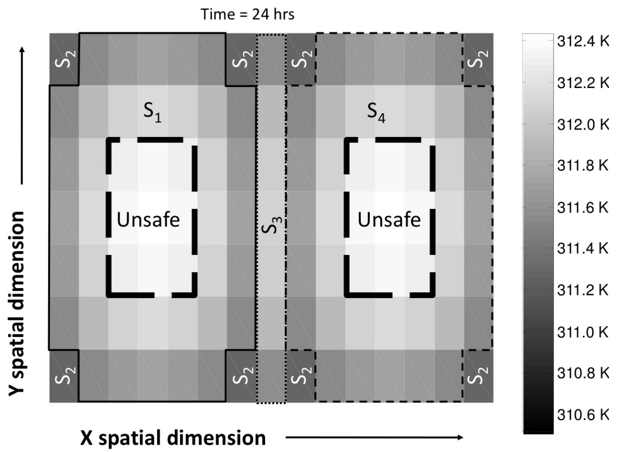

Figure 2. Temperature distribution across tissue.

3.2. Example 2: Task placement in data centers

During the past few years, with the prevailing usage of data centers for data processing, data storage, and communications networking, the heat dissipation density of data centers increases exponentially. Improperly designed or operated data centers may either suffer from overheated servers and potential system failures, or from over-cooled systems and paying extra utilities costs. The goal of this work is to find task placements (i.e., server assignments) so as to lower energy costs, reduce system failure rates, and consequently, optimize computing resources and minimize business expenditures.

A typical data center is laid out in a hot-aisle/cold-aisle arrangement, with the racks installed on a the raised floor which features perforated tiles. The air conditioners, normally referred to as *computer room air conditioner* (CRAC), deliver cold air under the elevated floor. This is referred to as *cool air*. The cool air enters the racks from their front side, picks up heat while flowing through these racks, and exits from the rear of the racks. The heated exit air forms hot aisles behind the racks, and is extracted back to the air conditioner intakes, which, in most cases, are positioned above the hot aisles. Each rack consists of several chassis, and each chassis accommodates several computational devices (servers or networking equipment).

The *recirculation* of hot air, i.e. *thermal interference*, from the air outlets of the IT equipment back into their air inlets (see Figure 3 increases the inlet temperatures and can cause the appearance of hot spots [14], [15]. Heat recirculation forces data center operators to operate their CRACs to supply cold air at a *much* lower temperature than the redline (although in the ideal case of no recirculation it could be equal to the redline temperature). Lowering CRAC's output temperature forces it to operate at a worse *coefficient of performance*, i.e. the ratio of

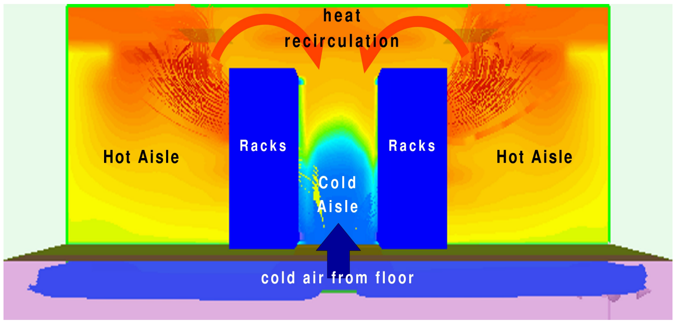

Figure 3. Recirculation in a data center.

the removed heat over the energy required to do so, which considerably increases the cooling cost.

The projected problem is ***how to assign (i.e., place) an incoming HPC job to the data center servers so that the requirement for cool air supply is minimized, thus allowing for the supply of warmer and cheaper cool air by the CRACs***. The problem was studied in [16].

3.2.1. Solution

The following solution is to map the data center to a CPS scheduling problem [18]: A CPS is assigned to execute a set of ***tasks***. The tasks can be assigned to any node and at any time within the given ***computational constraints***. The execution of each task causes interference, which can vary depending on the location and time of the execution. In addition to the computational constraints, there usually is an ***optimization objective***. Depending on whether the optimization is oriented toward computing performance or toward energy efficiency, a schedule will have to optimize a metric such as *throughput*, *makespan* (i.e., the length of the schedule), *total energy consumed*, or *average power*.

The CPS can then be modeled a way as depicted in Figure 4. The scheduler assigns tasks, which then generate heat when executed according a task-to-power function *G*, the heat is distributed across the CPS and its environment according to an interference function *F*, where the various conditions variables are affected at the designated *victim* entities.

The scheduling problem can be solved in the following manner

1. Determine the task-to-power function *G*.
2. Characterize the interference effect function *F*.
3. Define the physical constraints on the condition variables
4. Formalize the optimization objective function *H*.
5. Identify an optimal schedule that satisfies the constraints while optimizing the objective function *H*.

In the case of a data center, the task-to-power function of a computing server *i* is modeled as:

$$p_i = q\, b_{ij} + a_i,$$

where b_{ij} is the liner coefficient of server *i*'s power when running task T_j. This is a *linear* power model with respect to CPU utilization. Since a node has multiple blade servers, each server may be assigned to a separate task. Let **C** be the *task allocation matrix*, where each element c_{ij} denotes that c_{ij} servers are allocated to task T_j on node *i*. Then, the power consumption of node *i* is:

$$G_i() \equiv p_i = \Sigma_j c_{ij}\, b_{ij} + a_i \;\; \Rightarrow \boldsymbol{p} = \boldsymbol{C}\boxdot\boldsymbol{B} + \boldsymbol{a},$$

where $\boxdot$ stands for the row-for-row product of two matrices, yielding a vector. With a very small error, all the electric power is assumed to convert into heat.

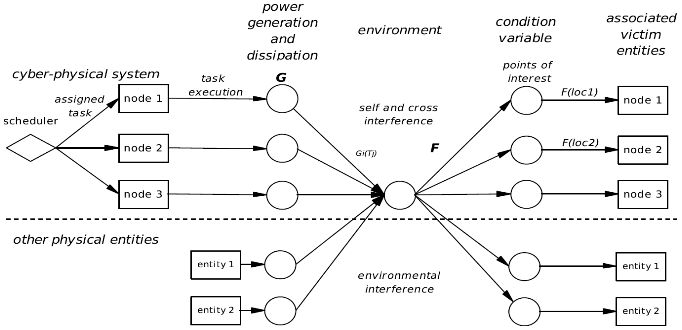

Figure 4. Modeling the heat interference effects in a CPS such as a data center.

In this application example, the heat interference is the recirculation of heat. The condition variables are the temperature rise at the server inlets, and we define the interference function as the vector of the temperature rises.

$$F \equiv \Delta\boldsymbol{T}_{\mathrm{in}} = \boldsymbol{\varphi Q_{in}} = \boldsymbol{\varphi D p} = \boldsymbol{\varphi D}[\boldsymbol{C}\boxdot\boldsymbol{B}+\boldsymbol{a}],$$

where D is the heat distribution matrix between each pair of nodes. The objective function H is then defined as the maximum of the vector $\Delta\boldsymbol{T}_{\mathrm{in}}$:

$$\mathrm{H} \equiv \max \Delta\boldsymbol{T}_{\mathrm{in}}.$$

Recall from above that the task allocation matrix $\boldsymbol{C}=\{c_{ij}\}_{\mathrm{n\times m}}$ denotes how many servers from each node *i* are allocated to task *j*. The sum of server assignments to tasks per node *may not* exceed the available processors on that node, i.e.,

$$\Sigma_{\mathrm{j=1}}^{\mathrm{m}}\; c_{ij} \leq q, \forall i=1\ldots\mathrm{n},$$

and the sum of processor assignments per task *must* be equal to the number of processors it requires, i.e.,

$$\Sigma_{i=1}^{\mathrm{n}}\; c_{ij} \leq \mathrm{Req}(j)\;, \forall j=1\ldots\mathrm{n},$$

The problem of minimizing the temperature rise can be now stated as an integer linear programming (ILP) problem, where H is the optimization objective, and the constrains are as described above.

3.2.2. Educational Outcomes

Optimization of power consumption or performance in CPS is a fundamental task, and CPS engineers should be able to formulate such problems and be able to solve them. Curricula can include assignment tasks such as:

- *Abstraction-to-specialization assignments*: Given an informal description of a CPS, identify the nodes, environmental entities, interference, condition variables, computational and physical constraints. The students should be able to modify the interference flow model of Figure 3 to the needs of the application.
- *Quantitative assignments*: Profiling methodologies for determining the function *G*, or other experiments to determine function *F*. These assignments require efficiency in executing experimental methods, and also skills in proper mathematical formulation of the optimization problems.

Such material has been introduced and used in a guest lecture in CSE591 "Theoretical Aspects of Cyber Physical Systems" (http://www.public.asu.edu/~gfaineko/courses/cse591/2010/schedule.html).

3.3. Example 3: Security in Cyber Physical Systems

Security of a CPS is defined as the ability to ensure that both data and the operational capabilities of the system can only be accessed when authorized. Security for CPS is a relatively new area. The need for security in CPS is many-fold. Some of the main factors are:

- *Mission Critical Nature*: CPSs are often used in mission critical applications. Therefore, any security compromise of either the cyber system or physical environment of a CPS can have profound consequences. This also makes them more likely targets for attacks. A case in point is the attack on pacemakers which not only forced them to reveal a patient's electrocardiogram (EKG) data but also actuate an untimely shock [22].
- *Information Sensitivity*: CPSs are privy to detailed and often sensitive information about a critical physical process. If this information is available to malicious entities, it can be exploited leading to loss of privacy, abuse and discrimination. For example, unauthorized knowledge of the electricity consumption of a neighborhood from a smart-grid CPS can result in socket-bombing attacks on households.
- *Ability to Actuate*: CPSs have the ability to actuate changes to the physical environment. Allowing unauthorized parties to actuate untimely changes to the physical environment can cause harm to the environment itself. For example, malicious entities can easily shutdown a CPS controlling an automobile leading to issues ranging from inefficient fuel consumption to brake-failure.

Addressing security presents for CPS numerous challenges. Traditional computer security work has focused mainly on the cyber attacks related to the cyber element, such as brute force attacks on session keys. With CPS, as both the attack on and effect on physical environment has to be considered in tandem with the cyber. An important consequence of this realization is that as with the traditional cyber security, it becomes imperative to be able to detect attacks and identify attackers who mount purely physical or hybrid attacks, this is a non-trivial task and needs efforts in multiple channels of operation and not cyber-alone. Additionally, the deployment of CPSs is not limited to specialized systems managed by tech-savvy people. Many of the applications of CPSs are systems of every-day use operated by non-technical people. Therefore, security solutions for CPSs should have a high degree of usability a characteristic that today's cyber-only security solutions only minimally possess.

3.3.1. Solution

In designing security solutions for CPS, one should not only consider the properties of the cyber components involved (CPU, RAM, ROM, data rate), but also the interaction of the components with the physical environment. In this regard, a novel perspective on securing CPS which takes this property into account, called Cyber Physical Security Solutions (CYPSec) was proposed in [19]. CYPSec solutions are environmentally-coupled security solutions, which take traditional security primitives along with the environment knowledge/ information to operate [19]. The idea is to use the monitoring capability of CPSs to provide security, by utilizing capabilities intrinsically linked to CPS operation and not something that is added from outside operational system to protect it from threats. Another merit of CYPSec solutions is that they can now harness the complex and dynamic nature of the physical environment for security purposes. Some of the principal characteristics of CYPSec solutions are:

- *Usability*: By using environment characteristics as a basis for security primitives, security deployment and management abstractions need not be actively considered freeing the users to focus on functional aspects of the system.
- *Emergence*: CYPSec solutions are designed to not only provide the appropriate security functions for which they are designed for example confidentiality, integrity, and availability but also demonstrate additional ``allied" properties, such as authentication, interoperability and adaptivity.

As CYPSec solutions have both cyber and physical aspects to them, enabling them usually requires integration of techniques from other domains with security. Further, as the solutions work in tandem with existing infrastructure, they should be implementable with well-defined computational primitives. Ultimately, securing CPS requires enabling: sensing security: deals with the validity and accuracy of the sensing process; storage security: required to prevent both cyber and physical tampering of any data stored by the CPS; communication security: required for securing both inter and intra-CPS communication from both active (interferers) and passive (eavesdroppers) adversaries; actuation control security: ensuring that no actuation can take place without the appropriate authorization; and feedback security: ensuring that the control systems in a CPS which provide the necessary feedback for effecting actuation are protected.

To demonstrate the capability of CYPSec solutions, we present two examples that demonstrate its use in providing communication and actuation security, respectively. The first example deals with establishing a cryptographic key between two entities within a health monitoring CPS. The idea is to use physiological parameters based features as a way to hide the keys during exchange, thereby eliminating the need for explicit key pre-deployment [20]. The second is an adaptive and proactive access control model for emergency management in generic smart-infrastructure CPS. The proposed approach combines role-based access control with stochastic planning methods to provide the right set of subjects, the right set of privileges, at the right time, for the right duration of time for controlling emergencies [21]. We chose the two application domains as they are: 1) good representations of CPS, and 2) they demonstrate the applicability of CYPSec solutions for meeting two diverse security requirements - communication and actuation.

3.3.2. Educational Outcomes

Specific educational outcomes of developing security solutions for CPS include the following:

- Security by nature requires thinking out of the box and identifying ways to attack a system from within and without. Given the tight coupling between the cyber and the physical in CPS, this is will become imperative rather than an aside. This will force students and the next generation of security experts to think of more holistic ways of attacking a system. This will also allow them to then develop solutions to address the attack vectors thus identified.

- Just as in Example 1, the consideration of co-operation of the computing system with the physical environment in developing security solutions will result in interdisciplinary approach towards teaching computer security.
- Development of simulation and emulation environments that model many of the physical dynamics of the CPS will allow students to design security for CPS and simulate various forms of realistic simulated attack scenarios to identify and improve it from a security stand-point.

4. Conclusions

From the above examples, research on CPS has been producing results including:

- Conceptual abstractions, such as the CPS interference terminology and the abstract interference model in Figure 3.
- Quantitative models, such as the *Spatio-Temporal Hybrid Automata*, and the *Heat Interference Matrix*.
- Methodologies of going from a informal descrption of a scheduling issue in a CPS, to a formal, quantitative problem.
- Introducing cyber-physical security features, such as *usability* and *emergence,* that go beyond traditional security considerations.

The study of CPS is inherently an inter-disciplinary subject, and does not conform to the standard division of disciplines: students either learn physics, or learn mechanics, or electrics, or computing etc.

References

[1] Business Wire, “NI CEO Gives Keynote Address at National Science Foundation Workshop”, Oct. 2006.

[2] T. R. F. Fulford-Jones and G. -Y. Wei and M. Welsh, A Portable, “Low-Power, Wireless Two-Lead EKG System”, IEEE EMBS conference, Sept. 2004.

[3] Prabal Dutta and Mike Grimmer and Anish Arora and Steve Bibyk and David Culler. “Design of a Wireless Sensor Network Platform for Detecting Rare, Random, and Ephemeral Events”. IPSN conference, 2005.

[4] Arora, A. and Dutta, P. and Bapat, S. and Kulathumani, V. and Zhang, H. and Naik, V. and Mittal, V. and Cao, H. and Demirbas, M. and Gouda, M. and others. “A line in the sand: a wireless sensor network for target detection, classification, and tracking”. Computer Networks, 46(5):605-634. 2004.

[5] Raoul Jetley and S. Purushothaman Iyer and Paul L. Jones. “A Formal Methods Approach to Medical Device Review”. IEEE Computer, 39(4):61-67, 2006

[6] Arney, David E. and Jetley, Raoul and Jones, Paul and Lee, Insup and Ray, Arnab and Sokolsky, Oleg and Zhang, Yi. “Generic Infusion Pump Hazard Analysis and Safety Requirements Version 1.0”. ScholarCommons@Penn, 2009.

[7] Wada, D.R. and Ward, D.S.. “The hybrid model: a new pharmacokinetic model for computer-controlled infusion pumps”. IEEE Transactions on Biomedical Engineering, 41(2):134-142, 1994.

[8] Jacobs, J.R.. “Algorithm for optimal linear model-based control with application to pharmacokinetic model-driven drug delivery”. IEEE Transactions on Biomedical Engineering, 37(1):107-109, 1990.

[9] Jan C. Willems. “The behavioral approach to open and interconnected systems”. Control Systems Magazine, 2007.

[10] Ayan Banerjee and Sailesh Kandula and Tridib Mukherjee and Sandeep K.S. Gupta, “BAND-AiDe: A Tool for Cyber-Physical Oriented Analysis and Design of Body Area Networks and Devices”. ACM TECS, 2010.

[11] Ayan Banerjee, Tridib Mukherjee, Sandeep K. S. Gupta. Spatio-temporal Hybrid Automata. Under review.

[12] Goran Frehse. PHAVer: Algorithmic Verification of Hybrid Systems Past HyTech. HSCC, 2005.

[13] Ayan Banerjee, Sandeep K. S. Gupta. “Ensuring Safety of medical devices”. Under review.

[14] Cullen Bash and George Forman. “Cool Job Allocation: Measuring the Power Savings of Placing Jobs at Cooling-Efficient Locations in the Data Center”

[15] Ratnesh K. Sharma and Cullen E. Bash and Chandrakant D. Patel. “Dimensionless Parameters for Evaluation of Thermal Design and Performance of Large Scale Data Centers”. Proceedings of the American Institute of Aeronautics and Astronautics (AIAA). 2002.

[16] Q. Tang, S. K. S. Gupta and Georgios Varsamopoulos. “Energy-Efficient, Thermal-Aware Task Scheduling for Homogeneous, High Performance Computing Data Centers: A Cyber-Physical Approach”. ACM Transactions on Parallel and Distributed Systems, 19(11):1458–1472, Nov. 2008.

[18] Qinghui Tang and Georgios Varsamopoulos and Sandeep K. S. Gupta. “A Unified Methodology for Scheduling in Distributed Cyber-Physical Systems”. ACM Transactions on Embedded Computing Systems. 2011.

[19] K. Venkatasubramanian, S. Nabar, S. K. S. Gupta, and R. Poovendran, "Cyber Physical Security Solutions for Pervasive Health Monitoring Systems", In E-Healthcare Systems And Wireless Communications: Current And Future Challenges, eds. Mohamed Watfa, IGI Global, 2011 (Accepted for Publication).

[20] K. K. Venkatasubramanian, Ayan Banerjee, and Sandeep K. S. Gupta, "PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks", In IEEE Transactions on Information Technology in Biomedicine (Special Issue on Wireless Health), vol. 14 (1), Jan. 2010.

[21] K. K. Venkatasubramanian, Tridib Mukherjee, and Sandeep K. S. Gupta, "CAAC - An Adaptive and Proactive Access Control Approach for Emergencies for Smart Infrastructures", In ACM Transactions on Autonomous and Adaptive Systems Special Issue on Adaptive Security, 2011 (Accepted for Publication).

[22] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. “Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses”, IEEE Security and Privacy (Oakland)2008, Oakland, CA, USA.