Ensuring Safety, Security and Sustainability of Mission-Critical Cyber Physical Systems

Ayan Banerjee[*] *Student Member, IEEE*, Krishna K. Venkatasubramanian[†] *Member, IEEE*, Tridib Mukherjee[‡] *Member, IEEE*, and Sandeep K. S. Gupta[*] *Senior Member, IEEE.*

***Abstract*—Cyber-physical systems (CPSes) couple their cyber and physical parts to provide mission-critical services, including automated pervasive health care, smart electricity grid, green cloud computing, and surveillance with unmanned aerial vehicles (UAVs). CPSes can use the information available from the physical environment to provide such ubiquitous, energy efficient and low cost functionalities. Their operation needs to ensure three key properties, collectively referred to as S3: i) safety: avoidance of hazards, ii) security: assurance of integrity, authenticity and confidentiality of information, and iii) sustainability: maintenance of long term operation of CPSes using green sources of energy. Ensuring S3 properties in a CPS is a challenging task given the spatio-temporal dynamics of the underlying physical environment. In this paper, the formal underpinnings of recent CPS S3 solutions are aligned together in a theoretical framework for cyber-physical interactions, empowering CPS researchers to systematically design solutions for ensuring safety, security, or sustainability. The general applicability of this framework is demonstrated with various exemplar solutions for S3 in diverse CPS domains. Further, insights are provided on some of the open research problems for ensuring S3 in CPSes.**

***Index Terms*—Cyber-physical systems, Safety, Security, Sustainability, Model based engineering, BANs, UAVs, data centers, smart infrastructures**

I. Introduction

Recent years have seen a dramatic rise in the development of smart and context-aware mission-critical systems that present a tight coupling between embedded computing devices and their physical environment. Representative examples include: (1) physiological sensors deployed on human body that continuously monitor the health and enable the fast detection of medical emergencies and the delivery of therapies [1]–[3], (2) smart buildings that detect absence of occupants and shut down the cooling unit [4] to save energy, (3) data-centers that use solar energy for cooling purposes [5], and (4) unmanned aerial vehicles (UAVs), that use an image of the terrain to perform surveillance [6]. A common theme in such smart systems is the role played by the underlying physical environment. The physical environment provides information necessary for achieving many of the important functionalities. Systems that use the information from the physical environment, and in turn can affect the physical environment during their operation are called *Cyber-Physical Systems* (CPSes).

The tight-coupling between the cyber and the physical in CPSes, though advantageous, is subject to new forms of risks that have not been considered adequately in the traditional computing domain. These new types of risks include the cyber element adversely affecting the physical environment (*e.g.*, untimely delivery of medication or therapies) or vice versa (*e.g.*, malfunctioning of UAV control algorithm may lead to crash of UAVs on unwanted regions causing potential loss of civilian lives). Recent works have shown that a CPS can utilize the information from the physical environment to make smart decisions for preventing these new types of hazards to both the physical environment and the computing unit thereby improving the **safety** of the CPS. For example, sensors in a body area network (BAN) can monitor their ambient tissue temperature and employ several control strategies (*e.g.*, rotate cluster leader nodes [7]) to reduce their thermal impact.

CPSes often collect sensitive and private information about the physical environment. For example, sensors in a BAN store and communicate vital signs of patients. Further, their ability to actuate change in the physical environment (*e.g.*, deliver electrical shock to the heart as in pacemakers) and their increasing pervasiveness makes them easily accessible to both legitimate users and criminals. A loss of security for a CPS can therefore have significant negative impact including loss of privacy, potential physical harm, discrimination and abuse. Though numerous security primitives have been developed in the cyber domain to address the very same issues, their applicability to the CPS domain is suspect given that they are usually complex to implement and oblivious to cyber-physical interactions. One of the ways of making **security** solutions more usable (simple) and efficient is to utilize information from the physical environment for security purposes. For example, one could use the physiological signals in a BAN to enable key agreement between sensors for trust establishment and secure communication [8].

As critical infrastructures CPSes are usually required to provide the desired services over an extended period of time with minimal maintenance. Utilizing resources from the physical environment can potentially enable a CPS to have a long operational lifetime. *Green energy* from the sun, bio-gas, and human body are used as supplement to the traditional energy sources of battery and power grid to power computing units in a CPS (green data centers [5]). This results in lower usage of energy from the battery or power grid and increases the lifetime and reduces the cost of operation of a CPS. However, due to the dynamic nature of the physical environment, the amount of available energy varies over time. In this regard, the energy availability characteristic of the environment need to be carefully considered to perform environmentally-coupled duty cycling of computing units in a CPS to **sustain** its operation using solely harvested energy [9].

To achieve safety, security, and sustainability (S3) in a

[*] School of Computing, Informatics, and Decision Systems Engineering, Arizona State University (ASU), Email: {abanerj3,sandeep.gupta}@asu.edu.

[†] Department of Computer and Information Science, University of Pennsylvania, Email: vkris@cis.upenn.edu.

[‡] Xerox Research Center, Webster, NY, Email: tridib.mukherjee@xerox.com. The work was done when the author was at ASU.

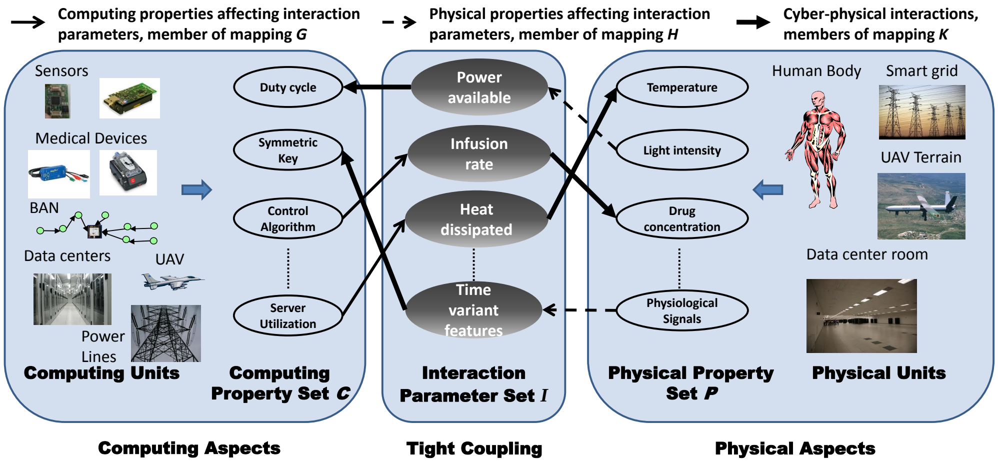


Fig. 1. **Cyber-physical systems, with tight coupling between computing and physical environment through interaction parameters.**

CPS, the computing unit needs to extract diverse types of information, related to say thermal, mechanical, and electrical properties of the environment. Design and analysis of CPSes thus requires in-depth understanding of the characteristics of these information and their effects on the computing operation. As Willems has aptly pointed out [10], systems researchers should incorporate detailed behavioral characterizations of the physical environment in the theories and techniques of computer science. Lack of such considerations results in serious violations of S3 properties. For example, in case of a pulse oximeter in a BAN, if the control of the sampling frequency is not aware of the temperature rise on human skin, severe burn hazards can occur [11]. In case of an access restricted health monitoring system, if during emergencies health data is not provided to skilled care givers, although unauthorized, life saving opportunities may be wasted. If a job scheduling operation in a sensor is not aware of the variation in the amount of energy scavenged from the green sources, then its operation may not be sustained. This stresses the need for a unified inter-disciplinary approach towards CPS design for achieving safety, security and sustainability, that combines theories from computer science with those from other sciences and engineering disciplines. Further, extensive deployments of CPSes as critical infrastructures require a low cost design and development methodology. This is especially important as the number of lines of Code (NLoC) to support complex mission-critical functionality is rapidly growing - the rate being exponential in some domains, such as avionics (http://www.nasa.gov/pdf/418878main_FSWC_Final_Report.pdf). A formal representation and analysis of CPSes enables design time feedback and correction of errors before deployment hence reducing cost incurred in redesign and risks of failure [12].

In this regard, this paper first represents CPSes in a formal framework, which enables identification of cyber and physical components and most crucially the cyber-physical interactions in any CPS. Such a formal representation enables CPS designers to better understand the required set of theories and their unification needs for an S3 ensured design. The paper then considers four CPS domains: BANs, data centers (DCs), smart infrastructures (SIs), and UAVs, and discusses some of the existing environmentally-coupled solutions to S3 for these domains. The general applicability of the formal framework is demonstrated by mapping the characteristic of the solutions to the formal constructs. The paper concludes by discussing some of the open research problems.

II. Cyber Physical Systems and S3 Issues

CPSes, as shown in Figure 1, consist of embedded computing units, which frequently interact with their physical environment to provide critical functionalities such as early detection of health problems, securing sensitive data, and enabling long term uninterrupted operation. The computing units of a CPS can be characterized by a set of quantitative properties, $\boldsymbol{C}$. These properties are related to the computing operation and are functions of the type of application executed. For example, members of $\boldsymbol{C}$ can be the utilization of a server in a data center, the initial concentration input to a drug infusion control algorithm [13], the duty cycle of a sensor, or a 128 bit key for encryption during communication. The physical environment in a CPS can be similarly characterized by a set of quantitative properties $\boldsymbol{P}$. Examples of physical properties include time varying physiological and environmental signals such as, temperature, humidity, and amount of sunlight.

In a CPS, the properties in $\boldsymbol{C}$ are closely related to those in $\boldsymbol{P}$ through physical processes that cause variation of the properties in the physical environment. Such physical processes can be characterized by a set of *interaction parameters*, $\boldsymbol{I}$. The interaction parameters can be associated with both the computing and physical properties of a CPS. Typical examples of interaction parameters include heat transferred from the servers in the data center to the ambient air, amount of energy harvested from the environment, or frequency domain features of physiological signals. Both the physical and computing properties affect the interaction parameters. The computing properties are time varying. Hence the mapping between the sets $\boldsymbol{C}$ and $\boldsymbol{I}$ can be represented by $\boldsymbol{G} : \boldsymbol{C} \times t \rightarrow \boldsymbol{I}$ (thin solid arrows in Figure 1), where t is time. The properties of the physical environment vary over both space and time. For example, temperature varies from place to place in a data center and the intensity of sunlight is low under shade and also has diurnal variation. Hence the mapping from the physical properties to the interaction parameters, $\boldsymbol{H} : \boldsymbol{P}\times t\times\{x, y, z\} \rightarrow \boldsymbol{I}$, is spatio-temporal in nature (dashed arrows in Figure 1), where $\{x, y, z\}$ represents a point in the coordinate space.

In practice mappings in $\boldsymbol{G}$ either have to be determined by performing profiling experiments, *e.g.*, utilization to power curves for a server in the data center [14], or can be a result of the execution of an algorithm. On the other hand, the mappings in $\boldsymbol{H}$ can be determined either by building of models of the physical processes, *e.g.*, electro-mechanical models of energy obtained from piezoelectric devices [15], or can be obtained through signal processing, *e.g.*, extracting security keys from physiological signals [8]. The interaction parameters define cyber-physical interactions as follows:

Definition 1: A cyber-physical interaction is an inverse mapping $\boldsymbol{K}$ from a subset of $\boldsymbol{I}$ to a subset of $\boldsymbol{P}$ or $\boldsymbol{C}$.

Example 1: Pulse-oximeter thermal effects: In case of a fingertip pulse oximeter operation [11], the sampling frequency ($\boldsymbol{C}$) affects the amount of heat dissipated ($\boldsymbol{I}$). Heat dissipated as a function of frequency ($\boldsymbol{G}$) can be obtained through power profiling of the pulse oximeter. The effect of the dissipated heat on the temperature rise of the human body ($\boldsymbol{P}$) is characterized by the Penne's bioheat equation [16]. Such a mapping is an example of $\boldsymbol{K}$. The specific heat and skin conductance of the human body also affect the temperature rise through mapping $\boldsymbol{H}$, which has to be experimentally characterized. ◇[1]

Example 2: Drug infusion: Infusion pumps operate in a close loop with physiological sensors such as glucose meter or SpO2 sensor to control drug infusion. The infusion rate ($\boldsymbol{C}$) affect the drug concentration in the blood ($\boldsymbol{I}$) through the diffusion process. The diffusion process ($\boldsymbol{G}$) can be characterized by the pharmacokinetic model [17]. The drug concentration then affects physical properties ($\boldsymbol{P}$) such as blood oxygen level, unconsciousness, or cell death rate in case of chemotherapy through physiological processes ($\boldsymbol{K}$) such as change in action potential. A control algorithm in the infusion pump takes the physical properties as input and adjusts the infusion levels so as to achieve the desired physiological effects while avoiding hazards such as respiratory distress [17]. ◇

Broadly, **cyber-physical interactions** can be of two types: a) *intended interactions*, which refer to the usage of information from the physical environment for performing useful computing operations (Example 2) and b) *unintended interactions*, which refer to the side effects of operation of the computing units on the physical environment (Example 1). Further, in case of networked CPSes, there are often combined effects of the individual interactions called *aggregate effects*, as observed in multi-channel drug infusion. A case in point is the increased death rates of cancer cell when α monoclonal antibody and mathotrexate drugs are infused simultaneously rather than when infused sequentially [18]. Given this generic model, CPS S3 properties are discussed next.

A. Safety, Security and Sustainability in CPS

In this section, intended and unintended interactions and aggregate effects are used to discuss S3 design goals of CPS.

1) Safety: Safety is essential given the mission critical deployments of many CPSes such as in health management and avionics. 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 [19]. 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.

Hazards in the physical environment can occur due to abnormal conditions on the properties in $\boldsymbol{P}$. Hence, they can be mathematically characterized as constraints on the values of the properties in $\boldsymbol{P}$. Definition 1 relates computing properties ($\boldsymbol{C}$) to $\boldsymbol{P}$ through the cyber-physical interaction mapping $\boldsymbol{K}$. Variations in the properties in $\boldsymbol{C}$ can thus cause constraint violations in $\boldsymbol{P}$. Assuring safety of the physical environment due to operation of the computing units should essentially consider characterization of the mapping $\boldsymbol{K}$.

Traditionally, researchers have focused on bypassing this characterization 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 mapping $\boldsymbol{K}$ have been considered, which abstract out the dynamic nature of the physical environment. For example, in works such as [12], [20], infusion pump software has been modeled as 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 [17], the safety analysis requires the time taken for the drug to reach a particular concentration[2]. 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 *interaction safety*.

Interaction safety hazards can occur due to different kinds of cyber-physical interactions:

- *Interaction between two computing units:* Cyber-physical interactions of two computing units in different CPSes may affect each other's operation in hazardous ways. Recently headphones are reported to interfere with pacemakers of heart patients (http://www.medicaldevicesafety.org/). The electromagnetic interaction of the headphone with the patient's body gets coupled with the electromagnetism induced by the pacemaker on the patient's heart and deactivates it.
- *Interactions from computing units to the physical environment:* Cyber-physical interaction between the computing units and the physical environment may have harmful effects on the physical environment (Examples 1 and 2).
- *Interaction from the physical environment to the computing units:* The operation of the physical environment may impose hindrance to the operation of the computing unit.

[1] ◇ - End of example marker.

[2] Rise in safety violation incidences in recent years has motivated calls [21] for FDA to reexamine the current procedure for pre-market safety evaluation of medical devices. We believe that increasing cyber-physical nature of medical devices and consequently the increase in interaction hazards should guide any policy changes in this regards.

For example, tissue growth around the implanted sensors can hamper sensing and communication capabilities.

Addressing interactions 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 interactions (mappings $\boldsymbol{H}$ and $\boldsymbol{K}$ are over space and time).

2) Security: 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 CPSes is a relatively new area. As with any new field most of the effort seems to be focused on efficiently mapping solutions from existing domains [22]. The need for security in a CPS is many-fold. Some of the main factors are:

- *Mission Critical Nature*: CPSes are often used in mission critical applications. Therefore, any security compromise of either the cyber system or the 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 [23].
- *Information Detail and Sensitivity*: CPSes 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*: CPSes 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 shut-down a CPS controlling an automobile leading to issues ranging from inefficient fuel consumption to brake-failure.
- *Ubiquity*: In a world, which is becoming increasingly dependent upon CPSes to provide automated, efficient management of essential services, care has to be taken to ensure that they are protected.

Addressing security in CPSes presents numerous challenges. Traditional computer security work has focused mainly on the cyber attacks related to the computing properties $\boldsymbol{C}$, such as brute force attacks on session keys. With CPSes this has to change, as both attacks and effects on the physical environment ($\boldsymbol{P}$) 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 CPSes is not limited to specialized systems managed by tech-savvy people. Many of the applications of CPSes are systems of every-day use operated by non-technical people. Therefore, security solutions for CPSes should have a high degree of usability, a characteristic that today's cyber-only security solutions do not adequately possess. Use of information from the physical environment can enable usable security. The following example illustrates integration of security primitives with signal processing of physiological data to achieve plug-n-play key distribution.

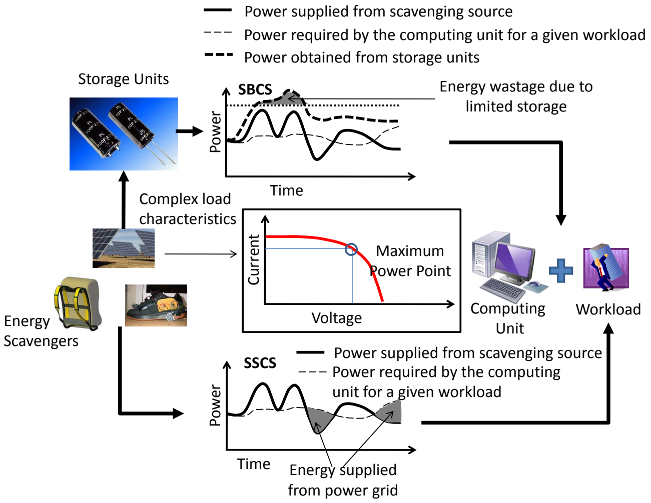

Power supplied from scavenging source
Power required by the computing unit for a given workload
Power obtained from storage units
Storage Units
SBCS
Power
Time
Energy wastage due to limited storage
Complex load characteristics
Current
Voltage
Maximum Power Point
Computing Unit
Workload
Energy Scavengers
SSCS
Power supplied from scavenging source
Power required by the computing unit for a given workload
Power
Time
Energy supplied from power grid

Fig. 2. **Power supply models of CPS: (a) green source directly supplying power, (b) green source charging a battery that feeds to the computing unit. Load characteristics of the green sources and the maximal power point for the sources to operate at maximum efficiency are also shown.**

Example 3: Physiological value based key agreement (PSKA) [8]: For a network of sensors on human body information security can be maintained by encrypting messages using keys derived from physiological parameters ($\boldsymbol{P}$) of the human body [8]. The transmitting sensor performs signal processing operations ($\boldsymbol{H}$) on the physiological signals and obtains frequency domain features ($\boldsymbol{I}$). A random key ($\boldsymbol{C}$) is generated by the transmitting sensor and is hidden with the help of the features using a fuzzy vault construct ($\boldsymbol{G}$). The vault is then transferred to the receiving sensor, which performs Lagrangian interpolation on the vault ($\boldsymbol{K}$) to extract the hidden key used for encryption. This example stresses the need for unification of approaches from different disciplines to achieve CPS security. ◇

3) Sustainability: Sustainability[3], from the energy perspective can be defined as the balance between the power required for computation and the power available from renewable or green sources (*i.e.*, sources in the environment such as solar power) [24]. Traditionally, CPS components such as sensors in BANs or servers in data centers are supplied energy from the battery or from the AC mains. However, with recent push toward alternative green sources of energy, the traditional energy supply model has to change. Figures 2 show two possible **energy supply models**: i)*Scavenging Source to Computing System (SSCS)* model, where the harvesting/ scavenging source directly supplies energy to the computing unit and ii) *Scavenging source to Battery to Computing System (SBCS)* model, where scavenging source first stores the energy to a battery and then the battery supplies energy to the computing unit. The cyber-physicality of such energy supply models can be explained using Definition 1. The properties of the physical environment ($\boldsymbol{P}$), which are utilized to scavenge energy, such

[3] Sustainability in CPS can be discussed from: (i) energy perspective; and (ii) equipment recycling perspective. The paper focuses only on the energy perspective and discuss the related issues.

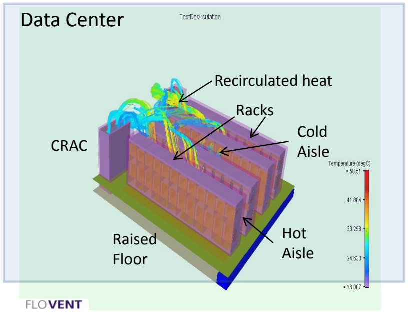


Fig. 3. **Heat recirculation in a data center**

as the intensity of sunlight, and the body temperature, affect the amount of energy available to power computing units. The amount of energy available can be the interaction parameter $\boldsymbol{I}$. The computing properties such as the allowable duty cycle, frequency of operation, or server utilization are adjusted based on the available energy. Here the cyber-physical interaction mapping $\boldsymbol{K}$ can be the result of execution of a duty cycling, frequency control or workload placement algorithm.

Cyber-physical energy supply model imposes several challenges to the sustainable design of CPSes.

- *Intermittent energy supply:* Environmental energy sources are inherently intermittent in nature. Hence there is no guarantee that the power needs of the computing units in the CPS will be met at every time instant from the green sources. As shown in the Figure 2, for the SSCS model of energy supply, often the power supply and demand does not match. For the SBCS model there is energy wastage when the amount of power obtained from green sources is greater than the amount the battery can store. To obtain a sustainable CPS design, the aggregate power demand from the computing units has to be matched by the power from scavenging sources at all instants and power wastage has to be minimized.

- *Unknown load characteristics:* The operating voltage obtained across a computing unit depends on its input impedance and the load characteristics of the source. For green energy sources the voltage and current are often related through a convex function [9] (Figure 2). The power drawn from the source is maximum at a certain voltage and current. *Hence for maximum efficiency the optimal operating voltage and current has to be determined from the load characteristic.*

The following example illustrates these challenges:

Example 4: Data center environmental aware scheduling: A data center consists of a cluster of servers networked with each other and capable of high performance computing (Figure 3). Server utilization ($\boldsymbol{C}$) has impact on the heat dissipation and temperature rise ($\boldsymbol{I}$) of the servers, which can be characterized through power profiling ($\boldsymbol{G}$). The dissipated heat from one server is recirculated to the input of other servers in the data center room. A cooling unit supplies cold air to the servers to maintain the inlet temperatures below redline. The heat dissipated by the servers are recaptured using cold plates and is used to power cooling units using heat activated cooling [5]. The efficiency of heat recaptured is dependent on the temperature of the servers, which can be characterized by thermodynamic laws ($\boldsymbol{K}$). The temperature however, varies with changing workload. Hence a heat recapture unit may not provide a steady source of power. The heat activated cooler thus has to be supplemented with power grid and other green sources such as sunlight. In this regard, a major challenge is to schedule workload being aware of the thermal and power availability characteristics of the data center to achieve low cost operation while meeting SLAs [25]–[27]. ◇

It is to be noted that for a CPS design there are other important issues such as reliability, data management, and real time operation. However, in the context of this paper we assume that these properties are subsumed by the overarching S3 issues. For example, if data transfer from an ECG sensor in a BAN to the base station was unreliable, detection of heart related emergencies would fail, hampering patient safety.

B. Expected Properties of S3 Solutions

As discussed earlier in Section I, 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 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 (Definition 1). Their characterization should involve unification of theories from different disciplines.

For instance, in example 2, a model predictive controller can be designed, which decides on the future infusion rate, in order to maintain unconsciousness of the patient without causing respiratory distress [13]. 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 S3 would involve synergistic employment of various approaches and techniques from different domains of science and engineering.*

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 [10]. The authors in [10] 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 illustrated in our discussion on the cyber-physically oriented solutions for S3.

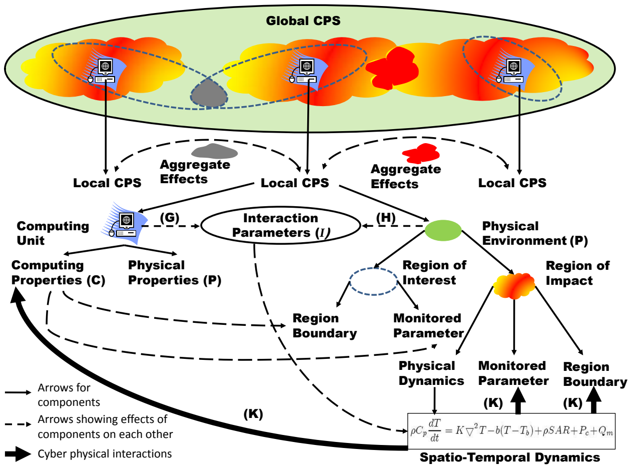


Fig. 4. **Abstract modeling framework for CPS, Global CPS (GCPS)**

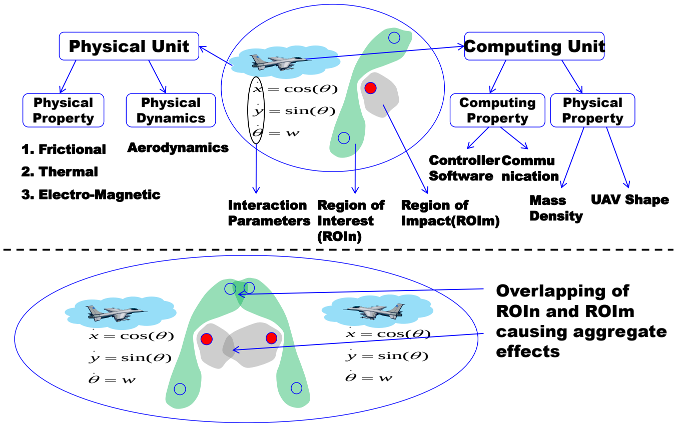


Fig. 5. **GCPS model of surveillance UAVs**

III. Cyber Physically Oriented Solutions for S3

Section I and II, hinted at the potential of using information from physical environment for S3 solutions. This section discusses some existing cyber-physically oriented S3 solutions.

A. *Ensuring Safety*

Ensuring safety of cyber-physical systems requires the characterization of the cyber-physical interactions. It involves understanding of the dynamic nature of complex physical environment such as physiology of human body. Traditionally such characterization is done through experimentation. For example, to characterize thermal interaction in a pulse-oximeter, experimentation on real deployments of the device on redundant tissues of volunteers were performed [11]. Such experimentation can cause burn risks to the human body as documented. Further, due to limited set of volunteers, experiments cannot capture an exhaustive list of test cases and are hence incomplete. In case of CPSes like data centers thermal safety of the servers are ensured by setting cooling unit supply temperature at the minimum required level [28], which is estimated by performing experimental trials before deployment. However, such estimations can be performed before the data center installation. Reiterating those experiments would require data center shutdown. In summary, experimental measures to characterize cyber-physical interactions are problematic due to: a) risk of physical harm to the environment, b) limited number of test cases prevents a comprehensive characterization, c) changes in the infrastructure requires reiteration of the experiments, which is often expensive or infeasible, and d) no theoretical guarantee on the system safety can be provided due to lack of comprehensive analysis.

In this regard, a widely used solution technique is model based engineering (MBE): a method of developing behavioral models of real systems and analyzing the models for requirement verification. There are two main phases in MBE: 1) *model development*, and 2) *model analysis* [29]. In the model development phase, a set of *expected properties* of the CPS is determined that are required for its safety. An abstract modeling of the different components of the CPS is then performed to extract properties of the physical environment, computing units, and the cyber-physical interactions. Mathematical analysis (*model analysis*) is then performed on the abstract model to *evaluate* the expected properties and *verify* the system requirements.

However, any model based technique for ensuring safety of cyber-physical systems will need to characterize the spatio-temporal cyber-physical interactions (Section II). In this regard, GCPS [29], is an abstract modeling framework for CPSes which is illustrated in Figure 4. The CPS is considered as a network of several local CPSes (LCPS). Each LCPS consists of computing unit, interaction parameters, and two associated spatial regions of the physical environment: a) *region of impact* (ROIm) and b) *region of interest* (ROIn). Associated with each computing unit are computing properties (***C***), such as frequency of operation, and physical properties of the computing unit (***P***) such as, specific heat, temperature rise. The interaction parameters are common to the computing and the physical unit and includes parameters such as heat transferred, air flow rate, and, infusion rate. The ROIn and ROIm characterizes the spatial extent of the effects of the intended and unintended interactions, respectively. The ROIn or ROIm of an LCPS has three components:

- *monitored parameter*, which is a property of the physical environment (***P***) and manifests the effects of the cyber-physical interactions. Typical examples include temperature, drug concentration, and cell death rate.
- *region boundary*, which signifies the spatial extent of the effect of interactions. The variation of the monitored parameters beyond this region is negligible.
- *physical dynamics*, a model of the physical process governing the spatio-temporal variation of the monitored parameters. For example, it can be a multi-dimensional partial differential equation governing the temperature rise on human body (*e.g.*, Penne's equation [16] in Figure 4).

Dashed single headed arrows in Figure 4, indicate the effects of the computing and physical properties on the ROIm and ROIn, given by the mappings ***G*** and ***H***. Thick solid arrows indicate the cyber-physical interactions, mathematically formulated as the mapping ***K***. Physical dynamics of the ROIm is a member of ***K***, which correlates the computing, physical and interaction parameters through complex spatio-temporal differential equations. The double headed arrows show aggregate effects when ROIns or ROIms overlap.

The use of GCPS is shown in the following UAV example:

Example 5: UAV surveillance: The UAV is given a set of target positions (unshaded bubbles in Figure 5). It has to visit these positions to carry out mission-critical operations such as imaging and wild fire suppression. The physical environment of the UAV further includes unsafe regions *e.g.,* hit range of Surface to Air Missiles (SAMs) (shaded bubbles in Figure 5). The computing properties (***C***) of the UAV include the UAV control algorithm and communication protocol between the UAV and base. The physical properties (***P***) include air frictional, thermal and electromagnetic properties of the environment. The position and velocity of the UAV are the interaction parameters (***I***), which are affected by the control algorithms and frictional properties through the aerodynamic equations (***K***). The ROIn in the GCPS is the spatial region covering the target positions. The range of the SAMs can be considered as the ROIm. Aggregate effects in case of multiple UAVs will have overlap in their ROIns, which may cause collision among UAVs [30]. The aim of an UAV path planning algorithm is to cover all possible target positions without getting in the hit range of any SAM missile [6]. ◇

GCPS models have been also proposed for mobile CPS such as automobiles [31] with simple extensions to the ROIm and ROIn to consider mobility. The GCPS model can be applied to any CPS and clearly incorporates the unified approach to CPS design by provisioning the constructs to model both the computing as well as the physical environment in the same framework. These models can be used for two purposes: a) to check the consistency of CPS models developed using specialized tools such as Ptolemy (http://ptolemy.eecs.berkeley.edu/) in specific domains and b) to perform simulation analysis of any CPS. Since GCPS is generic and provides a comprehensive set of modeling constructs it is a good candidate for the base architecture. Further, specific modeling needs may give rise to specialized modeling tools, since systems from various domains are CPSes. An important research problem in this regard is the ability to check the consistency and to capture cyber-physical inter-dependencies of the models developed in different domains. In a recent research [32], typed graphs are used to show isomorphism between different models of a CPS. In such a technique, the equivalence of models to a base architecture is considered as a consistency check. Potentially the GCPS is a good candidate for the base architecture. Apart from GCPS approach existing formal models are also considered in the literature for safety analysis of automobile software [33].

Traditionally there are two methods to analyze a CPS model: a) simulative analysis on a given set of test cases and b) model checking, where the formal methods are used to provide theoretical guarantees on properties of CPSes. In this paper, safety aspects of two example CPSes, BAN and data centers are considered to illustrate these two approaches.

B. Ensuring Security

In designing security solutions for CPS, one should not only consider the properties (***C***) of the computing components involved (CPU, RAM, ROM, data rate), but also the interaction of the components with the physical environment (mapping ***K***). In this regard, a novel perspective on securing CPS which takes this property into account, called Cyber Physical Security (CYPSec) was proposed in [22]. CYPSec solutions are environmentally-coupled security solutions, which take traditional security primitives along with the environmental knowledge/information to operate [22]. The idea is to use the monitoring capability of CPSes to provide security. By utilizing this fundamental capability of CPSes, security provision becomes intrinsically linked to a CPS operation and not something that is retrospectively added to an operational system to protect it from threats. Another merit of CYPSec solutions is 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:

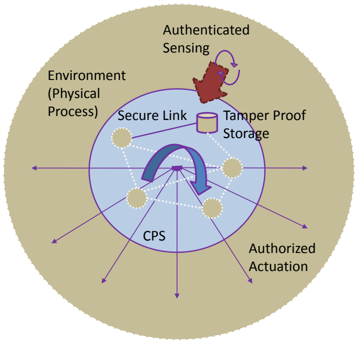


Fig. 6. **CPS Security Requirements.**

- *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, availability but also demonstrate additional "allied" properties, such as authentication, interoperability and adaptivity.
- *Multi-domain Primitives*: 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.

Figure 6 shows the security requirements for a typical CPS. It consists of five aspects: *sensing security* deals with the validity and accuracy of the sensing process; *storage security* is required to prevent both cyber and physical tampering of any data stored by the CPS; *communication security* is required for securing both inter and intra-CPS communication from both active (interferers) and passive (eavesdroppers) adversaries; *actuation control security* refers to ensuring that no actuation can take place without the appropriate authorization; and finally, *feedback security* requires ensuring that the control systems in a CPS which provide the necessary feedback for effecting actuation are protected.

C. Ensuring Sustainability

Resources from the physical environment are used to extract green energy, which is used as energy source in sustainable CPSes as discussed in Section II-A3. However, associated with this mode of power supply are the problems of intermittent

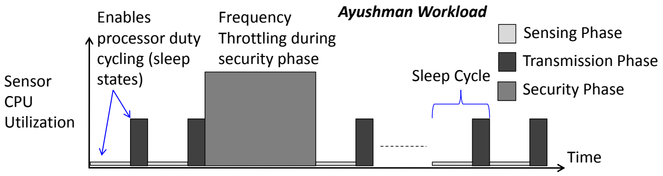


Fig. 7. **Ayushman workload showing duty cycling opportunities and variation in processing requirements. Higher bars indicate higher processor utilization as well as higher power consumption.**

energy source and unknown load characteristics. Moreover, the amount of energy available from the environment is often not sufficient to operate the computing units of CPSes. For example, recent studies [34], [35] show that the amount of power scavenged from human body through body heat, ambulation, and respiration is not sufficient to operate state of the art sensors at their maximum operating power. To overcome these problems sustainability research has focused on three key techniques: a) improving the efficiency of energy harvesting from the environment, b) environment aware duty cycling of computing units, and c) energy efficient computing.

Given these techniques, the goal of a sustainable design is to ensure that the CPS is *energy neutral* [9]. Energy neutrality of a system essentially means that the system consumes as much energy as harvested. Consider the SBCS power supply model of Figure 2 where at time $t = 0$ the battery capacity was $B(0)$. For an energy neutral operation of the system for δt onwards, the battery capacity at time $t + \delta t$ is also $B(0)$. In other words, the battery is never depleted for energy neutral operation of a system. The harvesting theory [9] is an analytical method for ensuring energy neutrality of a CPS design. It takes a model based approach, and considers stochastic models of the harvesting source and the computing unit. Based on the characterization of intermittent energy availability from scavenging sources, environmentally aware duty cycling of computing units are proposed in several domains such as in BANs [29] and data centers [24]. An analysis of BAN duty cycling for sustainability is discussed in the following example.

Example 6: BAN duty cycling: The computational workload ($\boldsymbol{C}$) in BANs are generally *periodic* and are known *a priori*. For example, health monitoring applications such as Ayushman [1] have deterministic workloads as shown in Figure 7. In Ayushman, the sensors in the BAN sense physiological data, store them in local memory, and periodically transfer the stored data to the base station in a single burst. Communication is secured by encryption with a secret key, which is established between BAN nodes using the PSKA protocol (Example 3).

Energy is scavenged from respiration, ambulation, body heat and sunlight and the available energy ($\boldsymbol{I}$) depends on the physical properties ($\boldsymbol{P}$) such as physical exertion, intensity of sunlight. The scavenging sources can be profiled ($\boldsymbol{H}$) for obtaining average energy availability over a day of operation [34]. Given the available average power, the sensors can be duty cycled to reduce the energy consumption to a level that is sustainable. The duty cycling algorithms are driven by the available energy as input and hence serve as the mapping $\boldsymbol{K}$. Further, allowable duty cycles of the sensors depends on the time taken for processing security related workload. Thus, the duty cycling algorithm should also be aware of the processing requirements of the security protocol, necessitating a unified approach to design. ◇

IV. Application of S3 Solutions

This section demonstrates the application of cyber-physically oriented solutions for S3 in three representative CPSes: BANs, DCs, and SIs.

A. BAN Safety Modeling

State of the Art: As discussed in Section III-A, Model based engineering (MBE) has been used extensively to characterize the cyber-physical interactions to verify interaction safety of medical devices, an important component of BANs. Most of these works try to characterize the computational aspects of the medical device or make simplifications to the physiology of the human body. For example, authors in [12], [20] propose the use of formal models in medical device safety review. However, none of these works consider formal representation of the interactions of the medical device with the human body. Jiang et al. [36] have considered modeling the physiology of heart using a timed automata. Timed automata is also used to verify the control actions in a closed loop infusion system with pulse oximeter signals as feedback [37].

Several modeling efforts to characterize the cooperation of computational and physical behavior of BAN components have used the linear hybrid automata [38], [39] with implicit assumptions that the human physiology is static. Such assumptions are not applicable in general for safety verification of BAN-CPS as they do not capture the dynamic spatio-temporal nature of cyber-physical interactions.

Focus — Formal Models for BAN Interaction Safety: As discussed in Section II-A1, CPS safety should concentrate on achieving interaction safety. This calls for modeling techniques that can characterize the spatio-temporal effects of cyber-physical interactions. Research efforts in this regard have resulted in modeling frameworks such as the one shown in Figure 4 [29], which can be used for CPS oriented modeling of BANs. Interaction safety with respect to thermal effects of the computation in the sensors are considered and GCPS is used to model such scenarios. Given the GCPS 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 GCPS as the modeling tool and a generic simulation analysis algorithm [29] to evaluate safety of BANs. The GCPS modeling constructs are further implemented as an annex (CPSAnnex) [40] to industry standard Architecture Analysis and Design Language (http://www.aadl.info/) and can be used to specify cyber-physical interactions in CPS.

For model checking purposes, hybrid automata based formal models have been recently considered, for modeling medical devices. The following examples show the use of hybrid automata that can capture cyber-physical interactions for model checking of CPSes.

Example 7: Hybrid model of thermal effects in sensors: Spatio-Temporal Hybrid Automata (STHA) [41] can capture the spatio-temporal cyber-physical interactions. Figure 8 shows the variation of skin temperature over space for the operation of two sensors on the human body. The thermal effects of the sensors are similar to the pulse oximeter example (Example 1). A formal model generally represent a system as

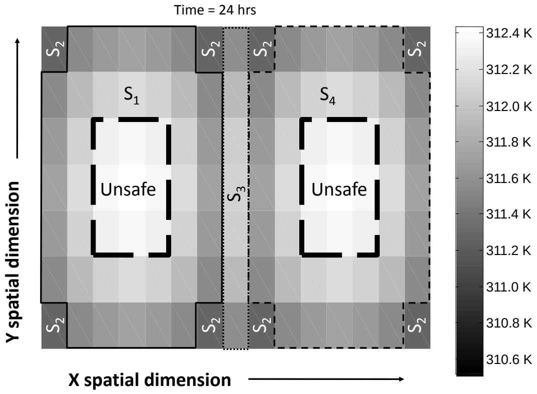


Fig. 8. **Spatial region partitioned into states (S_1, S_2, S_3, and S_4) to conceptualize a spatio-temporal hybrid automata.**

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 8, 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. ◇

Example 8: Model checking of STHA: 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 [42]. 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 [42] 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 [42]. This can be done by setting an initial state, incrementing time and checking the reachable states as the continuous dynamics evolves. ◇

B. Secure Information Access in Smart Infrastructures (SI)

State of the Art: Recent years have seen the development of Smart Infrastructures CPS (SI-CPS) which consist of a large number of heterogeneous, massively distributed computing entities. Such infrastructures provide their users with an aware, intelligent, information rich environment for conducting their day-to-day activities [43]. Examples of SI-CPS include - health monitoring systems [44], [45], smart-spaces [46], and aware-homes [47]. An important application of their monitoring capabilities is *emergency management*. Examples of emergencies include patient needing urgent medical attention, crisis such as building fire and the computing infrastructure under attack from outside. SI-CPS can be used to detect and provide useful and real-time information about the state of such emergencies to the planners and relief-workers and facilitate response, thereby improving the chances of saving lives and property.

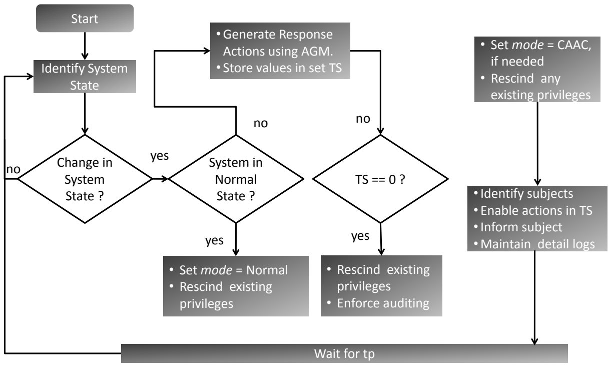


Fig. 9. **CAAC Execution Flowchart**

Traditionally in the event of emergencies, any security system are disabled in order to allow relief workers to utilize full capabilities of the system for controlling the emergency [48], [49]. Such an approach may work for non-smart systems and infrastructures. But given the extent of sensitive information available within smart-infrastructures, disabling security in the event of emergencies, will potentially leave the system vulnerable to hackers and tech-criminals. For example, let us consider that when a person faces a health related emergency, the security on his wearable health monitoring system is disabled so that any medical personnel can easily view the subject's health information without any security constraints. This allows any malicious entity in the vicinity, with the right set of tools, to access the person's health information as well. The malicious element may then dupe the smart-infrastructure into detecting a false emergency, disable the security system and collect sensitive information from the space.

Focus — Criticality-Aware Access Control: For securing access to information in an SI, novel access control models called Criticality Aware Access Control (CAAC) [50] has been developed. CAAC has the ability to provide the right set of privileges for the right set of subjects, at the right time for the right duration to facilitate criticality response. *Criticalities* are situations that require urgent response actions in order to maintain the stability of the system. Each criticality has a timing duration associated with it known as *window-of-opportunity*, within which response actions have to be executed for the criticality to be controlled [51].

CAAC is an adaptive access control approach designed to facilitate the control of all the active criticalities within the system. It uses an Action General Model (AGM) based on the stochastic crisis planning technique developed in [52]. The results of AGM execution (list of response actions for different combinations of criticalities such that the window-of-opportunity of all the criticalities is satisfied) are provided to the CAAC, before it is deployed. CAAC monitors its environment at regular intervals (every *tp* time units), and depending upon the system state, it identifies the best response actions that need to be taken to reach the normal state. Additionally it identifies the set of subjects that are best suited to execute the response actions, and provides them with credentials to execute the actions. This change in credentials of subjects is temporary and reverts back when the criticalities in the system change or expire. Figure 9 shows the CAAC operation flow chart. Being a CYPSec solution it inherently brings out new "allied" properties to security policy specification:

- *Proactivity*: CAAC can provide privileges to selected users in response to emergencies without explicit request.
- *Adaptive Risk Management*: CAAC minimizes the associated risks by dynamically controlling the changes in privileges in accordance with the principle of least privilege.

C. Data Center Energy Efficiency

State of Art: Sustainability research in data centers have mainly focused on energy efficiency. Recent research proposes energy efficiency improvements of data centers through throttling devices and workload shaping, which are usually with performance degrading implications. In this regard, some prominent approaches are: (i) system level power management techniques including inactive low power modes *i.e.*, transitioning to the sleep sate in idle times [53], [54], and active low power modes *i.e.*, frequency scaling of CPU according to the offered workload [55]–[57], (ii) server provisioning, adjusting the number of active servers in a servers depending upon load requirements [25], [58]–[62], (iii) thermal aware spatio-temporal job scheduling at both the chip-level and the data center-level [61], [63]–[66] and (iv) electricity cost efficient workload distribution across data centers [67]–[69]. Recent research also propose storing energy in Uninterruptible Power Supply (UPS) batteries during valleys - periods of lower demand — which can be drained during peaks periods of higher demand [26], [27].

Focus — Environmentally-Coupled Workload Scheduling and Green Cooling Energy Supply: Thermal aware spatio-temporal workload scheduling in DCs is an emerging area of research. Several online and offline algorithms for spatio-temporal workload scheduling [28] have been developed and analyzed for energy efficiency. Cooling unit control has been also incorporated into spatial scheduling algorithms such as HTS [70], which dynamically sets the cooling unit thermostat to reduce cooling power.

For Internet DCs [25] thermal aware active server set provisioning (TASP) and Thermal Aware Workload Distribution (TAWD) are designed to predict workload at fine time slots and skew it toward thermal and power efficient servers, thus increasing energy efficiency of systems by increasing the per-server utilization. TASP and TAWD policies are further evaluated under *energy proportionality* of servers in data centers [14]. These solutions clearly draw upon both computer science and thermodynamics. Further, methods for cost efficiency in data center operation has been developed considering the variation in electricity costs over different locations in the world [71]. A generic theoretical formulation of environmentally aware workload scheduling for CPSes is proposed in [72]. This framework considers the spatio-temporal variation of the properties of environment and judiciously employs discretization to points of interest for their characterization. Such a formal framework allows formulation of workload scheduling in any CPS domain into an optimization problem.

In [24], environmentally-coupled solutions are classified into several classes based on three objectives: (i) workload management, which determines the amount of workload in each computing unit, (ii) computing power management, which determines the power modes of the computing components, and (iii) management of the physical environment, which includes policies for reduction in heat recirculation or intelligent cooling unit control. The study provides characteristics of CPS workloads and categorizes the workload management algorithms with respect to three salient features: a) workload duration, long running or short running, b) workload arrival characteristics, periodic or aperiodic, and c) workload knowledge, offline (prior knowledge) or online (no prior knowledge). With respect to each of these five objectives, *i.e.*, three workload properties, power and physical environment management, the algorithms are given a ☆, if they support all the options in the objective. An important conclusion was that existing environmentally-coupled solutions can achieve four ☆ operation, where they may support all three characteristics of the workload and provision power management. However, controlling the physical environment often requires prior knowledge of the workload, which may compromise the capability of the algorithm to process aperiodic arrivals and perform online scheduling.

Recent works on green cooling equipment design (Example 4) have resulted in a theoretical model of a heat activated chiller. Preliminary theoretical analysis shows that a Power Usage Efficiency (PUE)[4] of very close to one is possible with such an approach. Further, for facilitating the design and testing of green strategies in data center, an intuitive open source simulation tool such as *GDCSim* [74] is also developed. Such research towards a sustainable data center design is work in progress under BlueTool NSF infrastructure grant (http://impact.asu.edu/BlueTool/wiki/index.php/BlueTool).

V. Some Open Research Challenges in S3

A. Safety

Physical processes in the ROIm can affect the monitored parameters in the ROIn. Consider the example where an implanted sensor that measures physiological values from the human body and transfers it to the base station. Let the ROIn be defined as the communication range of the sensor and the ROIm be defined as the area of the surrounding tissue that receives thermal energy from the sensor due to its heat dissipation. Implantation often leads to growth of tissue around the computing unit resulting in a change in the ROIm of the system [75]. However, this phenomenon leads to a change in the electromagnetic environment of the sensor thus altering its communication capabilities or affecting the ROIn. Analysis of such scenarios are difficult due to lack of models.

In the STHA reachability analysis, due to discretization of the dimensions, errors will be introduced. In this regard, an important research objective is to ensure that *the approximations caused due to the discretization is an over approximation.* In the analysis step there are two types of approximations during

[4] PUE is the ratio of power in to the data center measured at the utility meter to the conditioned power out to run the IT equipment for computing [73].

discretization of: 1) dimensions and 2) differential equations. Characterization of such two pronged errors in the reachability analysis is an open problem.

B. Security

In the long run several additional research challenges need to be considered in order to successfully deploy CYPSec solutions. First, CPSes can be *mixed-criticality systems* with both critical (those that perform critical computations or those that interact with the physical environment) and non-critical components. Interaction between these two components has to be carefully considered in order to ensure the safe operation of the system. One approach for handling the mixed critical nature is to formally verify the behavior of CYPSec solutions under different operational conditions of the system.

The close coupling of CYPSec solutions with the environment also brings to fore an important characteristic that traditional security approaches do not seem to consider - the notion of time. Traditional computing usually ignores the notion of time by abstracting the physical process [76]. Such abstractions are not applicable for CPS. As the operation of the CPS has direct consequence on a physical environment, safety of the process and its users is paramount. Indeed in many of the current CPS systems such as medical devices and smart grid safety has been given much more prominence than security, and rightly so, as a secure device that is unsafe has no utility. Safety may be compromised since security components of the CPS may interact in an unexpected manner with others.

Finally, as CYPSec solutions depend upon the physical environment to enable security, attacks on the physical environment can be potentially used to prevent the CYPSec solutions from functioning correctly. Attackers can artificially change the environment around the cyber elements of a CPS causing unexpected results with CYPSec including denial of service. Physical environment can be tampered with in CPSes such as power-grids and UAVs, since they are unmanned. Attackers can potentially control the sensors in a data center to cause overload of the air conditioner. Therefore, if the physical environment itself is not secure, some mechanism for authenticating the sensed value is required.

C. Sustainability

One of the major open problems in sustainability solutions is the efficiency of energy extraction from scavenging sources. The theoretical limit of efficiency of a solar electricity device is 70% and costs around \$0.30 per KWhr [77], an order of magnitude greater than current electricity costs. Further, the scavenged energy per unit area of a source that extracts electrical power from the human body through body heat, respiration or ambulation are very low [34]. This causes increase in the form factor of the scavenger. The development of cost effective and usable energy scavenging sources for CPSes is an open problem.

For effective environmentally-coupled duty cycling, scavenging sources have to be modeled to determine the power availability characteristics. However, often it is extremely hard to predict the amount of power available at a given time. For example, in case of a solar electricity device the available power depends on several environmental factors such as presence or absence of clouds and random obstructions providing shade. Characterization of the physical processes in the environment that affect scavenging to predict the available power at a future time is an open research problem.

Development of Five ☆ algorithms [24] for environmentally-coupled CPS workload is an important open problem. Being able to control the physical environment requires accurate characterization of the cyber-physical interactions during the workload scheduling duration. Aperiodic arrival of workloads introduces uncertainties in such characterizations. Prediction algorithms for CPS workloads exist in different domains such as for Internet data center. They can be used to predict the behavior of the physical environment. However, development of such prediction algorithms are still open research problems in application domains such as high performance computing [28] and context aware applications [78].

VI. Conclusions

CPSes are increasingly becoming pervasive and are enabling critical operations in systems providing improved health care, smart-spaces, green and cost effective amenities. To enable wide acceptance of CPSes, their safe, secure and sustainable operation has to be ensured. The tight coupling between computing units and physical environment in CPS when used intelligently can assure safe, secure and sustainable systems. This paper facilitates the design of environmentally aware solutions to CPS S3 problems by providing a formal framework for representing cyber-physical interactions in a CPS. Several examples from diverse CPS domains such as BAN, DCs, SIs and UAVs are shown to demonstrate the effectiveness of the framework in characterizing intended, unintended interactions and aggregate effects. In addition, this paper also provides a list of open research challenges for S3 in CPS. A detailed discussion of safety, security, and sustainability in the specific domains of BANs will be published in the form of a book [79].

Acknowledgments

This research was funded in part by NSF grants CNS #0831544, #0834797, and #0855277. Thanks to R. Jetley, S. Weininger, Y. Zhang and P. Jones, OSEL FDA for insights on safety and security issues for medical devices, and to Raytheon, Northrop Grumman, Intel, and SFAz, for funding.

References

[1] K. Venkatasubramanian, G. Deng, T. Mukherjee, J. Quintero, V. Annamalai, and S. K. S. Gupta, "Ayushman: A Wireless Sensor Network Based Health Monitoring Infrastructure and Testbed," in *Distributed Computing in Sensor Systems*, July 2005, pp. 406–407.

[2] I. Korhonen, J. Parkka, and M. Van Gils, "Health monitoring in the home of the future," *Engineering in Medicine and Biology Magazine, IEEE*, vol. 22, no. 3, pp. 66–73, May-June 2003.

[3] R. Paradiso, G. Loriga, and N. Taccini, "A wearable health care system based on knitted integrated sensors," *Information Technology in Biomedicine, IEEE Transactions on*, pp. 337–344, Sept. 2005.

[4] V. Hartkopf, V. Loftness, A. Mahdavi, S. Lee, and J. Shankavaram, "An integrated approach to design and engineering of intelligent buildings–the intelligent workplace at Carnegie Mellon University," *Automation in Construction*, vol. 6, no. 5-6, pp. 401 – 415, 1997. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0926580597000198

[5] A. Haywood, J. Sherbeck, P. Phelan, G. Varsamopoulos, and S. Gupta, "A sustainable data center with heat-activated cooling," in *Thermal and Thermomechanical Phenomena in Electronic Systems (ITherm), 2010 12th IEEE Intersociety Conference on*, june 2010, pp. 1 –7.

[6] T. Mukherjee and S. K. S. Gupta, "MCMA+CRET: A mixed criticality management architecture for maximizing mission efficacy and tool for expediting certification of uavs," in *IEEE Workshop on Mixed Criticality: Roadmap to Evolving UAV Certification, CPSWeek'09*.

[7] Q. Tang, N. Tummala, S. Gupta, and L. Schwiebert, "Communication scheduling to minimize thermal effects of implanted biosensor networks in homogeneous tissue," *Biomedical Engineering, IEEE Transactions on*, vol. 52, no. 7, pp. 1285–1294, July 2005.

[8] K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "PSKA: Usable and secure key agreement scheme for body area networks," *IEEE Transactions on Information Technology in Biomedicine SI Wireless Health*, vol. 14, no. 1, pp. 60–68, Jan 2010.

[9] A. Kansal, J. Hsu, M. Srivastava, and V. Raghunathan, "Harvesting aware power management for sensor networks," in *Design Automation Conference, 2006 43rd ACM/IEEE*, 2006, pp. 651 –656.

[10] J. C. Willems, "The behavioral approach to open and interconnected systems," *Control Systems Magazine*, pp. 46–99, 2007.

[11] D. G. M. Greenhalgh et al, "Temperature threshold for burn injury: An oximeter safety study," *Journal of Burn Care and Rehabilitation*, vol. 25, no. 5, pp. 411–415, 2004.

[12] R. Jetley, S. P. Iyer, and P. L. Jones, "A formal methods approach to medical device review," *Computer*, vol. 39, no. 4, pp. 61–67, 2006.

[13] J. Jacobs, "Algorithm for optimal linear model-based control with application to pharmacokinetic model-driven drug delivery," *Biomedical Engineering, IEEE Transactions on*, vol. 37, no. 1, pp. 107 –109, 1990.

[14] G. Varsamopoulos, Z. Abbasi, and S. K. S. Gupta, "Trends and effects of energy proportionality on server provisioning in data centers," in *International Conference on High performance Computing Conference (HiPC2010)*, Dec. 2010.

[15] C. Green, Z. Ounaies, and E. Hughesa, "Harvesting energy using a thin unimorph prestressed bender: Geometrical effects," *Journal of Intelligent Material Systems and Structures*, 2005.

[16] H. H. Pennes, "Analysis of tissue and arterial blood temperature in the resting human forearm," in *Journal of Applied Physiology*, vol. 1.1, 1948, pp. 93–122.

[17] D. Wada and D. Ward, "The hybrid model: a new pharmacokinetic model for computer-controlled infusion pumps," *Biomedical Engineering, IEEE Transactions on*, vol. 41, no. 2, pp. 134 –142, Feb. 1994.

[18] R. N. Maini, F. C. Breedveld, J. R. Kalden, J. S. Smolen, D. Davis, J. D. MacFarlane, C. Antoni, B. Leeb, M. J. Elliott, J. N. Woody, T. F. Schaible, and M. Feldmann, "Therapeutic efficacy of multiple intravenous infusions of anti-tumor necrosis factor a monoclonal antibody combined with low-dose weekly methotrexate in rheumatoid arthritis," *Arthritis and Rheumatism*, vol. 41, no. 9, pp. 1552 – 1563, 1998.

[19] "ISO 60601 safety standard," http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm\?csnumber=45605.

[20] D. E. Arney, R. Jetley, P. Jones, I. Lee, A. Ray, O. Sokolsky, and Y. Zhang, "Generic infusion pump hazard analysis and safety requirements version 1.0," 2009. [Online]. Available: http://repository.upenn.edu/cis_reports/893

[21] FDA urged to rethink approval of medical devices, http://www.latimes.com/health/la-na-medical-devices-approval-20110730,0,6697377.story.

[22] K. Venkatasubramanian, S. Nabar, S. K. S. Gupta, and R. Poovendran, *Cyber Physical Security Solutions for Pervasive Health Monitoring Systems*, ser. In E-Healthcare Systems And Wireless Communications: Current And Future Challenges, M. Watfa, Ed. IGI Global, 2011.

[23] D. Halperin, T. Heydt-Benjamin, K. Fu, T. Kohno, and W. Maisel, "Security and Privacy for Implantable Medical Devices," *IEEE Pervasive Computing*, vol. 7, no. 1, 2008.

[24] S. K. S. Gupta, T. Mukherjee, G. Varsamopoulos, and A. Banerjee, "Research directions in energy-sustainable cyber-physical systems," *Elsevier Comnets Special Issue in Sustainable Computing (SUSCOM) Invited paper*, vol. 1, pp. 57–74, 2011.

[25] Z. Abbasi, G. Varsamopoulos, and S. K. S. Gupta., "Thermal aware server provisioning and workload distribution for internet data centers," in *ACM International Symposium on High Performance Distributed Computing (HPDC10)*, Jun. 2010, pp. 130 – 141.

[26] S. Govindan, A. Sivasubramaniam, and B. Urgaonkar, "Benefits and limitations of tapping into stored energy for datacenters," in *Proc. The 38th International Symposium on Computer Architecture (ISCA)*, San Jose, CA, USA, June 2011.

[27] R. Urgaonkar, B. Urgaonkar, M. Neely, and A. Sivasubramaniam, "Optimal power cost management using stored energy in data centers," *Arxiv preprint arXiv:1103.3099*, 2011.

[28] T. Mukherjee, A. Banerjee, G. Varsamopoulos, S. K. S. Gupta, and S. Rungta, "Spatio-temporal thermal-aware job scheduling to minimize energy consumption in virtualized heterogeneous data centers?" *Computer Networks*, June 2009. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2009.06.008

[29] A. Banerjee, S. Kandula, T. Mukherjee, and S. Gupta, "BAND-AiDe: A tool for cyber-physical oriented analysis and design of body area networks and devices," *ACM Transactions on Embedded Computing Systems (TECS), Special issue on Wireless Health Systems 2009 (Accepted for publication)*, 2010.

[30] S.K.S. Gupta, "Model-based engineering of UAVs to ensure safety of critical missions," presented at the S5 conference Beavercreek, Ohio https://www.signup4.net/public/ap.aspx?EID=SAFE23E&OID=110.

[31] S. Kandula, T. Mukherjee, and S. Gupta, "Toward autonomous vehicle safety verification from mobile cyber-physical systems perspective," in *ACM/IEEE Second International Conference on Cyber-Physical Systems (ICCPS), Work-in-Progress (WiP) session*, April 2011.

[32] A. Bhave, B. Krogh, D. Garlan, and B. Schmerl, "View consistency in architectures for cyber-physical systems," in *Proc. of the 2nd ACM/IEEE Intl. Conference on Cyber-Physical Systems*, April 2011.

[33] Carnegie Mellon Methods Keep Bugs Out Of Software For Self-Driving Cars, http://www.cmu.edu/news/archive/2011/June/june21_selfdrivingcars.shtml.

[34] J. A. Paradiso and T. Starner, "Energy scavenging for mobile and wireless electronics," *Pervasive Computing, IEEE*, vol. 4, no. 1, pp. 18–27, Jan.-March 2005.

[35] G. Park, T. Rosing, M. D. Todd, C. R. Farrar, and W. Hodgkiss, "Energy harvesting for structural health monitoring sensor networks," *Journal of Infrastructure Systems*, pp. 64–79, 2008. [Online]. Available: http://link.aip.org/link/?QIS/14/64/1

[36] Z. Jiang, M. Pajic, A. Connolly, S. Dixit, and R. Mangharam, "Real-time heart model for implantable cardiac device validation and verification," *Real-Time Systems, Euromicro Conference on*, vol. 0, pp. 239–248, 2010.

[37] D. Arney, M. Pajic, J. M. Goldman, I. Lee, R. Mangharam, and O. Sokolsky, "Toward patient safety in closed-loop medical device systems," in *ICCPS '10: Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*. New York, NY, USA: ACM, 2010, pp. 139–148.

[38] T. A. Henzinger, "The theory of hybrid automata." IEEE Computer Society Press, 1996, pp. 278–292.

[39] G. Lafferriere, G. J. Pappas, and S. Yovine, "Reachability computation for linear hybrid systems," in *In Proceedings of the 14th IFAC World Congress, volume E*. Elsevier Science Ltd, 1998, pp. 7–12.

[40] IMPACT Lab, "CPSAnnex," https://wiki.sei.cmu.edu/aadl/images/0/00/CyberPhysicalSystemsTribidMay2010.pdf.

[41] A. Banerjee, T. Mukherjee, and S. K. S. Gupta, "STHA: Spatio-temporal hybrid automata for safe and sustainable cyber-physical systems," in *under preparation*, 2011.

[42] G. Frehse, "Phaver: Algorithmic verification of hybrid systems past hytech," in *HSCC*, 2005, pp. 258–273.

[43] F. Adelstein, S. K. S. Gupta, G. Richard, and L. Schwiebert, *Fundamentals of Mobile and Pervasive Computing*. McGraw Hill, 2005.

[44] Victor Shnayder and Bor-rong Chen and Konrad Lorincz and Thaddeus R. F. Fulford-Jones, and Matt Welsh, "Sensor Networks for Medical Care," April 2005, Harvard University Technical Report.

[45] K. Venkatasubramanian, G. Deng, T. Mukherjee, J. Quintero, V. Annamalai, and S. K. S. Gupta, "Ayushman: A Wireless Sensor Network Based Health Monitoring Infrastructure and Testbed," June/July 2005, pp. 406–407, In Proc. of the IEEE International Conference on Distributed Computing in Sensor Systems.

[46] M. Román, C. Hess, R. Cerqueira, A. Ranganathan, R. H. Campbell, and K. Nahrstedt, "A middleware infrastructure for active spaces," *IEEE Pervasive Computing*, vol. 1, no. 4, pp. 74–83, 2002.

[47] S. Helal, W. Mann, H. El-Zabadani, J. King, Y. Kaddoura, and E. Jansen, "The Gator Tech Smart House: A Programmable Pervasive Space," *Computer*, vol. 38, no. 3, pp. 50–60, March 2005.

[48] S. Mehrotra, C. Butts, D. Kalashnikov, N. Venkatasubramanian, R. Rao, G. Chockalingam, R. Eguchi, B. Adams, and C. Huyck, "Project RESCUE: Challenges in Responding to the Unexpected," in *Proceedings of the Sixteenth Annual Symposium on Electronic Imaging Science and Technology*. SPIE, January 2004, pp. 179–192.

[49] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder: new directions for implantable medical device security," in *HOTSEC'08: Proceedings of the 3rd conference on Hot topics in security*. Berkeley, CA, USA: USENIX Association, 2008, pp. 1–7.

[50] K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "CAAC - an adaptive and proactive access control approach for emergencies for smart infrastructures," *ACM Transactions on Autonomous and Adaptive Systems Special Issue on Adaptive Security*, 2011.

[51] S. K. S. Gupta, T. Mukherjee, and K. Venkatasubramanian, "Criticality Aware Access Control Model for Pervasive Applications," March 2006, In Proc. of 4th IEEE Conf. on Pervasive Computing (PerCom).

[52] T. Mukherjee, K. Venkatasubramanian, and S. K. S. Gupta, "Performance Modeling of Critical Event Management for Ubiquitous Computing Applications," in *Proceedings of the International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. ACM/IEEE, October 2006, pp. 12–19.

[53] D. Meisner, B. Gold, and T. Wenisch, "PowerNap: eliminating server idle power," *ACM SIGPLAN Notices*, vol. 44, no. 3, pp. 205–216, 2009.

[54] D. Meisner, C. Sadler, L. Barroso, W. Weber, and T. Wenisch, "Power management of online data-intensive services," in *Proc. The 38th International Symposium on Computer Architecture (ISCA)*, June 2011.

[55] S. Nedevschi, L. Popa, G. Iannaccone, and S. R. andDavid Wetherall, "Reducing network energy consumption via sleeping and rate-adaptation," in *USENIX Symposium on Networked Systems Design and Implementation, NSDI08*, April 2008, pp. 323–336.

[56] P. Ranganathan, P. Leech, D. Irwin, and J. Chase, "Ensemble-level power management for dense blade servers," in *ISCA '06: Proceedings of the 33rd annual international symposium on Computer Architecture*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 66–77.

[57] M. Elnozahy, M. Kistler, and R. Rajamony, "Energy conservation policies for web servers," in *USITS'03: Proceedings of the 4th conference on USENIX Symposium on Internet Technologies and Systems*. Berkeley, CA, USA: USENIX Association, 2003, pp. 8–8.

[58] B. Guenter, N. Jain, and C. Williams, "Managing cost, performance, and reliability tradeoffs for energy-aware server provisioning," in *Proc. IEEE INFOCOM, Shanghai, China*. IEEE, 2011, pp. 702–710.

[59] J. Chase, D. Anderson, P. Thakar, A. Vahdat, and R. Doyle, "Managing energy and server resources in hosting centers," in *SOSP '01: Proceedings of the eighteenth ACM symposium on Operating systems principles*. New York, NY, USA: ACM, 2001, pp. 103–116.

[60] A. Krioukov, P. Mohan, S. Alspaugh, L. Keys, D. Culler, and R. Katz, "Napsac: design and implementation of a power-proportional web cluster," in *Proceedings of the first ACM SIGCOMM workshop on Green networking*. ACM, 2010, pp. 15–22.

[61] A. Faraz and T. Vijaykumar, "Joint optimization of idle and cooling power in data centers while maintaining response time," *ACM SIGARCH Computer Architecture News*, vol. 38, no. 1, pp. 243–256, 2010.

[62] G. Chen, W. He, J. Liu, S. Nath, L. Rigas, L. Xiao, , and F. Zhao, "Energy-aware server provisioning and load dispatching for connection-intensive internet services," in *NSDI'08: Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation*. Berkeley, CA, USA: USENIX Association, 2008, pp. 337–350.

[63] J. Moore, J. Chase, P. Ranganathan, and R. Sharma, "Making scheduling "cool": temperature-aware workload placement in data centers," in *ATEC '05: Proceedings of the annual conference on USENIX Annual Technical Conference*. Berkeley, CA, USA: USENIX Association, 2005, pp. 5–5.

[64] Q. Tang, S. K. S. Gupta, and G. Varsamopoulos, "Energy-efficient thermal-aware task scheduling for homogeneous high-performance computing data centers: A cyber-physical approach," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 11, pp. 1458–1472, 2008.

[65] J. Moore, J. Chase, and P. Ranganathan, "Weatherman: Automated, online, and predictive thermal mapping and management for data centers," in *IEEE International Conference on Autonomic Computing (ICAC)*, Jun. 2006, pp. 155–164.

[66] F. Xie, M. Martonosi, and S. Malik, "Intraprogram dynamic voltage scaling: Bounding opportunities with analytic modeling," *ACM Transactions on Architecture and Code Optimization (TACO)*, vol. 1, no. 3, pp. 323–367, 2004.

[67] L. Rao, X. Liu, L. Xie, and W. Liu, "Minimizing electricity cost: optimization of distributed internet data centers in a multi-electricity-market environment," in *INFOCOM, 2010*. IEEE, pp. 1–9.

[68] K. Le, R. Bianchini, M. Martonosi, and T. D. Nguyen, "Cost and energy aware load distribution across data centers," in *SOSP Workshop on Power Aware Computing and Systems(HotPower '09)*, 2009.

[69] A. Qureshi, R. Weber, H. Balakrishnan, J. Guttag, and B. Maggs, "Cutting the electric bill for internet-scale systems," in *Proceedings of the ACM SIGCOMM 2009 conference on Data communication*. ACM, 2009, pp. 123–134.

[70] A. Banerjee, T. Mukherjee, G. Varsamopoulos, and S. Gupta, "Integrating cooling awareness with thermal aware workload placement for HPC data centers," *Sustainable Computing: Informatics and Systems*, vol. 1, no. 2, pp. 134 – 150, 2011, Special issue on selected papers from the 2010 International Green Computing Conference. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2210537911000229

[71] Z. Abbasi, T. Mukherjee, G. Varsamopoulos, and S. K. S. Gupta, "Dynamic hosting management of web based applications over clouds," in *Intl. Conf. on High performance Computing (HiPC)*, India, Dec 2011.

[72] Q. Tang, G. Varsamopoulos, and S. K. S. Gupta., "A unified methodology for scheduling in distributed cyber-physical systems," *ACM Transactions on Embedded Computing Systems*, 2010, Special issue on the Verification of Cyber-Physical Software Systems.

[73] ASHRAE, *Best practices for datacom facility energy efficiency*. ASHRAE Technical Committee 9.9, Mission Critical Facilities, Technology Spaces, and Electronic Equipment, 2009.

[74] S. Gupta, R. R. Gilbert, A. Banerjee, Z. Abbasi, T. Mukherjee, and G. Varsamopoulos, "GDCSim - an integrated tool chain for analyzing green data center physical design and resource management techniques," in *International Green Computing Conference (2011)*, Orlando, Florida.

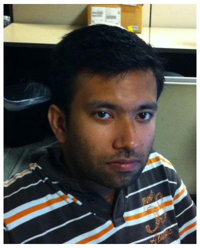
[75] D. Paul, L. Nathan, Y. Bazhang, M. Yvonne, and F. Moussy, "Study of the effects of tissue reactions on the function of implanted glucose sensors," *Journal of Biomedical Materials Research Part A*, 2007.

[76] E. A. Lee, "Computing needs time," *ommunications of the ACM*, vol. 52, no. 5, pp. 70–79, 2009.

[77] N. Lewis, "Toward cost-effective solar energy use." *Science*, vol. 315, no. 5813, pp. 798–801, 2007.

[78] F. Adelstein, S. Gupta, G. R. III, and L. Schwiebert, *Fundamentals of Mobile and Pervasive Computing*. McGraw Hill, 2004.

[79] S. Gupta, T. Mukherjee, and K. Venkatasubramanian, *Body Area Networks:Safety, Security, and Sustainability*. Cambridge University Press (In preparation).



Ayan Banerjee is a Ph.D. student at the School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ. He received his B.E. in Electronics and Telecommunication Engineering from Jadavpur University, Kolkata, India. Since Fall 2007 he has been with the IMPACT Lab at Arizona State University. His research interests include safety and sustainability of cyber-physical systems. His publications are available at http://impact.asu.edu/ayan/index.html

Krishna K. Venkatasubramanian is a post-doctoral researcher at the Computer and Information Science Department at the University of Pennsylvania, Philadelphia, PA. He received his B.S. in Computer Science from Webster University, St. Louis, MO, and M.S. and Ph.D. in Computer Science from Arizona State University, Tempe, AZ. His research focuses on secure cyber-physical systems, body area networks, trust management, and medical device security. Dr. Venkatasubramanian is a member of the ACM and the IEEE and his publication list is available at http://www.seas.upenn.edu/~vkris/.

Tridib Mukherjee is a Research Scientist at the Xerox Research Lab, Webster, NY. He received his B.E. degree in Computer Science and Engineering from Jadavpur University, Kolkata, India, and Ph.D. degree in Computer Science from Arizona State University (ASU), Tempe, AZ. His research interests include green/sustainable computing, cyber-physical systems, distributed systems, wireless embedded systems, and model-based engineering. Dr. Mukherjee is a member of the IEEE. His publication list is available at http://impact.asu.edu/ tridib/.

Sandeep Kumar S. Gupta is a Professor with the School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ and is the Chair of the Computer Engineering Graduate Program. He received the B.Tech degree in Computer Science and Engineering (CSE) from Institute of Technology, Banaras Hindu University, Varanasi, India, M.Tech. degree in CSE from Indian Institute of Technology, Kanpur, and M.S. and Ph.D. degree in Computer and Information Science from Ohio State University, Columbus, OH. His current research focuses on dependable, criticality-aware, adaptive distributed systems with emphasis on wireless sensor networks, thermal and power-aware computing and communication, and pervasive healthcare. He has co-authored the book Fundamentals of Mobile and Pervasive Computing, McGraw Hill, and is currently on the editorial board of IEEE Communication Letters, IEEE Transactions on Parallel & Distributed Systems and Springer Wireless Networks. Gupta is a Senior Sustainability Scientist, in the Global Institute of Sustainability, ASU. His research awards include a Best 2009 SCIDSE Senior Researcher and a Best Paper Award for Security for Pervasive Health Monitoring Application. He is a member of the ACM and a senior member of the IEEE. Dr. Gupta heads the IMPACT (Intelligent Mobile and Pervasive Applications and Computing Technologies) Lab at Arizona State University. For information about his recent research projects and publications please visit http://impact.asu.edu.