Future Generation Computer Systems 56 (2016) 449–475

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Robust Cyber–Physical Systems: Concept, models, and implementation☆

Fei Hu [a], Yu Lu [a], Athanasios V. Vasilakos [b], Qi Hao [c,*], Rui Ma [a], Yogendra Patil [a], Ting Zhang [a], Jiang Lu [a], Xin Li [a], Neal N. Xiong [d]

[a] Electrical and Computer Engineering, University of Alabama, USA
[b] Department of Computer and Telecommunications Engineering, University of Western Macedonia, Greece
[c] Electrical Engineering, South University of Science and Technology, China
[d] School of Computer Science, Colorado Technical University, CO, USA

HIGHLIGHTS

- Comprehensive survey on entire CPS design process.
- Qualitative and quantitative descriptions on CPS resilience.
- From basic concepts to case studies.
- Point out the future research trends.

ARTICLE INFO

Article history:
Received 14 January 2015
Received in revised form
7 May 2015
Accepted 16 June 2015
Available online 8 July 2015

Keywords:
Cyber–Physical Systems
Stability
Security
Sensors and actuators
Survey

ABSTRACT

In this paper we comprehensively survey the concept and strategies for building a resilient and integrated cyber–physical system (CPS). Here resilience refers to a *3S*-oriented design, that is, stability, security, and systematicness: Stability means the CPS can achieve a stable sensing-actuation close-loop control even though the inputs (sensing data) have noise or attacks; Security means that the system can overcome the cyber–physical interaction attacks; and Systematicness means that the system has a seamless integration of sensors and actuators. We will also explain the CPS modeling issues since they serve as the basics of 3S design. We will use two detailed examples from our achieved projects to explain how to achieve a*robust, systematic* CPS design: Case study 1 is on the design of a rehabilitation system with cyber (sensors) and physical (robots) integration. Case Study 2 is on the implantable medical device design. It illustrates the nature of CPS security principle. The dominant feature of this survey is that it has both principle discussions and practical cyber–physical coupling design.

1. Introduction

1.1. What is CPS?

The ultimate purpose of using *cyber* infrastructure (including sensing, computing and communication hardware /software) is to intelligently monitor (from physical to cyber) and control (from cyber to physical) our *physical* world. A system with a tight coupling of cyber and physical objects is called cyber–physical system (CPS) [1–3], which has become one of the most important and popular computer applications today. In Table 1 we have listed the major differences between cyber resources and physical objects [4,5].

Computational and digital technologies will soon be found in, and play an integral role in many physical structures and devices. Just like how the Internet has revolutionized how people interact with each other and allowed us to more easily connect and trade with one another, CPSs also have the same potential to change how we interact with the physical world around us [6]. The implementation of the Internet is based on the integration of major

☆ This work is partially supported by U.S. National Science Foundation (NSF) grants CNS #1335263, IIS-0915862, CNS-1059212, and DUE-1315328. All ideas presented here do not necessarily represent NSF's opinions.

* Corresponding author.
E-mail addresses: hao.q@sustc.edu.cn (Q. Hao), xiongnaixue@gmail.com (N.N. Xiong).

http://dx.doi.org/10.1016/j.future.2015.06.006
0167-739X/

Table 1
A comparison of cyber and physical properties of CPS.

	Cyber	Physical
Method of ensuring proper order	Sequences	Real time
Event synchronization	Synchronous	Asynchronous
Time properties	Discrete	Continuous
Structure	Computing abstractions	Physical laws

Table 2
CPS example—Smart Grid: power electronics sensors/controllers.

Location	Sensor/Controller names	Functions
Storage	• AC (Alternating Current) sensor: • Power level sensor: • Power release controller:	Measure AC frequency oscillation Indicate the current energy storage Controls release/storage of electricity
Transmission line	• Impedance sensor: • Inverter controller:	Detect power line breakage Stop/allow the local AC transmission
Wind turbine	• Pressure/wind speed sensors: • Wind blade controller: • Wind generator controller:	Shows the energy generation strength Stop the wind fans if hardware fault detected Control for wind power generation
Solar panel	• Solar PV voltage sensor: • Solar PV controller:	Shows the energy generation strength Control for solar power generation/integration
MG/PG interface Generator	• Switch Controller: • Temperature /vibration sensor:	Switch between islanded/connected modes. Indicates generator's working status

advancements in network technology, applications and infrastructure. Likewise, CPSs can be seen as the integration of embedded systems, sensors, and control systems [7].

There are a number of technological advancements being made that are opening the door for CPS improvement. Sensors are becoming cheaper as they get smaller and smaller. There is also the breakthrough in wireless communication, Internet bandwidth, and the constant rise in alternative energy sources [8]. Computer parts are becoming increasingly more high-capacity at lower power consumption and smaller form-factors. As a result, the CPS is also becoming more and more demanding in the fields of aerospace [5,9], defense [10,11], energy systems [12,13], healthcare [3,14–17], transportation [18–22], and others [23–25].

A CPS can be thought of as the utilization of the logical and discrete properties of the computers to control and oversee the continuous and dynamic properties of physical systems. Using precise calculations to control a seemingly unpredictable physical environment is a great challenge [26]. The uncertainty and lag from real-time physical system to discrete-time digital control is an obstacle that must be overseen. The failures or safety issues must be contained and dealt with in an efficient manner [27]. Synchronization within a system and over complexity are also other obstacles that must be taken into consideration in order for the CPS field to grow [28].

A CPS often relies on sensors and actuators (or called actors, in some cases even called controllers) to implement tight interactions between cyber and physical objects [12]. The sensors (cyber objects) can be used to monitor the physical environments, and the actuators /controllers can be used to change the physical parameters. Table 2 shows the examples of sensors and controllers used in a typical CPS—smart grid. The smart grid requires that all storage controllers timely release a certain level of electricity to different transmission line segments based on their local inverters' voltage measurements and other sensors' input.

Regarding the interactions between sensors and controllers, here we use a wind power system as an example (Fig. 1), in which there exist three types of communications among sensors and controllers [29]: (1) Sensor-to-sensor (S–S) coordination: the sensors in a power cluster (with hundreds of wind turbines) need to communicate with each other to find an electromagnetic distribution map for power flow analysis. (2) Sensor-to-controller (S–C) coordination: A controller makes decision based on the collected sensor data. A controller may need both local and remote sensors' data. (3) Controller-to-controller (C–C) coordination: A controller may need to coordinate with other controllers to make a coherent decision. For instance, a storage controller needs to work with other controllers (that control loads and renewable sources) to decide whether the storage unit should be charged or discharged and how much electricity load it should handle. A controller for a renewable energy source (such as a wind turbine or solar PV), needs direction from a system controller (Fig. 1) to control its power production so as to assure a stable and reliable system operation.

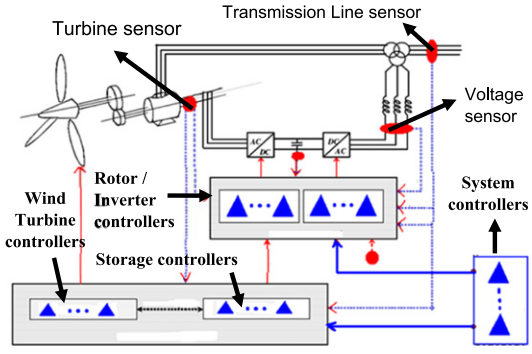


Fig. 1. Sensors/controllers' locations in a CPS (smart grid).

The sensor and controller relationship can be represented as a networked control system with inputs (sensors' data) and outputs (control commands) [30]. As shown in Fig. 2, a wireless sensor and controller (WSCN) with delay and packet loss can be used to describe a CPS. It has state transitions based on the control results.

Here we use another civilian example to illustrate CPS architecture. An intelligent water distribution network is shown in Fig. 3 [31]. Among the *physical* components, there are pipes, values, and reservoirs. Using this system, researchers are able to track water use. They are also able to predict where the majority of water will be consumed. It has a multi-layer architecture. One layer is the actual water flow, such as a reservoir of a sink. This layer has *cyber* objects (sensors) that communicate to the higher level cyber objects such as computer devices on how much and when the water will be used. This allows the computers to be able to allocate water to where it will be needed at the correct times. It also allows

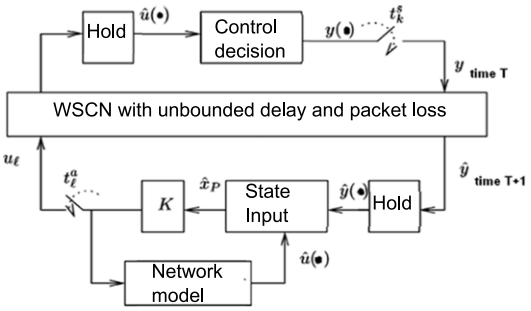


Fig. 2. CPS state transition (time $T \rightarrow T+1$).

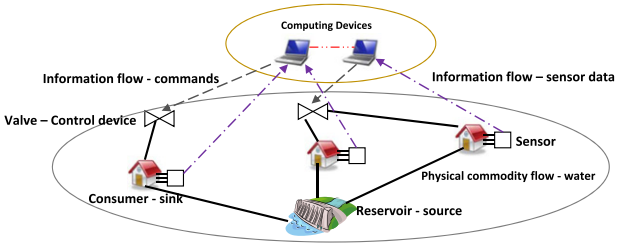


Fig. 3. CPS example: Water distribution system.

for monitoring of the maintenance side of water flow. It achieves this by monitoring what amount is being used at a house and how much water is being sent to that section. If there is a leak, then more will be sent to that section than what is being used so then they will know there is leak or malfunction.

1.2. CPS design challenges

A *resilient* CPS design includes three features (3S): (1) *stability*: no matter how the environment generates noise and uncertain factors, the control system should always reach a stable decision result eventually; (2) *security*: the system should be able to detect and countermeasure the cyber–physical interaction attacks; (3) *systematicness*: the cyber and physical components should be seamlessly integrated together into a systematic design [32–34].

To achieve such a resilient CPS, the following 5 challenges should be addressed:

(1) **Dependability**: Dependability is an important quality for any CPS. As an example, the framework called intelligent physical world (IPW) [35] helps to add the adaptive behavior to the CPS. Adaptability brings higher dependability. Here raw physical processes (RPP) data is collected, and the system is controlled by an intelligent computational world. For ease of understanding, physical world and computational world are denoted as A_p and A_c, respectively. Together A_p and A_c create a management-oriented feedback. This will allow A_c to see the behavior changes that A_p makes. When looking at A_p as a black box system, there are three domain characteristics: programmability, observability, and computability. Using these characteristics, three important categories in dependability can be achieved: QoS, fault-tolerance, and timeliness. The QoS is a measurement of how well the system resources are allocated depending on which part of the system the user is currently using. Fault-tolerance measures how a system is impacted by a failure. These factors need to be met so that dependability can be achieved during times of failure.

(2) **Consistency**: to achieve consistency, each component in the CPS can be accounted for in a base architecture (BA) [36], and every path of communication and physical connection between elements is allowed in the BA by connectors. This means

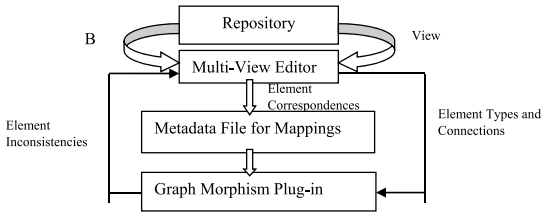


Fig. 4. Consistency checking design flow using AcmeStudio [36].

that the system should know all the possible paths. If a wrong connection or assumption is made, it will not be in the BA. To show this multi-view consistency, additional tools are needed. AcmeStudio framework [36] is used to help do this. It creates architecture design environments. Fig. 4 shows the design flow used to check consistency. The BA and system view are compared for consistency in AcmeStudio. The graph morphism plug-in checks the consistency of the system view. This is done by looking at the component-connector graph of the BA. If the elements are inconsistent, the multi-view editor can be used to make corrections.

(3) **Reliability**: A disconnection often lies between program execution and physical requirements. Programs have, essentially, 100% reliability in the sense that it will go through the exact same set of commands in exactly the same order every time it is run. However, physical systems rely not only on function but also on timing, and computer programs can be imperfect in this aspect. This mismatch causes much uncertainty and unreliability and becomes a problem for CPSs. There are essentially two ways to deal with uncertainty in computer systems: either reduce the uncertainty in each part as much as possible so that the reliability is very close to 100%, or implement algorithms to correct errors caused by imperfect reliability in the electronic components [37]. To make the CPS behavior predictable, some artificial intelligence or machine learning schemes can be used to predict the next-time system state. For example, we may build a regression model or hidden Markov model to describe the CPS time evolution dynamics. Thus we can predict the next-step system state based on the history state evolutions.

(4) **Cyber–physical mismatch**: In a CPS the interaction and coordination between the physical elements and the cyber elements of a system are key aspects. In the physical world, one of the most dominant characteristics is its dynamics, or the state of the system constantly changes over time. On the other hand, in the cyber world, these dynamics are more appropriately defined as a series of sequences that do not have temporal semantics. There are two basic approaches to analyzing this problem: *cyberizing the physical* (CtP) which is where cyber interfaces and properties are imposed on a physical system; and *physicalizing the cyber* (PtC) which is when software and cyber components are represented dynamically in real time [38,39].

(5) **Cyber–physical coupling security**: A CPS should be resilient to both natural faults and malicious attacks. Especially, we will describe how we could use a suitable control model and corresponding security schemes to build a resilient CPS. In CPS the physical systems are susceptible to the cyber security vulnerabilities from monitoring and control security perspective (Fig. 4). Here we list some examples of CPS attacks: in 2008 a senior analyst of the CIA stated that there were computer intrusions into some European power utilities followed by extortion demands [40]; in 2010 people demonstrated a software tool called CarShark [41] which could remotely kill a car engine; some hackers have broken into the US air traffic control systems [42]; in 2010 hackers designed a virus which can successfully attack Siemens plant–control system [43] (see Fig. 5).

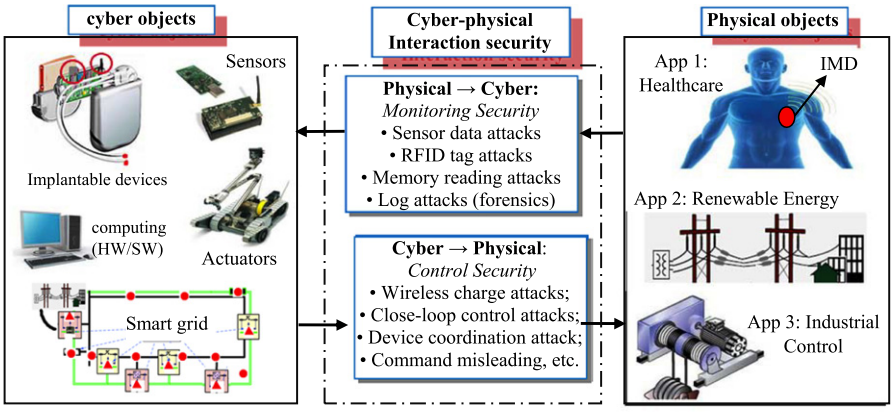
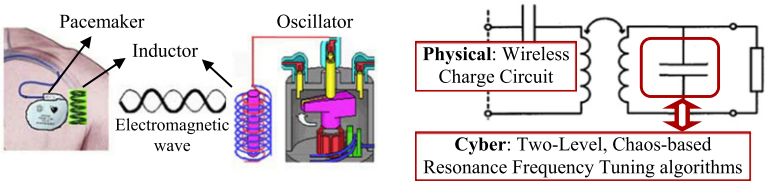


Fig. 5. Cyber–physical systems (CPS): Security Perspective.



(a) Wireless IMD power charge.

(b) CPS-oriented security solution.

Fig. 6.

We may not simply use conventional, general cyber security schemes to achieve all CPS protections. This is because most CPS security solutions need to be closely integrated with the underlying physical process control features [44,45]. As an example, a typical CPS, called implantable medical device (IMD), may be implanted in the human body for both physical-to-cyber medical sensing and cyber-to-physical organ control. Typical IMDs include pacemakers, neuro-stimulators, insulin pumps, and others. An IMD attack called wireless power charge attack, is a critical issue since an attacker who knows the coil resonance frequency can cause the IMD to overheat. It is meaningless to use conventional cryptographies to encrypt the power charge waves since energy transfer is entirely different from data transfer (Fig. 6(a)). We may use a *CPS-oriented security* solution to solve the above issue (Fig. 6(b)): using *cyber* scheme (chaotic maps) to control the *physical* object (circuit capacitors) in order to prevent an attacker from guessing the power charge resonance frequency that secretly switches values.

1.3. Contributions of this paper

This paper has the following three dominant features:

(1) *Comprehensive survey on entire design process*: First, unlike other CPS surveys (such as [3,10]) that only focus on a small aspect (such as security), this comprehensive survey covers the entire CPS design process including concept, modeling, control, security, and cyber–physical coupling. It summarizes the latest literature in those aspects. It describes the connections between control models and security.

(2) *Qualitative and quantitative descriptions on CPS resilience*: We will use both qualitative discussions and quantitative math models to describe the 3S-oriented CPS design. For instance, we will provide the detailed networked control models to describe the sensors and actuators interaction principles. We will also discuss CPS QoS models, as well as the multi-agent based CPS control. When we discuss CPS security issues, unlike existing surveys (such as [10]) that aim to cover all general security aspects, we focus on the math models for networked control and state estimation, and quantitatively describe how the CPS attacks mislead the actuators.

(3) *From basic concepts to case studies*: While other surveys mostly describe general concepts in CPS design, we will take our funded CPS projects as case studies with detailed control models and security support. We will use two typical CPS applications—virtual reality based rehabilitation and implanted medical device design, to introduce the important principles of sensor–actuator interactions, as well as CPS security issues.

Road map: The rest of this paper is organized as follows: In Section 2, we will introduce some important cyber–physical coupling models, which will serve as the fundamentals of 3S discussions. Section 3 will focus on stability-oriented CPS design. Section 4 moves to security topics. In Section 5 we describe the integration principles in CPS, and then use our two CPS projects in Section 6 to discuss about systematisms, that is, how to integrate cyber and physical units seamlessly. Section 7 discusses the future development trend in this field. Section 8 concludes this paper.

2. CPS modeling

A suitable CPS model with quantitative cyber/physical interaction descriptions is important to understand different types of control and security designs [46–48]. Therefore in this section we will explain some modeling issues in CPS. For example, how do we model the time and schedule between different actuator's events? How do we reflect the action inter-locking relationship? We will use a few examples to illustrate the modeling concepts.

Physical processes are made up of a combination of different processes that run in parallel with each other. The job of measuring and controlling these processes by orchestrating actions that influence on the processes is a very important task performed in an embedded system [49]. Models are a major stepping stone in the development of CPSs. Models can show how the design process has evolved, and help to form the specifications that govern a

system [50]. In addition, models allow a CPS design to be tested in a safe environment, which will allow engineers to determine if any design defects exist [51]. To model a CPS, engineers will have to include the models of the physical processes as well as models of the software, computation platforms and networks [52].

2.1. Models based on timed actors

The design of CPS requires attention to not only the functional aspects, such as behavior and correctness, but also to the non-functional aspects, specifically timing and performance. In [53] it introduces a theory of timed actors that contrast with the classical behavioral and functional refinements based on restricting sets of behaviors. The refinement of this theory improves efficiency and reduces complexity by allowing time-deterministic abstractions to be made. It shows how this theory can be used to increase both time and performance of CPSs. Two aspects that play key roles in developing these large and complex systems, are abstraction and compositionality. Such a theory falls under the category of *interface theories*, which focus on dynamic and concurrent behavior. The interfaces, called *actor interfaces*, are inspired by actor-oriented models of computation such as process networks and data flow. Actors generate tokens on their output ports, and consume tokens on their input ports. Actions are defined as relations between input and output sequences of discrete events occurring in a given time axis. The main point of this theory is centered on refinement, and is based on the principle *the earlier the better*. Such a principle is interesting because it allows deterministic abstractions of non-deterministic systems [54]. Due to some reasons such as high variability in execution and communication delays, dynamic scheduling, and other effects, it is expensive or impossible to model precisely. Time-deterministic models, on the other hand, suffer less from state explosion problems, and are also more suitable for deriving analytic bounds [55].

2.2. Event-based CPS models

Initially, the event has to be sensed and detected by the proper components in the CPS's cyber world. Next, the correct actuation decisions have to be made. All these duties must be performed within a specific time frame. In reality, the individual timing constraints for each individual component vary due to the non-deterministic system delay caused by the several different actions in the CPS, such as sensing, computation, communication, and actuation. When all these systems come together with their own individual timing constraints, the overall timing factor of the CPS becomes a significant challenge [56].

The close interaction that the CPS has to the physical world indicates that the time constraints can be handled by using an *event-based approach*. An event-based approach uses events in the CPS as units for computation, communication, and control in the system. CPSs consist of a distributed set of the aforementioned components that operate in their own individual reference frames, therefore a CPS is better characterized by spatio-temporal information. A common frame of reference does not exist since CPSs have a heterogeneous nature. Also, these events range from lower level events, such as the actuating and sensing events in the physical world, all the way to higher-level event, such as cyber events that are both machine and human understandable. There must be a unified definition and representation of these events. A certain systematic mechanism must be implemented to compose these CPS events from the higher and lower levels and across the different system boundaries [57]. The event model that results from this composition can both serve as an offline analysis and run-time implementation.

In [58] it introduces a concept—lattice-based event model for CPSs. The CPS event can be represented as three different components: the event type, the internal event attributes, and the external event attributes. These three components together can be used to define the spatio-temporal properties of the event, and also can be used to determine the components that observed the event.

2.3. SCADA model

Here we will introduce a popular, important CPS model—SCADA. Today's power grid is a complex system that continuously supplies power to an ever-changing and non-uniform customer base. In other words, the power grid must supply power to a variety of loads, whose demands will be constantly changing throughout a given day. This constant load change can result in fluctuations in the system voltage and frequency of the power grid. This results in an unstable system. To combat this problem, a system known as SCADA (Supervisory Control and Data Acquisition) is used to monitor conditions at High Voltage Substations. This collected data has been used to determine load forecasts at various parts of the day for different locations [59]. As a result, resources have been made available to maintain system integrity, with extra resources set aside in case of machine failure [60]. Large substations provide power to a variety of loads which can include residential, commercial, or industrial loads. As a result, the system continues to have stability issues because true system demands can never be accurately predicted [61]. Furthermore, to increase the overall efficiency of the power grid, more renewable energy sources such as Solar and Wind Farms need to be integrated into the existing system. For this to be successful there will need to be an increase in the overall intelligence capabilities of the various networks that control the power grid.

Large-scale sensor networks should be implemented to help gather more accurate data downstream of the substation. These sensors will be incorporated into the already used SCADA system. However, the sensors should not be used to bombard the ones responsible for the controlling the flow of power throughout the grid with data [62]. Instead, these sensors would be pulsed at regular intervals to determine the current demands on the power grid. This in a sense will provide real time data on the demands on the power grid. Using this data, different types of energy sources can also be integrated into the power grid to provide support; examples include Solar Panels and Wind Generators. These power systems provide a limited amount of power, while generator outputs at power plants can be increased or more generators can be brought online. Using this real time data, solar panel or wind farms can be utilized to help with the ever changing demands. As an example, if the demand for a certain area rises be a few megawatts, a nearby wind farm that is currently capable of meeting this demand can be used. This would result in less use of fossil fuels to increase the output of a generator at a nearby power plant.

2.4. Other modeling issues in CPS

For current mainstream programming paradigms, given the source code, the program's initial state, and the amount of time elapsed, we cannot reliably predict future program state [63]. When such a program is integrated into a physical system with physical dynamics, it makes the design of the CPS hard to accomplish. Furthermore, the differences in the dynamics of the physical plant and the controlling program can lead to several errors that can lead to catastrophic implications for the system.

Although CPU have become fast enough to control many physical objects, modern cyber techniques, such as CPU instruction scheduling, computer memory hierarchies, memory garbage collection, multi-thread processing, networking, and reusable

component libraries, (which do not expose temporal properties on their interfaces), introduce enormous temporal variability [64]. CPS does not rely on fast computing, but does require physical actions to be taken at the proper time [65].

The integration of cyber and physical processes is a challenge. This challenge has motivated the emergence of hybrid systems theories. However, progress in hybrid systems theories has been limited due to the combination of ordinary differential equations and automata in relatively simple systems [66]. These models have a uniform notion of time that is inherited from control theory [67]. In these systems, time (t) is simultaneously available in all parts of the system. By integrating the consensus concept with control theories, we can describe a series of dynamical systems such as flocking, sensor fusion, coupled oscillators, etc. But those dynamical systems often lack the uniform time model that governs the dynamics [63].

A CPS is made by integrating computational and physical processes. The computational processes include computer and networking systems to monitor and control a physical process [68]. This is accomplished by using feedback control loops. The signals received from the feedback loops will be used to control the computational part of the process. As a result, the controller will cause a dynamic change in the system based on the computations and feedback signals. The process will then repeat. As a result, a designer must have a thorough understanding of the dynamics of software, networks, and the physical process to be controlled [69].

The physical processes of a CPS can be represented as continuous-time models of dynamics and computations, which results in a hybrid model [68]. There are several software programs that can be used to model dynamic systems. Simulink and LabVIEW Control Design are two examples [70].

There are some high level modeling methods could be used to make the developing progress more efficient, such as model-driven development (MDD) (e.g., UML), model-integrated computing (MIC), and domain-specific modeling (DSM) [71].

MDD is a software design methodology. It defines the system functionality using a platform-independent model (PIM) with an appropriate domain-specific language (DSL). MDD emphasizes the use of rigorous visual modeling schemes (such as UML, BPMN, SysML, ArchiMate, etc.) during the whole software development life cycle.

MIC is an enhanced MDD concept. It emphasizes the formal representation, composition, analysis, and manipulation of software design elements. It covers the entire software design cycle, including specifications, design, development, verification, integration, and maintenance. It uses DSM, and includes the fully integrated metaprogrammable MIC tool suite. It also has an open integration framework for formal analysis and model transformations.

3. Stability

3.1. Robust control to achieve CPS stability

In this section we will cover the CPS stability issues. Stable system often needs solid control theory as its input–output interactions. For example, how do we design the closed-loop models between sensors and controllers? What is the impact of control delay in CPS management?

Here we use an example called data center cooling [72] to explain the basic principle of CPS control. In today's world, the need for data centers is quickly growing with the expansion of computational resources integrated with everyday life. Demand for resources such as cloud computing and mass data storage require the use of large data centers with dedicated hardware to support multiple users [73]. Utilizing a cyber–physical approach to model the system yields two interrelated models, the computational network

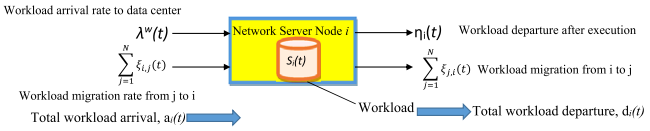


Fig. 7. Graphical representation of data center node.

and thermal network, which model the cyber and physical dynamics of the data center. The cyber aspects of the model represent the computational variables, such as data rate and processing speeds. The physical dynamics cover the heat generated by such activity in addition to the computer room air conditioning (CRAC). The current paradigm revolves around three general models: server level, group level, and data center level controls:

(1) At the server level, control takes place at each individual server machine. Things such as computing resources in terms of CPU cycles, networking, and memory are maintained to reduce power consumption and in turn, heat generation. Previous solutions to the server level model of control include dynamic voltage and frequency scaling (DVFS) which throttles certain CPU characteristics under idle conditions to achieve better power efficiency. In addition, server specific fans are included in this category, in which constraints on the thermal generation of a unit are applied to the processing capabilities.
(2) Group level control applies to the nodes which describe a single application using multiple servers. In the case of group level control, performance tends to involve migration of workloads across virtualized environments. This is accomplished by hosting servers in virtual machines (VM) which can in turn be transferred to different hardware. This allows for processing to be distributed across multiple platforms to balance the workload and lower power consumption across the group.
(3) Lastly, in data center level control, certain capacities are shared amongst all the units, elevating control to cover entire data center. One of the main characteristics in data center level control is that several aspects from the previous mentioned levels are integrated into this top level. This includes measures such as server level optimization and group level migration. In addition, CRAC control is used while enforcing certain constraints to address thermal distributions across the data center. Current solutions at this level implement the previous level solutions with regard to power consumption as well as heat distributions. This can involve consolidation of server loads into a smaller subset of servers for energy efficiency. This allows idle servers to shut off during idle times. The problem with this approach lies with the unacceptable effects on QoS.

In development of a model for the data center cooling, a CPS control model is proposed in [72]. Network servers are represented as nodes with data arriving for computation and leaving by execution or migration to a different node. A graphical representation can be seen in Fig. 7 with mathematical notations.

This graphical representation is derived from the following set of equations:

$$a_i(t) = \lambda^w(t) S_i(t) + \sum_{j=1}^{N} \xi_{i,j}(t) \tag{1}$$

$$d_i(t) = \eta_i(t) + \sum_{j=1}^{N} \xi_{i,j}(t). \tag{2}$$

In addition to these equations, a third equation governs the bounds in which they operate:

$$\upsilon_i(t) = \mu_i(t) + \sum_{j=1}^{N} \delta_{i,j}(t) \tag{3}$$

where the desired departure rate for a given node, $\upsilon_i(t)$, is given by the desired execution rate, $\mu_i(t)$, plus the required migration rate $\sum_{j=1}^{N} \delta_{i,j}(t)$. In addition to this, $\eta_i(t)$ is defined as either $\mu_i(t)$ (if the total arrival rate a is greater than the total departure rate d) or arrival rate $a_i(t)$ otherwise. The thermal network of the data center is represented in a similar fashion with input and output with the following equations:

$$T_{\text{in},i}(t) = \sum_{j=1}^{M} \Psi_{i,j} T_{\text{out},j}\,(t) \tag{4}$$

$$T_{\text{out},i}(t) = -k_i T_{\text{out},i}(t) + k_i T_{\text{in},i}(t) + c_i p_i(t). \tag{5}$$

In the above equation, the input temperature for a node is given as the sum of all the nodes' output temperature from i to M. Furthermore, the output temperature is given as a linear time-invariant description involving time constant k and power consumption coefficient c. Power consumption is proportional to the temperature by the departure rate by execution from a node, η by a non-negative coefficient α. By solving the above sets of equations as a minimization problem for temperature, various results are given for different implementations of the control system strategies.

Simulation of the data center's cooling is completed using three different scenarios: coordinated, uncoordinated, and baseline strategies. The first scenario utilizes data from both the cyber and physical aspects of the data center to achieve optimization. The second scenario implements strategies for both the cyber and physical aspects, but independently from each other. Lastly, the baseline strategy implements a constant method of dealing with temperature that is independent of optimization. Results for power and average utilization demonstrate the effectiveness of the CPS control in the case of the data center cooling.

3.2. Multi-agent management to achieve CPS stability

In a CPS, the sensors and controllers need to exchange states among them in order to reach a convergent decision result. Multi-agent theory could be used to represent the interaction models among sensors and actuators/controllers and reach a convergence status [74]. Here we use power grid CPS as the example to illustrate the benefits of using multi-agent models. The same principle can be easily applied to other CPS.

One of the most challenging issues for power grid (PG) design is to handle the electricity load oscillation problem due to sudden micro-grid (MG) interconnection/islanded operations [75]. As shown in Fig. 8, the renewable energy system achieves electricity load balancing through the distributed sensor–controller (S–C) coordination: in order to determine the amount of released electricity for entire MG load balance, a storage controller needs to collect parameters from all neighboring sensors (such as turbine speeds and generator voltage), and also to communicate with other MG storage controllers for coherent decision making. On the other hand, a wind turbine or a solar PV controller may need to reduce or shut off its energy generation after receiving an overload message from storage power level sensor. The challenging issue is: How to design a scalable S–C coordination protocol that runs a distributed convergence algorithm to achieve the global MG optimization (i.e., load balancing)? Here we can use multi-agent concept and its corresponding distributed cost propagation algorithm to achieve scalable S–C coordination.

Multi-agent model: *Agents* are autonomous entities that can receive sensory inputs from the environment and then act on it using their effectors based on the knowledge they have of the environment [76]. Agents are able to interact, when appropriate, with other agents in order to solve their own problems and to help

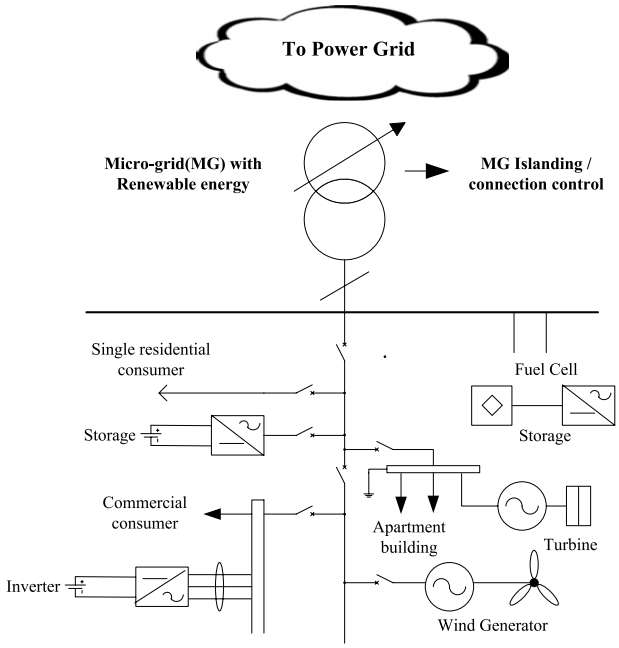


Fig. 8. Power grid CPS architecture.

others with their activities. A multi-agent system (MAS) is a system composed of multiple autonomous agents, and it allows for the distribution of knowledge, data, and resources among individual agents. Its modularity supports the development and maintenance of complex highly reliable systems [77].

In this CPS, an agent could be a controller (called active agent since it can make decisions) or a sensor (called passive agent since it only provides inputs). An agent can collect the statistics from other agents nearby. An agent's neighborhood consists of those agents with whom it has frequent interactions. These interactions include sharing of information and negotiating about resource assignments. Based on locally collected inputs, each agent makes control decisions based on optimization functions, negotiates control decisions with other agents [78].

Agent-based S–C coordination: First, we consider the following parameter inputs from different MG agents (Fig. 8): the amount of released/stored energy in storage controllers, the rotation speed from turbine controllers, the generator output affiance (watts per second) from generator controllers, and the regional AC (Alternating Current) frequency and voltage from *Inverter controllers*. Then, we seek an MG electricity load balancing between different agents through the following typical AC voltage models:

$$\omega = \omega_{\text{grid}} - k_P \times P, \qquad V = V_{\text{grid}} - k_Q \times Q, \tag{6}$$

where P and Q are the inverter active and reactive power outputs, k_P and k_Q are the droop slopes (positive quantities), and ω_{grid} is the angular frequency (phase), and V_{grid} is the terminal voltage. The purpose of distributed S–C coordination is to achieve a global load optimization:

$$\Delta P = \sum_{i=1}^{n} \Delta P_i \tag{7}$$

where ΔP_i is the power variation in the ith inverter agent? The AC frequency variation is:

$$\Delta\omega = k_{Pi} \times \Delta P_i. \tag{8}$$

As we can see, the ith inverter agent contributes the entire MG load balance at a certain weight k. From agent-model viewpoint, this is a typical dynamic optimization issue. We need to design

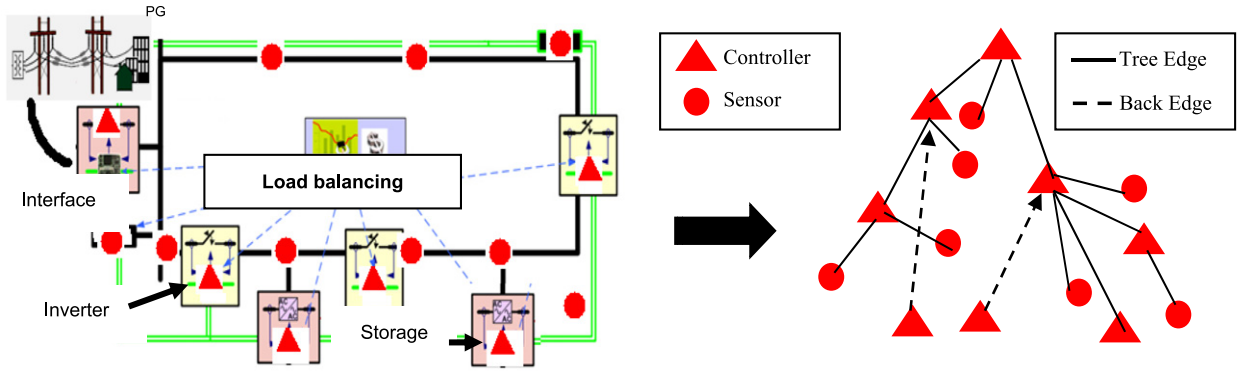


Fig. 9. Establish pseudo-tree in multi-agent model.

fully distributed algorithms to achieve the equivalent outcome of centralized control. The distributed algorithm should have the following features [79]: (1) Completeness: it should be guaranteed to find the global optimal solution, not any local optimum; (2) Bounded solution-finding delay: it should be guaranteed to reach the final solution in a bounded delay; (3) Low generated overhead: it should use only local information collection and exchange.

Considering the above requirements, we can use an Adaptive Distributed Optimization (ADOM) algorithm for MG S–C coordination. It is fully distributed without a centralized controller. It uses tree propagation algorithms with bounded solution-finding delay, and it is guaranteed to reach the global optimal solution, i.e., a complete algorithm [80]. The ADOM algorithm uses DFS (Depth-First Search) traversal: it performs a distributed depth-first traversal of all the agents involved in the control to establish a pseudo-tree structure. Each agent (sensor or controller) is a node in the constructed pseudo-tree. The pseudo-tree provides divide-and-conquer techniques for search algorithms. An example of the established pseudo-tree for a MG is shown in Fig. 9. The agent with the maximum number of neighboring agents in the topology graph is chosen to be the root.

3.3. Other strategies for robust CPS control

There are some other works on achieving a robust CPS control. In [81] the authors pointed out that any robustness models for CPS should be based on the existing results of physical systems, which can be analyzed via continuous mathematics and continuity concepts. It states that the cyber part is especially important in a CPS from robust design viewpoint. Therefore, it clearly defines the behavior models of robust cyber components. It also quantifies "small" disturbances and "close" behaviors. Those concepts serve as the foundation of continuity model. Another contribution of [81] is that the transducers and cost functions are provided. The verification and synthesis issues that come with robustness models are also discussed.

In [82] a fast optimization solver for model predictive control (MPC) at Megahertz rates is detailed. They have proposed a few custom computational architectures for different 1st-order optimization models in order to handle linear–quadratic MPC problems with inputs and states. For input-constrained problems, it provides architectures for Nesterov's fast gradient method. For state-constrained problems it uses architectures based on the alternating direction method of multipliers (ADMM).

The CPS control needs to have stable performance even under communication constraints and limited resources. In [83] it has investigated the optimal control design for arbitrary non-linear processes under communication and processing constraints. It has deduced the stability results in terms of an inequality that relates open-loop growth of the plant state, packet erasure probability, and parameters of the processor availability model. The sensors use event-triggered scheme instead of continuous state updating in order to reduce the communication overhead.

In addition, other CPS control stability issues have been investigated through event- or self-triggered updates of the control parameters, with the goal of reducing the processor load and communication overhead [84–86].

4. Security

Security is critical to the CPS since the sensing or acting units could be attacked in various ways [87]. For instance, from individual CPS component viewpoint, an adversary may make a sensor generate falsified data or make a controller generate wrong commands. From unit communication viewpoint, the attacker can intercept the messages, launch DoS (denial of service) attacks, inject/modify/drop communication messages, etc. [88].

In this section, we will discuss CPS attack models, attack detection methods, and countermeasures. We will also use concrete examples (such as power grid) to illustrate the CPS security issues. Unlike other CPS surveys (such as [10]) that cover general security descriptions, here we focus on the math description of CPS attack models as well as the attack detection methods. Due to the special networked control architecture in a CPS, the attack models should involve the system stability and state transmission issues. Our discussions here will focus on how an attack can mislead the state estimations.

4.1. CPS attack types/models

4.1.1. Denial of service (DOS) attack

Denial-of-Service attacks can be represented graphically as a switch that opens and closes, effectively shutting out new data from reaching either the sensors or controllers in CPS. Two types of mathematical representations can be used to describe DOS attacks.

(1) *Bernoulli model*: Befekadu uses in his first model [89], an independent Bernoulli process to model a DOS attack against a discrete-time partially observed stochastic system:

$$x_{k+1} = Ax_k + \beta_{k+1}Bu_k + v_{k+1} \tag{9}$$

$$y_{k+1} = Cx_k + w_{k+1}. \tag{10}$$

The first equation represents the state given as a closed loop system where x is the state, β is the DOS sequence $\{0, 1\}$, u is the control input, and v is a normal distribution to introduce randomness. In the second equation, the observation of the output, y, is related to the control state with additional noise or randomness. The attack

model is represented with Bernoulli probabilistic trials. In the case of success, the switch is opened, preventing flow and thus '1'. In the opposite case, a '0' represents failure. The general solution is developed such that a recursive function as below, provides an information state, δ, of the control system based on its own current value in relation to control data, anticipated attack sequence, and observations.

$$\delta_{k+1} = \delta_{k+1}(\delta_k,\ u_k,\ y_{k+1},\ \beta_{k+1}). \tag{11}$$

(2) *Markov model*: While the Bernoulli model in the previous section suffices to model a DoS attack on CPS control loop, it is possible to model a more sophisticated attack by using Markov hidden variables. This approach allows states to be taken into account, compared to the memory less Bernoulli model [90]. Given the above system, the Markov process is:

$$Y_k = F_k(Y_{k-1}) + W_k \tag{12}$$

where F_k is a bounded measurable function acting on sensor distribution Y_{k-1}, and W_k is a random noise.

4.1.2. False data injection attack [91,92]

False data injection attacks tend to be more subtle than their DOS attack counterparts [93,94] and thus difficult to detect. It is shown by Cardenas et al. [95] that given a linear representation of a CPS, it is possible to solve for an attack strategy that goes completely undetected by prevention schemas. Mo and Sinopoli formulate the necessary conditions under which an attacker is able to perfectly bypass defensive strategies of a control system scenario defined with a Kalman filter, linear–quadratic-Gaussian (LQG) controller, and a failure detector. The CPS is modeled classically as a LTI (linear time-invariant system):

$$x_{k+1} = Ax_k + Bu_k + w_k \tag{13}$$

where x is the state variable for a time k, u defines the control input, and w describes a certain amount of noise with $N(0, Q)$. An initial state x_o is also given as $N(0, \sum)$. The following sections will describe the individual components of the CPS with relation to the LTI system.

The Kalman filter accomplishes the task of providing a certain system state estimation, $\varkappa$, given in the measurements provided by:

$$\varkappa_{k+1} = A\varkappa_k + Bu_k + K[y_{k+1} - C(A\varkappa_k + Bu_k)] \tag{14}$$

$$y_k = Cx_k + v_k, \tag{15}$$

where K is the Kalman filter gain which varies with time. The measurement y is given by the state variable and randomness $v \sim N(0, R)$. $y_{k+1} - C(A\varkappa_k + Bu_k)$ is further simplified to z_{k+1}, which defines the residue generated by various processes. The error in state estimation is given by $e_k = x_k - \varkappa_k$.

To ensure system stability, the LQG controller must minimize the function:

$$J = \lim_{T\to\infty} \min E\frac{1}{T}\left[\sum_{k=0}^{T-1}(x_k^T W_{x_k} + u_k^T U u_k)\right]. \tag{16}$$

Through this equation and the error of state estimation from the previous section, the stability of the system is assured assuming $cov(e)$ and J are bounded. Failure detection is described with a quantified value from a function:

$$g_k = z_k^T \boldsymbol{COV} z_k, \tag{17}$$

where **COV** is the covariance matrix of the residue. Due to the Gaussian nature of the residue, the value g can be used in comparison to a threshold value such that an alarm is triggered when $g >$ threshold. This further refines the attack sequence to $\beta = P(g_k > threshold)$.

4.1.3. Risk assessment model [91,92]

In order to minimize the impact of a given attacking event, risks are evaluated using a metric that calculates average loss by event [96]. The metric is given as $R_u = E[L] \approx \sum_i L_i p_i$, where R_u is the average loss, L_i is the loss given an event i, and p_i is the probability of the event. In testing this metric, the experiment involves a sensor network and an attack that compromises sensor i, and the corresponding loss L_i. Individual sensors in the network are measured as part of a vector $x(t) = \{x_1(t), \ldots, x_p(t)\}$ such that at time t there is a measurement $x_i(t) \in \mathbb{R}$ of sensor p within bounds of $x^{\max}$ or $x^{\min}$. Furthermore, the controller receives a certain measurement $\sim x_i(t) \in \mathbb{R}$ of sensor p. Therefore, under an attack situation, the received and actual value may be different. From this model, two types of attacks can be represented: integrity attacks and DoS attacks [11,97,98]. In the first type, a given sensor is compromised and arbitrary values are injected. To test the attacks, the model known as the Tennessee-Eastman Process Control System (TE-PCS) [99,91,92] is used.

The goal of the controllers is to regulate several flow rates within the system. First the flow rate of the product must be maintained at a consistent pace. Also, the operating pressure of the tank must be kept below 3000 kPa due to safety limitations. In addition to this, the pressure should remain as close as possible to the limit without exceeding it. The experiment assumes that at any given time, only a single sensor is compromised by the attacker. Effectiveness of an attack is determined by whether or not the compromised sensor can result in unsafe states or not. Examination of the effects of a DOS attack on the same sensor showed that under the duration of an attack, the pressure never exceeded the safety limitations. In general, DoS attacks were ineffective against the other sensors as well. Under cost constraints, sensor X5 should be secured under more advanced safety measures. Furthermore, defenses against integrity attacks should be prioritized given their effectiveness over DOS attacks [99,91,92].

4.2. Attack detection methods

(1) **Sequential/Change detection** [91,92]

Detection of attacks in a controls system differs from IT systems in that models can be made of the physical system based on expected reactions to a known input [100,91,92]. Given a certain control input sequence, the output sequence can be compared to the expected output to determine if the signal is compromised or not. In solving the problem of detection, two components are needed: a model of the physical system's behavior and a detection algorithm [101]. Two methods of detection are to be used in the simulation, sequential detection and change detection [102]. In optimizing these methods, the goal is to obtain the correct hypothesis within a minimum number of samples the former, while in the latter the goal is to detect a change at an unknown time. Sequential detection starts with the assumption that observations taken under a time sequence is either under the normal or attack hypothesis. Change detection on the other hand starts with the assumption that the observations start in the normal hypothesis before moving into the attack hypothesis [103].

With sequential detection, if it is assumed that there is a fixed probability of a false alarm and detection, the solution to the problem is a classical sequential probability ratio test (SPRT) [104,91,92]. The use of SPRT has been known to extend to other problems in security such as worms and port scans. Under SPRT, the following description is made: $S(k+1) = \log\frac{p_1(z(k))}{p_2(z(k))} + S(k)$, where $z(k)$ represents an observation generated by the probability distribution p_i. The decision is then made, defined as $d_N =$ attack hypothesis if $S(N) \geq \ln\frac{1-b}{a}$ or normal hypothesis if $S(N) \leq \ln\frac{b}{1-a}$. Variables a and b are the probability of false alarm and

missed detection respectively. N is equal to an infinite set of n such that $S(n)$ is not a false alarm or missed detection. Change detection can be represented identically to the sequential detection solution using cumulative sum (CUSUM), $S(k+1) = \log \frac{p_1(z(k))}{p_2(z(k))} + S(k)$. A simple alteration is made such that N now represents a set of n such that $S(n)$ is greater than or equal to a given threshold. Detection is made by $d_N =$ attack hypothesis if $S_i(k) > \tau_i$ or normal hypothesis otherwise. τ_i represents a threshold of false alarms. Only small constraints on placed on the observation sequence, taken from the ideas of nonparametric statistics, such that assumptions about the probability distribution for an attacker can be avoided.

Further establishing the simulation model, several types of attacks are considered to be used with the detection schemes. In [103] three types of attacks are discussed: surge, bias, and geometric attacks. Also, each attack is considered to be stealthy in which the attacker has complete knowledge of the system parameters such as the linear model matrices A, B, and C. Surge type attacks model an attack whose aim is to inflict maximum damage once access to the system is achieved. Bias attacks describe small modifications made to the system through small disruptions. The last attack describes small modifications initially, before moving to inflict maximum damage once the system is vulnerable. In running the experiment, the TE-PCS model is used, but replaced with a linear representation. In testing the system threshold, selected values of τ are tested against stealthy geometric attacks.

(2) **Probabilistic dependence graph**

In large-scale CPS, fault detection and localization are needed to ensure proper function. Using power grid as an example, a probabilistic graphical approach is introduced in [105] to utilize spatially correlated information from phasor measurement units and statistical hypothesis testing. A Gaussian Markov random field (GMRF) [106] is employed to model phasor angles across the buses in a power system in a way that the phasor angles are evaluated as random variables and their dependencies can be studied. The dependence graph illustrates the connections using a Markov random field that is induced by a minimal neighborhood system by inserting an edge between sites that are neighbors. The pairwise Markov property of a GMRF is also exercised such that a MRF is normal with the mean u and variance J^{-1} where J is the information matrix of the MRF, so in this instance J is zero. Also, Gaussian random variables are used to approximate fault diagnosis functions such as flow injection as a result of multiple load requests as well as difference of phasor angles across a non-slack bus [91,92].

Several models and hypotheses have been used to further illustrate these concepts. The conditional auto-regression (CAR) model [107] is a noteworthy model that explains the conditional distribution where X_{-i} is a MRF:

$$X_i|\mathbf{X_{-i}} \sim N\left(u_i + \sum_{j \neq i} r_{ij}(x_j - u_j),\ 1\right).$$

An approach was hypothesized such that the null hypothesis is as follows:

H_0 : {there is no change in r_{ij}, for all $\{i, j\}$ as an element of E'}

where E' is the edge set.

A challenge faced by these models and hypothesis is the difficulty in correctly estimating the information matrix of the MRF and in effect the actual value because of a small sampling number or noise involved. In the past, a centralized approach would have been exercised when faced with this problem. Samples are controlled to the size of the biggest subfield in the decentralized approach as opposed to the entire GMRF as is in the centralized method; therefore the involvement of the computations and measurements are significantly and beneficially reduced. Hypothesis investigation is also decomposed into smaller subproblems and as a result sites are divided into border sites and inner sites, and the edges are divided into tie-line, border-line, and inner-line edges. Tie-line edges connect subfields, border-line edges connect border sites within the same field, and inner-line edges connect subfields but have at least one of its ends as an inner site. To make the decentralized approach even more reliable, two-scale decomposition is employed to achieve message-passing used to accumulate data involving the subclasses of border sites and edges. Just as the two-scale decomposition, a multi-scale decomposition can be utilized as necessary for larger scale systems. Fig. 10 demonstrates this approach [91,92].

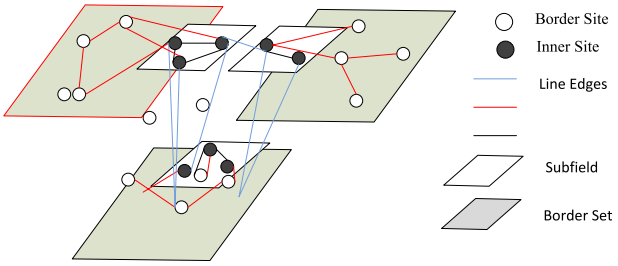


Fig. 10. Decentralized estimation with multi-scale message-passing [91,92].

(3) **Anomaly detection**

In [108] the anomaly and vulnerability detection are identified and resolved for the protection of power grid substations. Firstly, the type of intrusion methods must be identified such that normal operation of the power system will remain undisturbed. In power grid the CPS attacks can be employed in various ways. Some of them include synchronized attacks on several substations because of the accessibility of the infrastructure at multiple locations. And attacks from a vast array of combinations could remain unnoticed because of intelligence capabilities on the attacker's end. Fig. 11 illustrates the possible course an attack could take. As shown, intrusions could occur in remote connections through TCP/IP or through DNP/Modbus protocols. If the attacker is successful in gaining contact with *C1* or *C2*, the user interface as well as the substation IED's are vulnerable. The user interface contains a direct contact to overall substation communications and can therefore be used destructively to identify and devastate the exact components used for controlling switches, breakers, and other electrical equipment. Once a password for an IED is ascertained, the intruder will have access to important documents such as one-line and data flow diagrams, which can then be used to administer commands to circuit breakers that would cause catastrophic events to occur at the substation.

In order to become aware of such intrusions on substation networks made by cyber-attackers, an anomaly detection algorithm which employs benefits such as monitoring in real time, analysis of possible effects of intrusion, and approaches for mitigation, is examined. Monitoring the power system in real time enables the algorithm to rapidly and efficiently determine the status of computers and equipment in order to allow a maximum number of connections to be implemented, as well as authenticate the connection via response times and IP addresses. Such features can detect and track anomalies such as unsuccessful logon attempts in accordance with time and frequency and destructive modifications to files that are vital to the substation well-being. These are characteristics of an intrusion being attempted, and if an attack is suspected, an alarm list of possible attackers is created and the device the intruder is attempting to attack is put on lock. Table 1 explains the anomaly detection algorithm described. The last column in which the intruder attempts to change factory settings is the location in which the event is extracted (see Table 3).

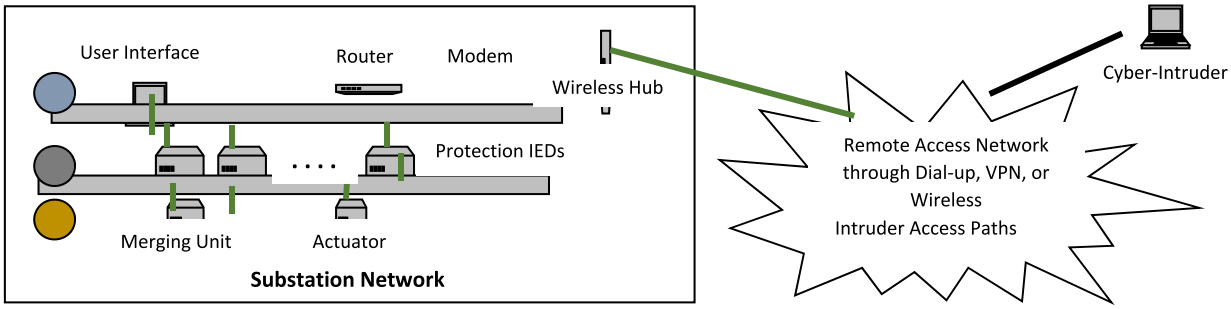


Fig. 11. Remote CPS attack scenario.

Table 3
On the anomaly detection algorithm.

To/From control network or user interfaces	Attempts of cyber-intruders
Control	Attempt to connect to IED
Setting	Acquire login information
Measurement	Successful log in to IED
Data log	Gain control of circuit breaker
Test/Diagnosis	Change setting to factory status

Along with the algorithm, status bits are used to aid in the detection of certain intruder based irregularities. Below, a row vector is presented to illustrate the weight given to the different bits.

$$\pi_{(1\times k)} = (1 \quad \alpha\pi^{a}_{(T\times L)} \quad \beta\pi^{fs}_{(T\times M)} \quad \delta\pi^{cs}_{(T\times N)} \quad \varepsilon\pi^{o}_{(T\times O)}) \tag{18}$$

π^a is the discovery of intrusion attempts on computers or IEDs, π^{fs} is a modification made to a file system, π^{cs} is a modification to an important IED setting, and π^o is a modification made to switches. The weighting factors are α, β, δ, and ε, and L, M, N, and O are the sizes of the components, and T is the number of anomalies in a given amount of time. The resulting matrix is then ranked using the equations below in order to establish whether an intrusion event has taken place at the given substation:

$$\prod = \frac{\pi}{\|\pi\|\,2}, \qquad \zeta = \operatorname{rank}\left(\prod\right) - 1 \tag{19}$$

$\prod$ is the normalized vector of π, and ζ is the index determined by the rank of $\prod$ for the substation. If the index, ζ, is non-zero then an anomaly event could have occurred, and the substation is then put on the list of possible attacks to be further investigated. A malicious attack on a substation can be incredibly detrimental, but if an intrusion occurs in critical or multiple substations, the potential outcome can be even more disastrous. In order to detect and diminish such attacks, we should take some precautions, such as generating an inventory of substations in which de-energizing components would result in complete voltage collapse, ranking suspected intrusion events made to multiple substations in a short timeframe, and designing a system to alert power workers when disturbances occur are accomplished. In addition, an impact factor, γ, is calculated using the following equation:

$$\gamma = \left(\frac{P_{LOL}}{P_{Total}}\right)^{L-1} \tag{20}$$

P_{LOL} is power flow where Loss of Load occurs, P_{Total} is total power flow, and L is the loading level of the substation. Using this impact factor, the vulnerability of substations is estimated and evaluated so that the least potential damage is realized when an intrusion transpires.

The anomaly detection algorithm presented has been thoroughly tested and analyzed using the well-established IEEE 118-bus system model [109] in order to establish its credibility and ability to preclude a malicious attack on substations. As expected, the algorithm effectively pinpoints multiple simultaneous logon attempts, impact factors, efforts to manipulate critical files in a detrimental way, and attacks made on multiple and/or critical substations. However, to efficiently implement such a security effort more research has to be completed in the area of application to already established software and framework currently within the substations.

4.3. Dynamic security model

In [94] mathematical models called structure-preserving power network models are used at the transmission level to describe dynamic swing equation for the generator rotor dynamics and the algebraic load-flow equation for the power flows through the network buses. Most security analysis today is based on *static* estimation techniques for magnitudes at buses and voltage angles. This is because of the low bandwidth of communication channels for measurements to the control centers, the difficulty in finding and tuning an accurate dynamic model, and dynamic models being more difficult to use. However, it is critical to design an integrated modeling framework for *dynamic* systems exposed to cyber–physical attacks. Here we use a power system security example to explain the dynamic CPS security concept [110].

Attack model: The network studied in [111] includes n generators $\{g_1 \ldots g_n\}$, n generator terminal buses $\{b_1 \ldots b_n\}$, and m load buses $\{b_{n+1} \ldots b_{n+m}\}$. The interconnection structure is encoded by a connected admittance-weighted graph. The Laplacian matrix of this graph is $\begin{bmatrix} \mathcal{L}_{gg} & \mathcal{L}_{g1} \\ \mathcal{L}_{1g} & \mathcal{L}_{11} \end{bmatrix} \in \mathbb{R}^{(2n+m)\times(2n+m)}$. The differential–algebraic model of the power network is provided by the linear continuous-time descriptor system shown here.

$$E\dot{x}(t) = Ax(t) + P(t). \tag{21}$$

Here, $x = [\delta^\top \omega^\top \theta^\top]^\top \in \mathbb{R}^{2n+m}$ is made up of the frequencies $\omega \in \mathbb{R}^n$, generator rotor angles $\delta \in \mathbb{R}^n$, and bus voltage angles $\theta \in \mathbb{R}^m$. The input $P(T)$ is the acknowledged changes in mechanical input power to the generators or real power demand at the loads.

Let $y(t) = Cx(t)$ represent the p-dimensional measurements vector and let $C \in \mathbb{R}^{p\times n}$ be the output matrix. Disturbances that show up in the measurements vector after being integrated

through the network dynamics are called state attacks. Disturbances that corrupt the measurements directly are called output attacks. The network dynamics in the existence of a cyber–physical attack can be written as shown below:

$$E\dot{x}(t) = Ax(t) + \begin{bmatrix} F & 0 \end{bmatrix} \begin{bmatrix} f(t) \\ \ell(t) \end{bmatrix} \tag{22}$$

$$y(t) = Cx(t) + \begin{bmatrix} 0 & L \end{bmatrix} \begin{bmatrix} f(t) \\ \ell(t) \end{bmatrix} \tag{23}$$

The inputs $\ell(t)$ and $f(t)$ are the output and state attacks respectively. Throughout this section, $T \subseteq \mathbb{R}_{\geq 0}$. An attack can be called undetectable if there is an attack set K that has an initial condition $x_1,\ x_2 \in \mathbb{R}^{2n+m}$, and an attack mode $u_K(t)$ so that, for all $t \in T$, $y(x_1, u_k, t) = y(x_2, t)$. An attack can be called unidentifiable if there is an attack set R and an attack set K, with $R \neq K$ and $|R| \leq |K|$, initial conditions $x_K,\ x_R \in \mathbb{R}^{2n+m}$, and attack modes $u_K(t), u_R(t)$ are so that for all $t \in T$, $y(x_K, u_k, t) = y(x_R, u_R, t)$.

Let $L = [L_\delta^\top L_\omega^\top L_\theta^\top]^\top$, $F = [F_\delta^\top F_\omega^\top F_\theta^\top]^\top$, and $C = \begin{bmatrix} C_\delta & C_\omega & C_\theta \end{bmatrix}$. The bus voltage angles $\theta(t)$ in (3) can be conveyed via the state attack mode $f(t)$ and the generator rotor angles $\delta(t)$ as shown here

$$\theta(t) = -\mathcal{L}_{11}^{-1}\mathcal{L}_{1g}\delta(t) - \mathcal{L}_{11}{}^{-1}F_\theta^\top f(t). \tag{24}$$

The elimination of the algebraic variables $\theta(t)$ in (3) points to the state space system:

$$\begin{bmatrix} \dot{\delta} \\ \dot{\omega} \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & I \\ -M^{-1}(\mathcal{L}_{gg} - \mathcal{L}_{g1} - \mathcal{L}_{11}{}^{-1}\mathcal{L}_{1g}) & -M^{-1}D_g \end{bmatrix}}_{\tilde{A}} \begin{bmatrix} \delta \\ \omega \end{bmatrix} + \underbrace{\begin{bmatrix} F_\delta & 0 \\ M^{-1}F_\omega - M^{-1}\mathcal{L}_{g1}\mathcal{L}_{11}^{-1}F_\theta & 0 \end{bmatrix}}_{\tilde{B}} u, \tag{25}$$

$$y(t) = \underbrace{[C_\delta - C_\theta\mathcal{L}_{1g}\mathcal{L}_{11}^{-1} \quad C_\omega]}_{\tilde{C}} \begin{bmatrix} \delta \\ \omega \end{bmatrix} + \underbrace{\begin{bmatrix} -C_\theta\mathcal{L}_{11}^{-1}F_\theta & L \end{bmatrix}}_{\tilde{D}} u.$$

The reduction of the passive nodes is called the Kron reduction. For the power network descriptor system (3), the attack set K is identifiable (resp. detectable) if and only if it is identifiable (resp. detectable) for the associated Kron-reduced system. Here we differentiate between two types of attack detectors: (1) A Static Detector is an algorithm that utilizes measurements from the network to check for the attacks at predefined instants of time, and without manipulating any relation between measurements taken at different times. Following are two theorems that define how an attack set is undetectable and unidentifiable for a Static Detector. (2) Dynamic Detectors check for attacks at all times $t \in \mathbb{R}_{\geq 0}$. Dynamic Detectors are harder to deceive than Static Detector, but with this comes more complications. The following residual filter is presented to answer the attack detection problem: Assume that the attack set is detectable and that the network initial state $x(0)$ is known. Consider the detection filter

$$\dot{\omega}(t) = \left(\tilde{A} + G\tilde{C}\right)\omega(t) - Gy(t) \tag{26}$$

$$r(t) = \tilde{C}\omega(t) - y(t) \tag{27}$$

where $\omega(0) = x(0)$, and $G \in \mathbb{R}^{2n\times p}$ is such that $\tilde{A} + G\tilde{C}$ is a Hurwitz matrix. The $r(t) = 0$ at all times $t \in \mathbb{R}_{\geq 0}$ if and only if $u(t) = 0$ at all times $t \in \mathbb{R}_{\geq 0}$. It has successfully demonstrated that a dynamic detection and identification method utilizes the network dynamics while requiring possibly fewer measurements.

In summary, *dynamic* detection and identification can be extremely useful to prevent attacks [112–115]. Static detection and identification has been used for several years for many logical purposes. Static detection processes are incapable to identify any attack disturbing the dynamics, and that attacks corrupting the measurements can be designed to be undetectable without difficulty. Using a dynamic algorithm will allow the system to use continuous time, instead of predefined instances.

5. Systematicness

In this section we will explain how we can integrate all cyber and physical components together into a *systematic* CPS. We will explain some important principles in systematic CPS design.

5.1. Systematic CPS design: distributed controller model

Here we illustrate the importance of distributed controller model in systematic CPS design. As we mentioned before, a systematic CPS architecture can be formed as a sensor–controller network, i.e., a networked control (NC) model [116]. Wireless communications have often been used in large-scale, complex CPS due to the difficulty of deploying cables between all devices. A stable NC model should be able to overcome the noise or errors in the sensor inputs [117], in other words, it can still correctly generate next-step (time $T + 1$) control commands based on current (time T) sensor status, see Fig. 16.

To overcome sensor data errors, a controller should predict its next state when true inputs are not received [118]. The reason of using controller's state *prediction* instead of packet retransmissions is motivated from the following fact: A controller has strict decision-making "rounds", which means that a delayed message at time T will not be useful any more for control decision calculation at time $T + 1$.

On the other hand, the controller-to-controller (C–C) coordination protocol should be designed to implement *multi-controller co-decisions*. In many CPS applications, we cannot simply reply on a single controller's state prediction. As shown in Fig. 16, at time T multiple controllers need to coordinate with each other to deduce a new state at $T + 1$. To coordinate multiple controllers, the traditional approach is to request all controllers to send data to a central server, which runs next-state prediction for all controllers and then sends prediction result to each individual controller. This approach suffers from two shortcomings: First, there is the single-point-failure issue, and the server burdens a high calculation load. Second, it is not realistic to ask all controllers to use hop-by-hop, high-loss-rate wireless links to send data to the server for central processing [119–121].

A good solution to the above multi-controller co-decision issue under wireless link errors, is to use localized, in-network co-prediction, which means that a set of distributed controllers use C–C coordination protocol to co-predict control state parameters to make a co-decision during $T \rightarrow T + 1$ state transition (Fig. 12). The control state update is determined from the following control theory equations [122]:

$$X_n(T + 1) = A_nX_n(T) + B_nW(T) + C_nU(T) \tag{28}$$

$$Y_n(T + 1) = D_nX_n(T) \tag{29}$$

where $X_n(T)$ is the system state, $W_n(T)$ is the disturbance acting on the CPS (such as packet loss and delay), $U_n(T)$ is the control force, and $Y_n(T)$ is the variables to be controlled. To design C–C coordination protocols for in-network control state prediction, we could use a promising state prediction method called Sequential Monte Carlo (also called particle filters). The motivation for using particle filters is that particle filters are well-suited to accommodate the types of uncertainty that arise in our distributed control scenario. Each *particle* can be thought of as an entire

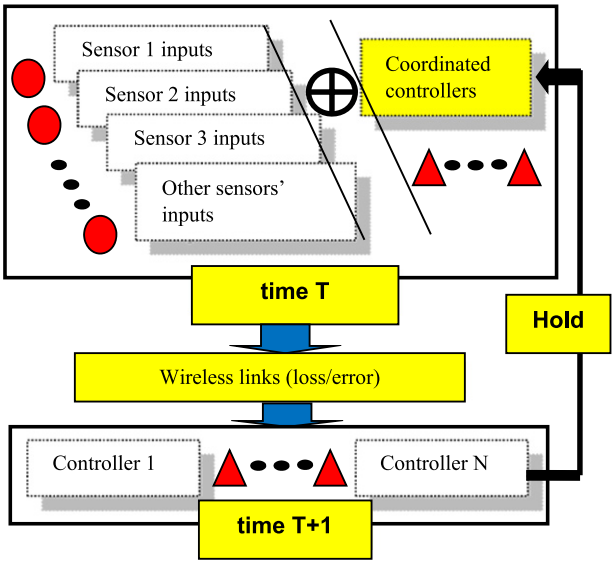


Fig. 12. Predictive CPS control model.

history or trajectory. This property of particle filters is not owned in Kalman filters [123]. However, we need to extend traditional, centralized Monte Carlo model to deal with in-network distributed control.

Here we first briefly explain the traditional *centralized* Monte Carlo model. Let us consider the real-time next state prediction for non-Gaussian MG control signals. The unobserved (i.e., hidden) global state $\{x_t; t \in N\}$ is modeled as a Markov process with initial distribution $p(x_0)$ and transition probability $p(x_t|x_{t-1})$. The observations $\{y_t; t \in N^*\}$ are assumed to be conditionally independent in time given the process x_t and of marginal distribution $p(y_t|x_t)$. We denote system state up to time t as $x_{0:t} \triangleq \{x_0, \ldots, x_t\}$ and observations up to time t as $\{y_t; t \in N^*\}$. The measurements y_t are recorded by K controllers, and we use y_t^k to denote the subset of observations made by the kth controller. Our goal is to predict (in real-time) the posterior distribution $p(x_{0:t}|y_{1:t})$ of $y_{1:t} \triangleq \{y_1, \ldots, y_t\}$.

We call state trajectories as particles. There is an importance weight associated with each *particle*; at a given time instant, this weight is the representative of how well the state trajectory conforms to model dynamics and describes the set of observations, relative to the other particles.

Traditional, centralized state prediction assumes that there exists a center in the entire system that accepts all sensors/controllers' inputs and controls all devices. For such centralized Monte Carlo model, we can follow generic steps [124] to estimate the posterior distribution as follows [125]: *Step* 1 (particle initialization): Each particle (total number: N) is sampled from the initial distribution. $x_0^{(i)} \sim p(x_0)$, and every importance weight is initialized to $\omega_0^{(i)} \sim 1/N$. *Step* 2 (importance sampling): For each $I = 1, 2, \ldots, N$, $\tilde{x}_0^{(i)}$ is sampled from an importance distribution $\pi(x_t|x_{0:t-1}^{(i)}, y_{1:t})$, which may be any distribution. *Step* 3 (selection): N particles $\{x_{0:t}^{(i)}; i = 1, \ldots, N\}$ are formed by sampling with replacement from the set $\{\tilde{x}_{0:t}^{(i)}; i = 1, \ldots, N\}$ where the probability of sampling the i-th trajectory is $\bar{\omega}_t^{(i)}$.

The above centralized Monte Carlo scheme needs to be extended to *distributed* multi-controller prediction case. Each controller needs to update its particle approximation to the posterior distributions when new data become available at time t, and it needs to calculate, for each particle $i = 1, \ldots, N$, the likelihood function $p(y_t|x_t^{(i)})$. In in-network prediction, the dissemination of quantized data through the network can generate an unacceptable communication overhead among wireless controllers. We can especially use the following two enhanced design:

(1) Parameterized data exchange: instead of sending raw data, we extract some coefficients from likelihood function factorization as follows: $p(y_t|x_t) = \Pi_{k=1}^K p(y_t^k|x_t)$, and each factor $p(y_t^k|x_t)$ can be described approximately by a parametric model $F_k(x_t; \theta_t^k)$. The model parameters θ_t^k are estimated from training data pairs $\{(p(x_t^{(i)}, y_t^k|x_t^{(i)})); i = 1, \ldots, N\}$, and the parameters are disseminated.
(2) Network aggregation: Instead of disseminating the entire parameter set $\{\theta_t^k; k = 1, \ldots, K\}$ through the network, we can send out a reduced set of model parameters, which we denote as ϕ_t that has a dimension substantially less than K. The parameter set reduction occurs in each tree parent node.

The in-network prediction protocols need to perform the following operations: First, each controller needs to sample N particles from $p(x_0)$, and each controller's importance distribution should not depend on other controllers' measurements. Each controller calculates the value of the likelihood factor for each particle of the current observation. The quantized result is sent to next controller in the routing path. Second, each controller extends its training data based on its received message from the last controller. The algorithm should attempt to more and more fit the global likelihood $p(y_t|x_t) = \prod_{k=1}^K p(y_t^k|x_t)$. Third, the final controller propagates back its estimated parameters along the reverse routing path. Each controller then determines its importance weights.

5.2. Systematic CPS design: sensor and controller coordination

Another important aspect to achieve a systematic CPS design is to build a tightly coupled sensor–controller coordination model. In CPS we need a set of efficient communication schemes among sensors and controllers (i.e., actuators). For example, in a water distribution network, reliable water filtration and distribution systems are in high demand. When aided with software and hardware intelligence, leaks can be detected and in the case of contaminated water, it can be controlled and localized. Sensors are used to monitor the physical elements and reports the data collected to the cyber system. Valves, pipes, and reservoirs are used along with software and hardware components to achieve a water distribution system that can filter and aid in distributing treated fresh water to a population [126].

In the water distribution example, to collect the necessary information to maintain healthy drinking water, RFID-based sensors are located within a water pipes infrastructure. These sensors are connected to access points that lead to the internet. The cyber data server can then utilize the data collected. The algorithms on the cyber data server then operate through hardware controllers on the findings to manage the quality and quantity of water that is produced. In [127] PipeSense was developed. It is an in-pipe water monitoring system that also uses RFID-based sensors. Some parameters that are measured with the sensors include water pressure, chemical composition and volume of the water. These measurements can be taken at various places within the pipe. PipeSense uses acoustic signals that are susceptible to noise to detect any leaks within a pipe. As one might predict, this process is very prone to false alarms. The intention is to create a system that monitors a real time water quality sensing mechanism that will determine the changes occurring within the real time water distribution network. Their system encompasses a large amount of inexpensive nodes that are able to communicate with each other. This benefits the overall system making it more efficient and reducing the number of possible false alarms. The CPS

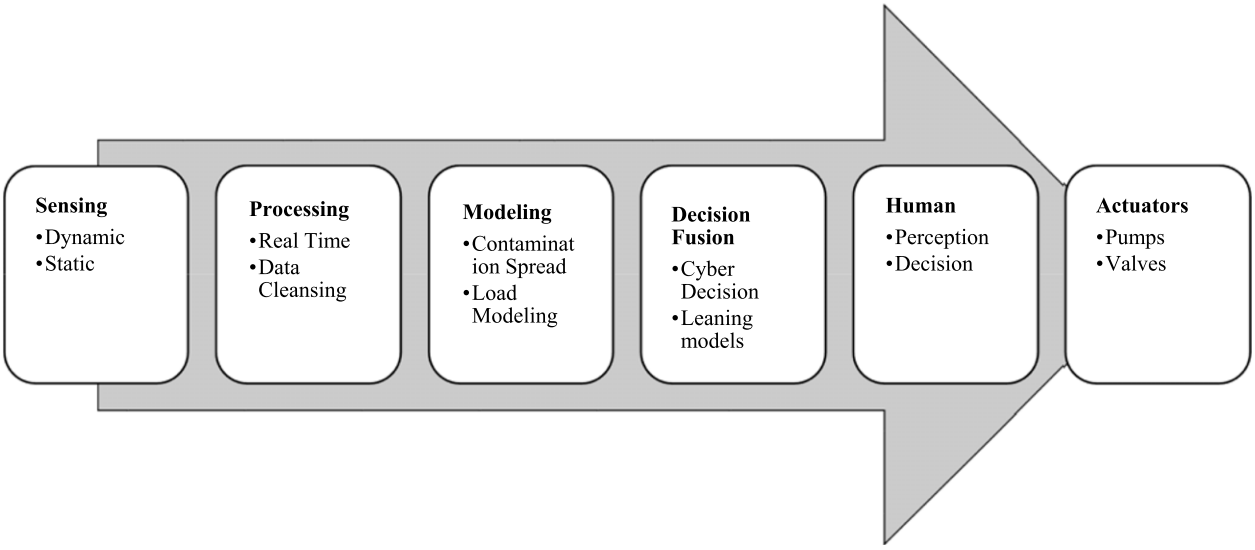


Fig. 13. Six levels in CPS framework [127].

is driven by events that take place. The human centric framework architecture will introduce a human as the means of monitoring the water within the application. Six levels are located within the CPS framework. These are illustrated in Fig. 13.

The first tier is the sensing tier. It is made up of many sensors that can detect temperatures, pressures, pollution, and among others pH levels. They can be classified as either dynamic sensors or static sensors. Dynamic sensors monitor within the pipe through variously placed nodes and it also identifies the location of the nodes. Static sensors can monitor actuators functionality and temperatures within the pipe. Information collected by either type of sensor is fully analyzed at the server level. The next tier is naturally the processing tier. The information is only partially cleansed when it arrives at this stage. After receiving the real time information from the sensors, it is fully and thoroughly cleansed. It can also be stored to review at a later date. Thirdly, the modeling tier detects the likely hood of a spreading of contaminated elements can be predicted along with different patterns that may occur. The Decision Fusion tier is next. During this stage, the decisions within the cyber systems are made depending on the models that have been taught or previously programmed according to the situations. However, these decisions are not acted upon until a later step.

The Human tier incorporates the input of a human along with the information being decided upon. This combination makes up the base for the human centric CPS framework. A human agent is able to omit the decisions made in the previous stage and override with a new action. This is helpful to prevent false alarms. These instances are recorded by the cyber system and used to alter the training models over time in an attempt to possibly reduce the amount of false alarms. The next and last tier is the Actuator tier. This is comprised of pumps and valves. The valves can either be automatic or manually controlled. They can be used to stop, start, or pause a process. Also, they can be used to alter the pressure or isolate a certain section of pipe. This may be necessary in the case of a contamination being detected or a leaking pipe. The suggestions to make the changes to a pump or valve are sent to human operators or carried out immediately if operating automatically. The sensing tier then plays the most important step of repeating and analyzing the result of its previous data collected.

In the future, this process can be improved by incorporating a multi-interface data service for the human tier so that the humans can easily make the correct actions occur. Also, this data has the possibility of utilizing a wireless handheld device for processing and decision making. Doing this through Wi-Fi and Bluetooth are being explored in [127]. Ultimately, a CPS framework would positively aid the effort of improving the quality of current water distribution systems.

5.3. Systematic CPS design: quality of system (QoS) issues

From network viewpoint, a systematic CPS design should consider quality of service (QoS) issues. CPS infrastructure typically is built from WSAN (wireless sensor and actuator network). Any network has QoS issues. Resource constraints apply to both actuators and sensors. Sensors are normally low-cost and offer restricted data processing, battery energy, and memory. The actuators have stronger computation capabilities than sensors along with more energy. Although used together, sensors and actuators are greatly different from each other including their capabilities and what they are used for. Another feature of WSAN is dynamic network topology. There are times where new sensor and/or actuator nodes may need to be added or removed, and some could even die due to drained battery energy. Different applications will have different QoS requirements. For instance, a system that regulates the temperature in an office building from the air conditioning unit may allow some packet loss and long delays but this would not be acceptable for systems that are intended for safety-critical systems.

In terms of WSAN QoS, some areas of interest that are being researched are service-oriented architecture, QOS-aware communication protocols, resource self-management, and QoS-aware power management. It is very important for service differentiation to be supported by the communication protocol when looking at QoS. A CPS may have very different applications with various QoS requirements. The new design will have to observe the service requirement associated with each application so that a service adapted to each particular application will be provided. Cross-layer design has shown to be very useful in making network performance. It is also a good idea to incorporate cross-layer design into QoS-aware network communication protocol for CPS.

Delay/jitter has also been a big issue in QoS support [128]. The difference in time of sending packets to those being received is called a delay. The jitter is the delay difference between neighboring packet arrival events. The jitter can be reduced by holding received packets within a buffer for a certain period of time before they are accessed. That specified amount of time is

referred to as the playback delay. A new approach using the one-way delay variation has been taken to improve the possible length of the delay.

CPSs have been created over time within network control systems (NCSs) [121]. NCSs function in real time and must deal with occurrences of delays, delay jitters, and the loss of packets. The quality of the system is affected greatly by these events. The delays can be sudden and cause a possible prediction of the received time to be incorrect. This is when the previously mentioned playback delay is useful. The packets that are received are held for a period of time before they can be accessed. This delay provides some packets, in cases where errors were present, more time to arrive. If it is received after the processing time has passed, it is considered to be a lost packet and a jitter is present where the missing packet should be. Buffers at the physical system send control signals at predictable times in an attempt to soften the jitter. The correct amount of time that the packets are held is very important. If it is not lengthy enough, it is possible to lose more packets. If the time is extended, there is a delay is processing time and weakens the quality of the system.

A new way to predict more accurate playback delay times are to decompose the variations in the round trip times (RTTs). There are two components of this. First is the forward path that is the one way delay variation of the physical system to the controller. For this review, we will call it f_{pc}. The other is the reverse path of the controller to the physical system, or r_{cp}. The controller has an advantage in the forward path because it can accurately predict the f_{pc} time. The one-way delay variation (*OWD*) is extracted using the round trip times (RTTs). Much research was done on forward and reverse one-way delay variations. The dependency of the forward and reversed variations was also studied. The recently developed method of predicting the playback delay value is more advantageous in that it can shrink the delay time window by using known forward RTTs and approximating reverse RTTs. It examines and produces a more acceptable forward RTT than previously used methods.

The newest method of playback delay prediction is as follows [129,130]. If a sensor performs a reading y and it is received at the controller after a time t, y can either arrive, be lost, or late. If it does arrive at the controller, it is used to control an action, u. This signal of control can be applied at some unknown time due to delay jitters or be lost. This proves the physical system to then act on a function of u. If the signal u arrives, it can be held within the play back buffer at a predictable $t + r$ time. If it does not arrive before $t + r$ expires, the signal is considered lost. The factor of r must be a close approximation of the round trip time (RTT). If it is too large or too small, the physical system's actions can in no way be predicted. r is found at the controller because the controller can then in turn produce the needed control signals that can shift the state of the physical system. To find the approximate value based on the RTT and the *OWD*, or one way delay, the following Eq. (1) was used.

$$RTT_{pcp}(i) = RTT_{pcp}(i-1) + \hat{RTT}_{pcp}(i) \tag{30}$$

$RTT_{pcp}(i-1)$ represents the round trip time of the $(i-1)$th packet that is sent from the physical system to the controller and back. $\hat{RTT}_{pcp}(i)$ represents the deviation of the previous round trip time of the $(i-1)$th packet with respect to $RTT_{pcp}(i-1)$. Fig. 14 displays each step in which the network control system sends and receives packets from the physical system to the controller. It can be seen at k_i in Fig. 18 that the delay r is predicted at the controller side because it will use that value to create the u_i value. By observing the figure one can also deduce that the controller is able to know the exact value of both $RTT_{pcp}(i-1)$ and $f_{pc}(i)$. The controller uses these known values to then calculate the only unknown value of r_i. This will then produce the value of $r_{cp}(i)$.

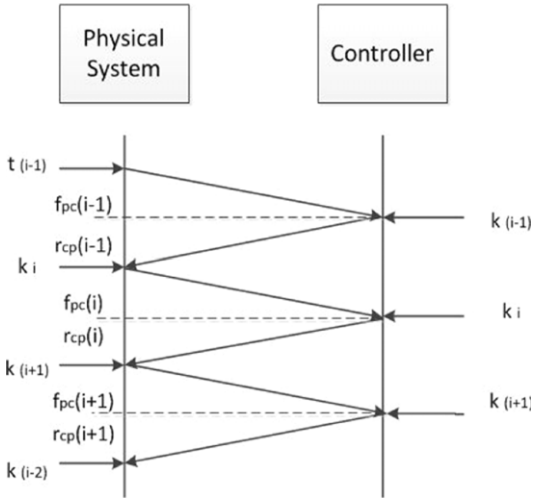


Fig. 14. Packet sending/receiving schedule.

In this method, $f_{pc}(i)$ can be predicted from the controller. This can be used by the controller to predict the play back delay. This will in turn decrease the unpredictability of the play back delay time.

6. Resilient CPS design: case studies

In this section, we will use two of our CPS projects to explain the process of resilient CPS design as well as the cyber–physical coupling principles. The first case study is on the integration of virtual reality and the robot for rehabilitation training. It is a typical cyber–physical coupling system due to the interactions of medical sensors, actuators, and virtual world interactions. The second case study is on the design of implantable medical device—pacemaker. It is also a typical CPS since the cyber parts (heart beat detection sensors) collect data which is used by the controller (electrical pulse wire) to control the beat patterns of the heart (physical object). It has the security considerations—the attack-resilient wireless power charge circuit, as well as other resilient features such as energy-efficient sensor sampling, noise-resistant pattern recognition, etc.

6.1. Case study 1: CPS design for virtual rehabilitation

Efficient rehab training could greatly help to recover functional body *coordination and flexibility* (C&F) capabilities. Efficient rehab training is especially important to the prevention of disabilities for stroke survivors since stroke is the leading cause of disability among adults. Other neuro-disorder diseases such as Parkinson's disease, cerebral palsy, etc., are also accompanied by disabilities. Therefore, there is an urgent need to investigate new, intelligent rehab methods to efficiently restore C&F of people with various disabilities.

Importance of robot-aided rehab training: Today many in-clinic rehab training methods are based on labor-intensive assistance from clinicians such as physical/occupational therapists (PTs/OTs). Because the patient needs to practice various hazard-based training (e.g., intentionally using slippery surface to walk) [131], it is difficult and dangerous for a clinician to hold the patient all the time to protect them from training hazards. To overcome such an issue, this project will use a robot-aided rehab training system, the KineAssist [132], to achieve complex training tasks within the context of hazard environments, such as perturbation recovery training and gait training in hazardous conditions [133].

Importance of virtual reality (VR) based rehab training: VR-based rehab system allows the trainee to recover his or her body C&F

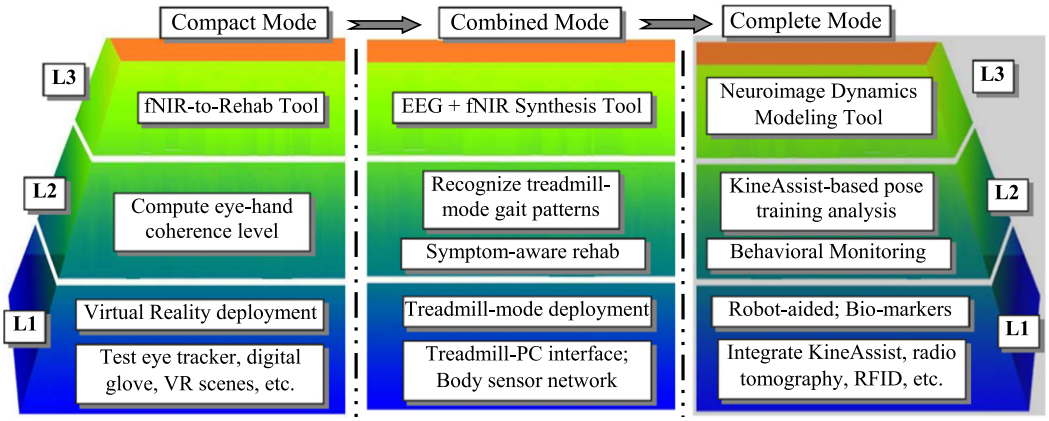


Fig. 15. Hierarchical, incremental CRI development (L1: Physical Layer; L2: Computation Layer; L3: Cognition Layer).

through various virtual scenes without the need of going through complex real environments. The digital signals collected from devices, including the neuroimages from the fNIR/EEG devices, trajectories from the digital glove, eye focus data from the eye tracker, and other signals, can be processed to *quantitatively* analyze the rehab training effects. Moreover, this project will extend the VR system to an *augmented* VR (AVR) platform, which can embed a reconstructed 3D body motion graphics into the VR scenes. The AVR makes the trainee more interactive with the scenes.

The goal of our CPS design is to establish a new platform to support the research of computational and cognitive rehabilitation (briefly called *rehab*) for disability recovery applications. Our CPS follows an innovative development methodology that consists of two aspects (see Fig. 19): (1) First, it uses a *hierarchical* architecture with three design layers: in layer 1 (L1)—*physical layer*, we focus on the hardware device debugging and their interface design (such as treadmill–computer interface); in layer 2 (L2)—*computation layer*, we will design software tools to support the above mentioned *computational* rehab training (such as eye–hand coherence level computation); in layer 3 (L3)—*cognition layer*, we design software tools to support the above mentioned *cognitive* rehab training (such as neuroimage-to-rehab mapping). Such a 3-layer design simplifies the CRI management. (2) Second, this platform follows an *incremental* development plan with 3 setup modes: *compact, combined, and complete modes*. The compact mode has the simplest setup since it mainly consists of virtual reality units; the combined mode adds programmable treadmill as well as health monitoring system (via medical sensors); and the complete mode builds a comprehensive platform with robot-aided virtual rehab system.

In the *complete mode*, the CPS development has the integration of the co-robot, AVR, treadmill, and some bio-markers (such as gait sensors) (Fig. 15). It has been found that body weight supported treadmill training (BWSTT) is highly effective in improving locomotors flexibility and speed after stroke [134]. Therefore, we propose to use a co-robot, KineAssist from HDT Inc. [102], to support intelligent body assistance in disability recovery. The KineAssist is not just a body holder. Instead, it can provide a user-intent-based smart response. It moves in response to the forces applied by the trainee to the pelvic mechanism. (Note that there are some force sensors deployed in the KineAssist's holding belts, see Fig. 16). Moreover, HDT's KineAssist has the programmable interface to the treadmill and other computing devices.

The proposed design has the intrinsic characteristics of a CPS, that is, it has the tight coupling of computational objects (including programmable sensors, VR gaming system, digital inputs such as digital glove) and physical objects including patient body and the robot (i.e., the integrated KineAssist and treadmill). As shown in Fig. 17, it has the following 3 cyber–physical interactions:

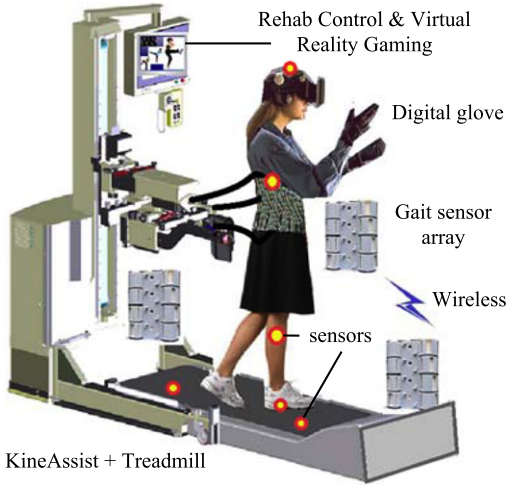


Fig. 16. Complete mode.

(1) Interaction between the intelligent sensors (cyber objects) and the robot (physical object): The sensing signal analysis module (❶) collects signals from medical, gait, and motion sensors and then uses machine learning algorithms to extract the intrinsic patterns such as gait anomaly level. Then the module ❶ will use those patterns to control the operations of the robot.
(2) Interaction between Head Mounted Display (HMD)/eye tracker/digital glove (cyber objects) and the patient body (physical object): The patient wears digital glove and HMD to interact with a virtual cyber world through VR interfacing software module (❷). Another cyber object—eye tracker, is used to capture the patient's eye pupil movement for the analysis of patient brain concentration level (if the patient has mind distractions, the eye movement will not synchronize with his/her hand movement).
(3) Interaction between VR virtual scenes (cyber object) and the robot (physical object): The VR gaming system can control the robot's behaviors. For example, if the patient has successfully achieved a low-speed walking training, the VR system can use the control module (❸) to speed up the belt.

Note that there also exist interactions between the two physical objects (i.e., patient and robot) as follows: (a) Patient → robot: the treadmill belt can move in response to the forces applied by the patient to the pelvic mechanism. Such user-intent-based robot control makes the platform achieve intelligent rehab-training. (b) Robot → patient: KineAssist uses a few bands with controllable holding strength in case that the patient loses body balance and falls down. This is achieved through signal analysis of the force

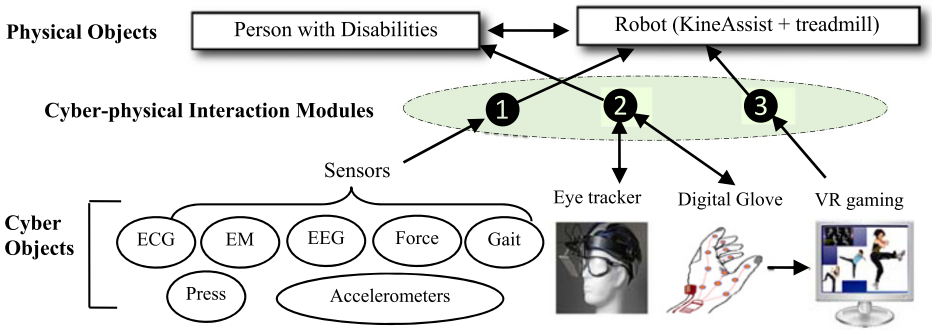


Fig. 17. Cyber–Physical Coupled Design (Here, ❶: Sensing Signal Analysis module; ❷: Virtual Reality Interfacing module; ❸: Gaming-output-triggered Control module).

sensor attached to the pelvic. Such a feature does not disturb the patient's natural gait pattern (for instance, it does not turn the body into a pendulum). Such a feature helps the patient to overcome the fear of falling down. Such fear could occur in traditional rehab-training.

Build software tool for automatic mind concentration computation: We have used the treasure hunt game, for mental concentration training. It has complex maze paths that require the trainee to have good coherence between her eye focus movement and her hand cursor trajectory. We can measure the mental concentration rehab progress based on the eye–hand coherence level. This CPS includes a software tool that can *quantitatively* measure how well the eye focus movement aligns with the hand trajectory. A challenging issue is that there are two important differences between eye tracker (ET) measurements and hand cursor positions: (1) *Spatial deviation*: Typically an ET can only provide 2D, coarse eye focus spots. On the other hand, the cursor's trajectory could be a clear 1D curve. (2) *Temporal deviation*: Human's eyes can reach a targeted position faster than hand movement. This is especially true for stroke patients without good hand flexibility.

To overcome the above issues, our software tool design uses an iterative, *spatial and temporal warping* (STW) scheme based on the enhancement of the *style translation* model [135], in order to find a *translation correspondence* (TC) for the alignment of ET data and hand trajectories (see Fig. 18). The sum of all deviations reflects the matching level between the TC positions (P_{TC}) and real hand positions (P_{hand}). If the patient has good eye–hand coherence level, we should have: $\Sigma\|P_{TC} - P_{hand}\| < D_{Th}$, here D_{Th} is a preset threshold. We use *three parameters* (S, O, W) to describe TC solution: the spatial warp is performed by a matrix operation: $US + O$, here U is a diagonal matrix from a ET data series (L_{ET}), S is a vector for spatial scaling, O is a vector for spatial offset. And W is a warping matrix for a monotonically increasing time warp. Given ET and hand trajectories: L_{ET} and L_{Hand}, the TC solution (S, O, W) should meet an objective function as follows:

$$f(S, O, W) = \|W(US + O) - L_{Hand}\|^2 + \|\alpha S\|^2 + \|\beta O\|^2. \quad (31)$$

Here the two constraints, $\|\alpha S\|^2$ *and* $\|\beta O\|^2$, are for a smooth spatial transform from L_{ET} to L_{Hand}. The solution to the above function should adopt an iterative optimization, with independent gradient optimization for spatial warping parameters (S, O) and temporal warping parameter W.

To help the researchers study the relationship between neuroimages and rehab training, in the cognition layer of compact mode CPS, we build *software tools for fNIR signal processing*: The fNIR patterns need to be extracted in order to observe the rehab training effects from neuro statistics variations in terms of UMC. We will build the software tools to achieve the following fNIR signal processing tasks: First, the tools can perform fNIR motion artifact cancellation based on Wiener filtering [136] that

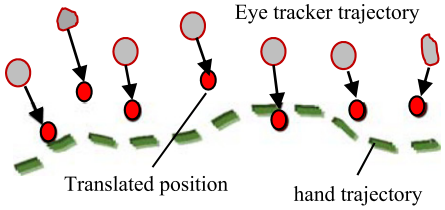


Fig. 18. Translation correspondence.

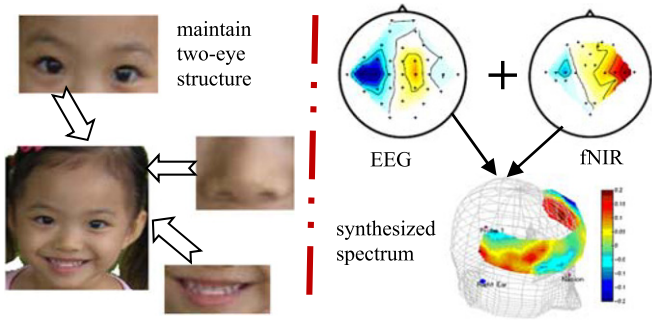


Fig. 19. Neuroimage Synthesis (1) an analogy; (2) EEG + fNIR.

has been verified to have better effects than popular method—adaptive filtering [137]. Second, we have found that the wavelet-based scheme with local holder exponent (LHE) can effectively capture the bio-signal patterns. We have used it to successfully extract the patterns from some neuro-images including EEG and fMRI [138]. We further enhance our previous scheme by using Wavelet Transform Modulus Maxima (WTMM) [77], and then build tools for fNIR pattern recognition. WTMM is an important approach in terms of detecting some pattern singularities. This is because that it can efficiently use "space-scale" partitioning to detect low-frequency (<100 kHz) fNIR image features:

$$Z(s, q) = \sum_{\Omega(s)} \left|W_{s,x0}(f)\right|^q, \quad \text{and} \quad Z(s, q) \propto s^{\tau(q)} \quad (32)$$

where $Z(s, q)$ is a partition function, $\Omega(s)$ is the set of all maxima at scale s, and $W(f)$ is the wavelet transform of a function f. It is convolution product of the image data with the scaled kernel.

Build *software tool for (EEG + fNIR) neuroimage synthesis*: A unique feature of this CPS is that it adopts two non-invasive, low-cost neuroimaging tools, i.e., EEG and fNIR, to achieve *cognition* activity measurements via the cognition layer tools. Other neuroimaging methods are either invasive (such as intracranial recordings), or require expensive machines (such as fMRI). EEG and fNIR can be worn simultaneously: EEG signals can be measured on the scalp surface through electrodes, while fNIR can be worn as a headband. More importantly, *they can*

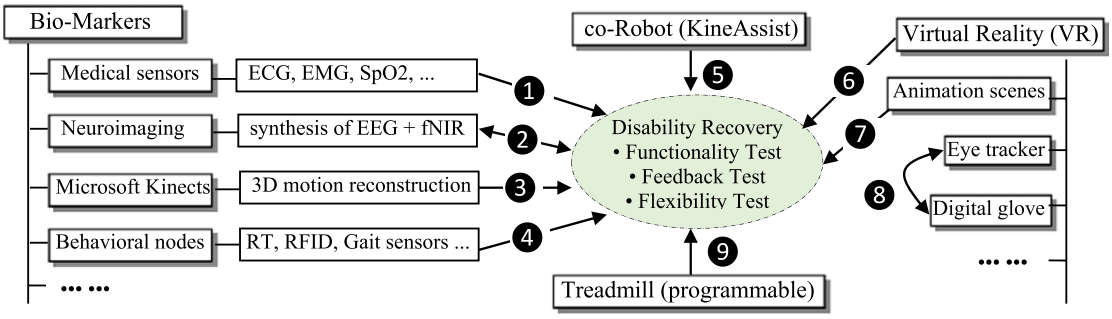


Fig. 20. Qualitative evaluation—3F test.

generate complementary imaging data: EEG can capture the event-related potentials (ERPs) [139] through the measurement of electrical amplitudes in different scalp positions. Especially, it has different features in each frequency band. fNIR uses lights in the near-infrared range (700–900 nm) to monitor changes in the concentrations of oxygenated or deoxygenated hemoglobin [140].

While using only EEG or only fNIR alone may not provide high-resolution, pattern-rich neuroimage, synthesizing them together into a new spectrum allows us to exploit their complementary patterns for a higher spatio-temporal neuroimage resolution. To more clearly see the advantage of (EEG + fNIR) synthesis, here we use an analogy from a face recognition task. As shown in Fig. 19, it is difficult to recognize a person's identity by just looking at the eyes' or the nose's image *alone*. However, by synthesizing all images through a geometry-preserved scheme (such as ensuring the nose is below two eyes), facial identity is accomplished more successfully. Therefore, by synthesizing EEG and fNIR through special methods such as manifold learning, we can generate a more comprehensive neurovascular dynamics model for each rehab training exercise. Then we can further build the neuroimage-to-rehab mapping model.

We build a software tool based on our created manifold-oriented Bayesian learning scheme [94] for the geometry-preserved synthesis of EEG and fNIR. To describe the geometric structure in each manifold to be fused, we use a weighted graph $G^{(k)}$, $k = 1, 2, \ldots, M$, to represent each manifold. In order to compute the distance matrix of the merged manifold, we first transform the *distance* between any two signal points in the kth manifold, denoted as D_{ij}, into a statistical probability P_{ij}, which means a transition probability from ith to jth point. After we obtain all manifolds' transition probability matrices, i.e., $P^{(1)}, P^{(2)}, \ldots, P^{(M)}$, we can adopt the α-*integration* concept [141], to fuse those M manifolds into one manifold (i.e., synthesized EEG and fNIR).

CPS evaluation: The *qualitative evaluation* (QLE) validates if the CPS meets the desired operational requirements in terms of operation correctness and sensitivity. QLE metrics may simply be "yes or no" answers (i.e., *qualitative*) instead of "how much" (i.e., *quantitative*). Particularly we propose to use a *3F* method (i.e., *Functionality, Feedback*, and *Flexibility* test) to perform a systematic QLE for our CPS (Fig. 20):

(1) Functionality test (in all positions of Fig. 24, i.e., from ❶ to ❾): It focuses on the basic functionalities of individual or systematic units. For example, in position ❶—Does the body area network timely transmit all sensors' data into a PDA? ❷—Can the manifold learning tool perform EEG + fNIR synthesis? ❽—Does the mental concentration tool recognize different eye–hand coherence levels? etc.

(2) Feedback test (❶, ❺, and ❻): This test aims to see how our CPS adaptively adjust its operations based on some feedback signals. It mainly include three aspects: In ❶—Can the rehab training immediately stop when any medical sensor reports health emergency? In ❺—Can the KineAssist adjust its holding strength based on the pelvic sensors' feedback signals? In ❻—Can the VR scene automatically increase the game complexity level when the trainee shows a better rehab training effect?

(3) Flexibility test (❷, ❸, and ❹): This test focuses on the CPS operation sensitivity such as: ❷—How flexible is the neuroimaging tool in terms of capturing spatial (i.e., in different scalp positions) neuro-activities even when the fNIR band is worn with unstable positions in the forehead? ❸—Can the Kinect-based AVR system clearly reconstruct the 3D body motions even when the trainee has fast move? ❹—How sensitive can the gait sensor network be in terms of detecting various abnormal gaits?

The *quantitative evaluation* (QTE) focus on metrics for the proposed rehab research platform. For instance, how accurately can the platform measure eye–hand coherence level through trajectory matching algorithms? how accurately can the system detect patient symptoms through medical sensor data analysis? Table 4 lists our *quantitative* evaluation plan with metrics and optimization units.

As an example of QTE, here we explain how we can test the capability of our CPS in terms of measuring treadmill-mode rehab efficiency. A complete subject test process for a stroke-related disability recovery includes *rehab protocol, rehab measures*, and *outcome analysis* as follows: (1) *Rehab protocol*: Subjects will be asked to participate in a 5-min warm up on the treadmill, followed by a 30-min treadmill exercise (walking) with rest periods, and then a 5-min cool down, with stretching. The subject will be walking with the body weight support provided by the KineAssist. (2) *Quantitative rehab measures*: The Fugl-Meyer scale will be used to assess sensorimotor stroke recovery. Its evaluative measures are divided into 5 domains: motor function, sensory function, balance, joint range of motion, and joint pain. Each domain contains items that are each scored on a 3-point ordinal scale (0 = cannot perform, 1 = performs partially, 2 = performs fully). (3) *Outcome analysis*: We will then compare the automatically computed rehab training effects with conventional manual rehab case. We will see if the proposed platform can achieve similar rehab progress reorganization accuracy compared to the manual rehab case.

6.2. Case study 2: analog-information-coupled implantable medical device (IMD)

An implanted computing platform (ICP) is a typical cyber–physical system (CPS) that involves tight interactions between the physical object and its implanted intelligent hardware. For example, in a structural health monitoring application, a fiber-optic strain gauge sensor could be embedded into the elastic layer of a bridge to detect bridge fracture. In this research, we target an important ICP, called implantable medical device (IMD), which is implanted in human body for both physical-to-cyber health

Table 4
Summary of evaluation metrics, methods, measures and optimization components.

Metrics	Methods	Measures	Optimization units
Eye–hand coherency	Subject tests; Algorithm analy.	Measure eye tracker's attention span angles, mouse cursor trajectories	Eye-tracker operation software; Time warping algorithms.
Symptom recognition accuracy	Subject tests; Bayesian/statistical models	Recognition accuracy of disease symptoms from the processing of medical sensor signals (ECG, etc.)	NMF algorithms; HMM state transition models; Data pre-processing (such as noise removal)
Gait anomaly detect. accuracy	Subject tests; Model analysis	Accuracy of detectable gait disorders; RFID/RT tracking accuracy	Gait sensor network protocols; NMF-based recognition models.

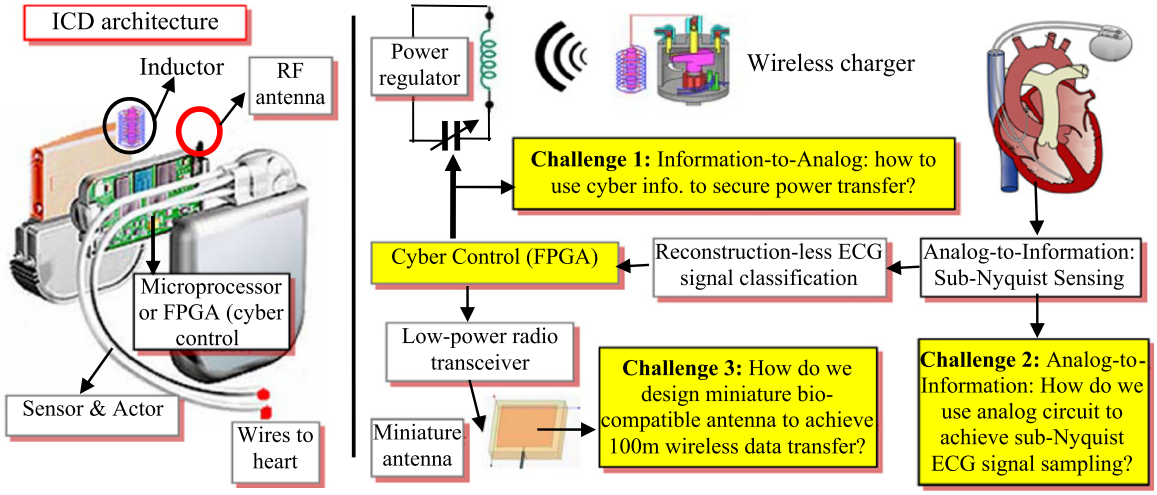


Fig. 21. The proposed three CPS research issues related to ICD design.

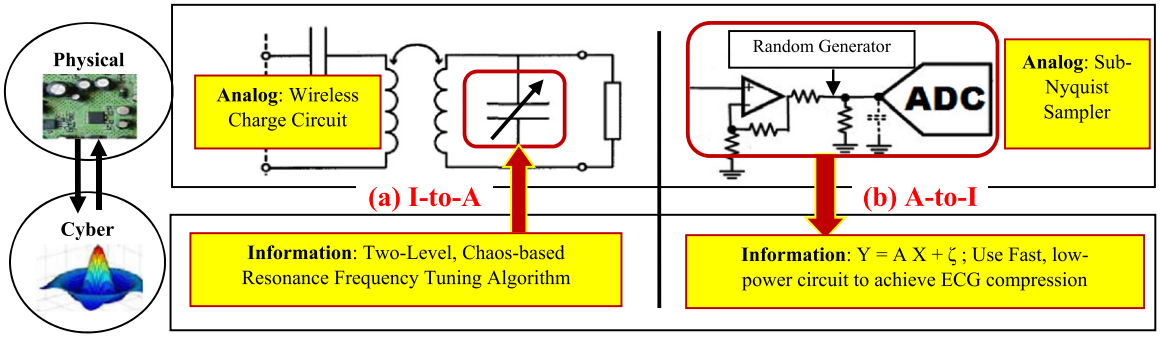


Fig. 22. Cyber–physical coupling: (a) Information-to-analog conversion; (b) Analog-to-information conversion.

sensing and cyber-to-physical organ control. Typical IMDs include pacemakers, neuro-stimulators, insulin pumps, and others. In this work, we specifically target the heart IMDs used in the cardiac CPS (C-CPS) to automatically treat heart diseases. The C-CPS mainly consists of an IMD such as pacemaker or implantable cardioverter defibrillator (ICD), and some medical sensors such as electrocardiogram (ECG) sensor. The difference is that pacemakers are more often temporary and generally designed to consistently correct bradycardia, while ICDs are often permanent safeguards against sudden abnormalities [142]. The basic ICD architecture is shown in Fig. 25.

Although wireless power charge has been studied for IMDs [143,144], and wireless data transfer to/from IMDs has also been achieved [145], there are still many unsolved issues such as the attack-vulnerable power charge procedure, very limited wireless communication range (existing IMDs typically first transmit signals to a cell phone that is only 1–3 m away [146]), and energy-consuming bio-signal processing algorithms, and so on. The goal of this design is to significantly improve the existing IMD architecture (with wireless power and data transfer capabilities) from a cyber–physical system (CPS) design perspective. Specifically, our CPS design is based on tight analog-information coupling. The following are the two challenging issues we target (Fig. 21):

(1) Information-to-analog conversion, i.e., use security algorithms (cyber part) to control wireless charge circuit (physical part): In order to make wireless charge operate in practical environments where power attacks could be easily launched, we propose to use confidential binary sequence information to control frequency switching analog circuit (Fig. 22(a)).
(2) Analog-to-information conversion: we propose to use low-power circuit (physical part) to achieve compressive signal sampling algorithm (cyber part). In order to minimize the required heart beat sensing samples (needed for correct heart disease classification), we propose to *use* an analog circuit (*instead of using slow, power-inefficient software implementation*) to generate Sub-Nyquist Sampling (SNS) information (Fig. 22(b)). Moreover, while traditional signal analysis schemes try to first recover the original bio-signals from SNS data, we propose to *directly* perform pattern analysis from SNS data. This saves lots of computation overhead and energy consumption.

Why information-to-analog control? Current wireless charge schemes assume that the external power charger works at a constant frequency and the ICD has an inductor that is set to the same frequency. The wireless energy transfer is assumed to occur in a safe, insulated environment. However, in reality an attacker who knows the ICD's coupling frequency, could use a customized self-resonant coil with high-resolution oscillation circuit to easily achieve power charge from a location close to the patient. Such a power charge attack has a series of serious consequences: (1) *Organ damage due to overheating*: The attacker could first reach strong coupling with the ICD coil and then use beyond-threshold electric current profile to transfer energy. The ICD could reach energy saturation in a very short time, which causes overheating and thus damages nearby organs. (2) *ICD dysfunction from voltage instability*: After reaching a resonant frequency with the ICD, an attacker could intentionally make the charger's electric currents and charge densities significantly vary in time. Such an unstable oscillator could cause the ICD's operation voltage to have an abnormal sinusoidal profile. As we know, an ICD needs a stable spatial average of electric current in order to control the heart beat patterns at an even pace. However, the unstable power charge makes it unable to control the electric pulses evenly. In order to overcome the above attacks, we need to solve a few issues: How do we build a robust ICD coil control scheme to prevent a malicious power charge? What is the secure way to fine-tune the ICD's inductor parameters to accurately accept power transfer signals from legal charger while blocking an attacker's charger?

To the best of our knowledge, there is no research conducted on the ICD power charge security under wireless inductor coupling. In our CPS security design, we propose to use confidential, *two-level* coupling coefficient adjustment **information** ('cyber') to control wireless charger **analog** circuit ('physical'): (Level 1) Coarse-tuning of ICD's resonance frequency based on three-dimensional (3-D) Chaotic Maps; and (Level 2) Fine-tuning of resonance frequency based on fast capacitance match.

(Level 1) Coarse-tuning of ICD Resonance Frequency via Chaotic Maps: The weakest point in existing ICD charging systems is the use of a preset, fixed resonance frequency. We thus propose to update the coupling coefficients (such as capacitors' values) in the analog charge circuit to achieve a time-varying resonance frequency switch. It has been validated from circuit design viewpoint that it is entirely feasible to adjust the ICD's shunt capacitance [142]. To make the frequency *switch sequence* confidential to attackers, we propose a *Chaotic Maps* (CM) based capacity control as shown in Fig. 23. The CM has been verified to have stronger unpredictability than conventional pseudo-random number generation schemes [147]. Specifically, we will adopt an extended CM, i.e., 3-D CM [148] to achieve a larger pseudo-random sequence space and can thus efficiently overcome guessing attacks. A 3-D CM sequence is extremely sensitive to initial parameters (i.e., *CM seeds*).

Unlike medical emergency cases, power charge typically occurs in a prepared environment (but attacks could still occur since we use *wireless* power charge). Therefore we make a reasonable assumption here (as in [149]): in the first very short time (1–3 s), an ICD and a charger could safely exchange a few initial parameters (such as CM seeds, the charger's energy density, etc.). However, if the first few seconds cannot be assumed to be safe, we could use a special RF signal pattern (called RF fingerprint) to achieve keyless, confidential data exchange between an ICD and a charger. (Such a data exchange will be achieved through our RF antenna transmission, Section 4.3).

Note that traditional 1-D CM has a key space of only 53 bits and is weak against adaptive parameter synchronization attack [148]. A 3-D CM overcomes such a shortcoming through

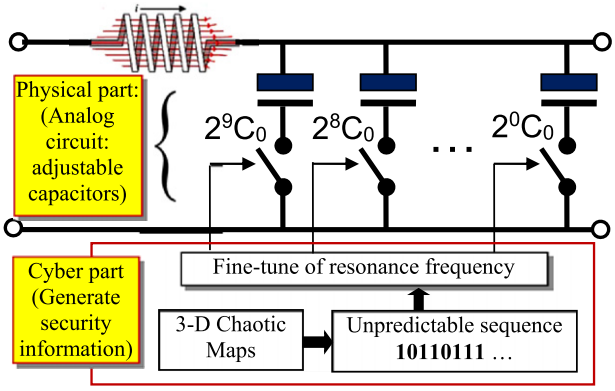


Fig. 23. Cyber–physical design for secret resonance fine-tuning.

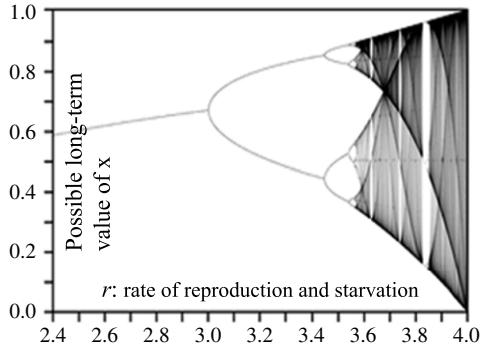


Fig. 24. Logistic map (bifurcation diagram).

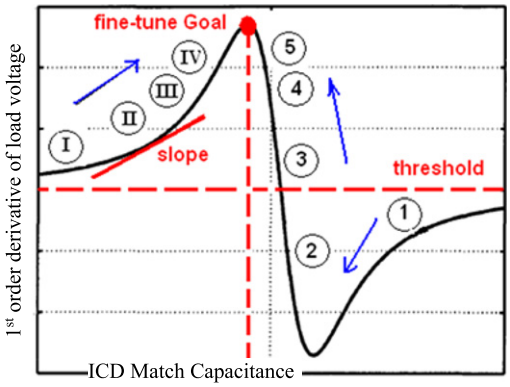


Fig. 25. Non-even peak approaching algorithm.

nonlinear transform of three *Logistic maps* (LMs)' outputs. A single LM function has the following format:

$$x_{n+1} = rx_n(1 - x_n), \quad 0 < x_n < 1,\ r > 0. \tag{33}$$

A bifurcation diagram (Fig. 24) reflects LM's behavior when r changes. When $r > 3.57$, the chaos (fractal) begins. The nonlinear transform of three LMs' output sequences (called 3-D CM) has been verified to be a binary Bernoulli distributed pseudorandom sequence [148], which means that any bit of a 3-D CM has 50% probability of being 1 or 0, and is statistically independent. Based on the 3-D CM sequence, an ICD will know which resonance frequency to be switched to in the next time interval. We further divide the CM sequence into small, 9-bit groups. Thus we have 2^9 values. Each is:

$$I = b_8 \cdot 2^8 + b_7 \cdot 2^7 + \cdots + b_0 \cdot 2^0. \tag{34}$$

Suppose the entire range is $R = [f_1, f_2] = [100\ \text{MHz}, 2\ \text{GHz}]$. We can divide R into $2^9 = 512$ different sub-ranges as follows:

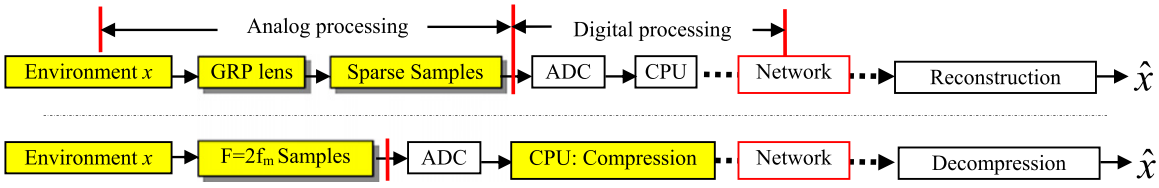


Fig. 26. (Top): GRP-based "analog compression"; (Bottom): conventional "digital compression".

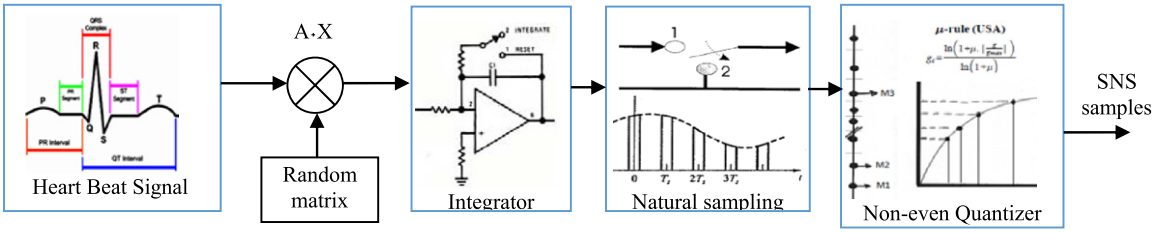


Fig. 27. Analog-to-information SNS circuit design principle.

[100 MHz, 103.72], [103.73, 107.45], and so on. However, in Fig. 6 we can see that we actually have used $2^{10} = 1024$ different levels of capacitor adjustments. This is because we will perform fine-tuning of frequency for each sub-range as follows.

(Level 2) Fine-tuning Process via Fast Capacitance Match: The above coarse-tuning of resonance frequency can only provide a coarse range $R = [f_1, f_2]$ to be used in next frequency adjustment. An accurate power transfer needs a fine-tuning process since the resonance point could be missed due to ICD nearby tissue's resistance change from time to time. Therefore a low-cost optimal capacitance search is needed to fine-tune the frequency. A naïve search is to start from f_1 and scan through each 10 kHz (0.01 MHz) incremental value. However, this could take hundreds of coupling verifications (each time the ICD needs to test whether or not the coupling reaches a desired peak value, see Fig. 2). Thus we propose to use a fast search algorithm with an uneven step change (either incrementally or decrementally). Our scheme is based on the observation of the first-order derivative (δ) of ICD load voltage (V) with respect to match capacitance C in $[f_1, f_2]$, that is, $\delta = \partial V/\partial C$ [142]. As shown in Fig. 25, δ changes slowly in the beginning and then sharply when it gets closer to the fine-tune peak point. Thus we can select an initial capacitance C_1, and update it either slowly or quickly based on δ's value.

Analog-to-information: *Random Projection ECG Sensing and Signal Processing:* the analog-to-information through Sub-Nyquist Sampling (SNS) analog circuit (instead of performing signal compression in software) could bring a series of advantages: (1) It avoids the use of slow, complex compression software, as well as saving memory space; (2) It reduces sensing power and prolongs the ECG electrode's lifetime; (3) It also greatly decreases wireless transmission power consumption by reducing the ECG data amount to be transmitted to external devices. In our previous work [150], we designed SNS hardware that can perform *analog compression* with very sparse measurements through a *Gaussian random projection* (GRP) hardware lens instead of using traditional *digital compression* that needs to compress $N = 2 * f_{\max}$ measurements ($f_{\max}$ is the maximum cut-off frequency in the signal's spectrum). Their differences are illustrated in Fig. 26. It shows that SNS can save a significant amount of sensor energy by collecting much fewer samples ($M \ll N$) in *analog processing* phase. The GRP lens is just a low-cost, ultra-thin signal projection chip that naturally filters signals through a multi-channel structure.

In an ICD, we need to re-design the ADC (analog-to-digital conversion) circuit in order to meet the requirement of all-in-package for any IMD. Such a package is necessary to prevent circuit corrosion in humid tissue environment. Therefore, we propose to design a new ADC circuit (Fig. 27) to achieve SNS. The heart beat signals are multiplied by a random matrix (to be discussed later). Then the result passes through an integrator and a natural sampler. Finally, a non-even quantizer is used to generate the sparse ECG samples. The reason of using a *non-even* quantizer (instead of *even* one) is because that the heart beat strength has much higher amplitude in its signal peak than in other ECG segments.

One of the most important design considerations is the selection of the dimension of the random matrix. Based on SNS theory [151], for a K-dimensional subspace of R^N, giving constant δ, β belonging to (0, 1), the random matrix Φ with dimension $M \times N$, should meet the following condition in order to be a δ-stable embedding space (it is also a GRP requirement):

$$M \geq 2[K \ln(42/\delta) + \ln(2/\beta)]/(c\delta^2). \tag{35}$$

To further reduce the hardware design cost, we choose the random matrix as a random Bernoulli matrix with each element either $+1$ or -1. Every certain number of samples (say, N), we re-seed the pseudo-random generators, each of which determines one row of the random matrix. To generate M rows of matrix elements, we would need M generators. *However, many generators could cause high power consumption in the SNS circuit.* We thus propose to use only a few generators (<5), and use XOR operations between any two generators to generate new random elements as follows: we first take the bit-by-bit register value (i.e. state outputs), and then XOR with the last output of the other generator on a sample-by-sample basis. Fig. 28 shows a simple 2-generator case, which generates each matrix element $A_{11}, A_{12} \ldots A_{MN}$. As we can see, the last register's output from the second generator is used for XOR.

CPS prototype design: We finally integrate the above hardware units into an ICD prototype. The integrated PCB (print circuit board) has the functional architecture as shown in Fig. 29. We use VHDL to program Altera Cyclone V (it is a low-power tiny FPGA to be interfaced to the PCB), in order to achieve three tasks: (1) (Cyber algorithm → Physical control) Generate Chaos series to secure wireless power charge; (2) (Physical circuit → Cyber compression) Generate random matrix to achieve sub-Nyquist sampling; (3) Other important functions including communication control by interacting with a RF transceiver (we use Altera Cyclone V GX transceiver), generating electric pulses to the heart (based on heart beat rate sensing result), bio-signal (ECG) reconstruction-less SNS classification, and others.

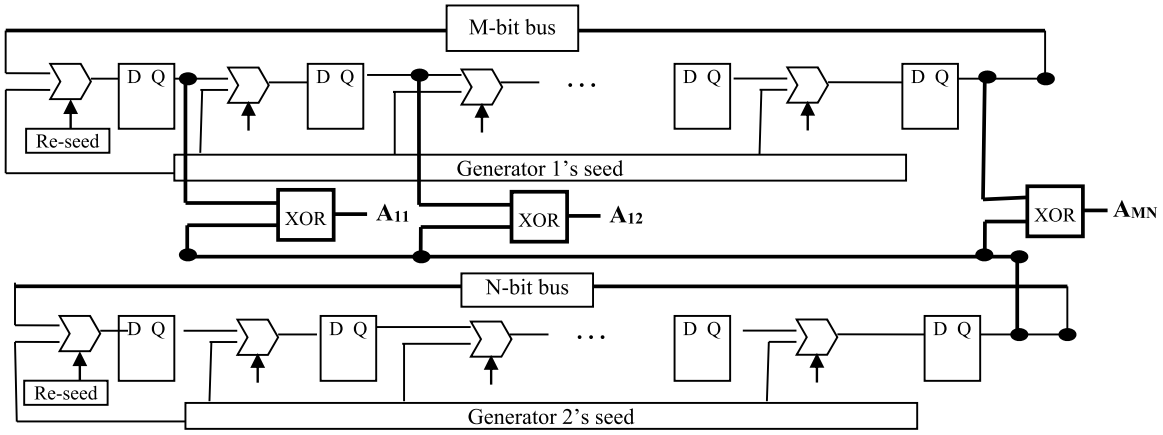


Fig. 28. Use less generators to generate SNS random matrix elements.

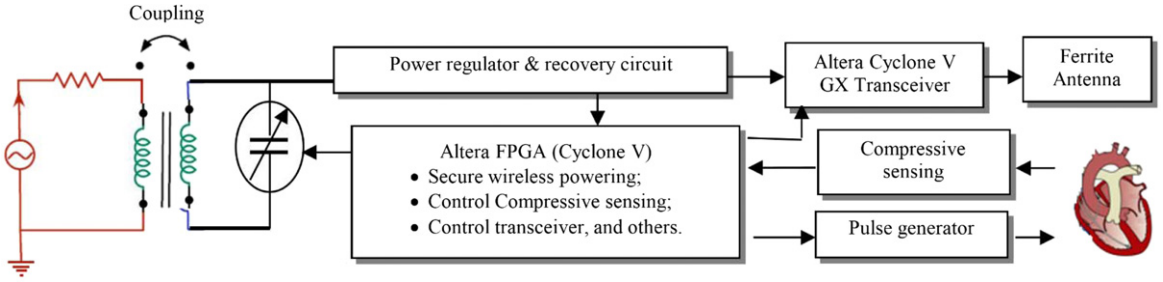


Fig. 29. Integrated FPGA/analog circuit design.

7. Open research issues

Based on our long-term CPS design experience, we have found that the most challenging issue in resilient CPS design is how to achieve a real-time, closed-loop, networked control system that can tolerate the natural noise (which causes packet loss and errors), as well as the internal or external attacks. In the following we discuss some promising research issues in resilient CPS design.

(1) *Error-tolerant networked control*: In a closed-loop sensor-to-controller interaction system, the sensors' data are sent to the controllers (via wireless or wired media), and then the controller makes real-time decision. The decision results can be seen from the new sensor readings, which trigger a new round of controller's decision. Note that such a closed-loop system should be described by a nonlinear model with noise model. The natural noise (from communication channels) can cause the packet loss or errors, which have negative impacts on the controller's decision correctness. An error-tolerant networked control model should be able to predict and adapt to such natural noise. Although networking protocols can certainly help to avoid packet errors, the repeated packet retransmission can bring intolerant network delay, which makes the controller's decision useless since the system state may have already changed in a new time. Therefore, the controller should be able to predict the possible sensing data errors based on the history sensor-to-controller communication channel conditions. It then makes up the gap by using a reasonable, safe decision if no new sensor data can be received due to network delay. It should also be able to recognize the obvious sensor data errors (such as significantly deviating from history average) and reject the coming sensor data.

(2) *Reinforced learning for intelligent decision*: Although general digital control theory can achieve state estimation and closed-loop control, it does not have an accurate utility/cost function to measure the effects of the current decision on the future rewards. Reinforced learning or Markov Decision models can be used to intelligently adjust the decision results based on the accumulative rewards in the history. It uses optimization theory to seek the best decision that can achieve the highest sum of rewards from current decision round to future states. It defines a cost/reward function to measure the effects of a decision. The POMDP (Partially Observable Markov Decision Process) can further used to enhance reinforced learning by considering incomplete or erroneous sensor data.

(3) *Machine learning for complex sensor data mining*: Any decision is based on the understanding of sensor data. However, in a realistic CPS, the sensor data could be complex: multiple sensor types, each with different sensor sampling rate and data format. More importantly, each may have totally different intrinsic patterns. For example, in a healthcare CPS, the EKG sensor measures the heart beat rhythm, which has periodical patterns; but EEG sensor measures brain activities that do not show regular shapes; the SpO2 sensor gives a slowly changing curve. Some signal transform tools are more suitable to one than others. For example, Fourier transform may capture EKG features well; but EEG may need wavelet transform. A more challenging issue is, how do we combine those sensors' data together into a single indication for a medical device control? Simple data fusion cannot capture the priority levels of different sensor data. General multi-sensor aggregation methods can lose the intrinsic high-dimensional features of sensor data. Manifold Learning may be a more accurate way to extract the universal features from different sensors since it can reserve the high-dimensional patterns during data mergence. But Manifold mergence is still an unsolved issue.

(4) *Multi-granularity event scheduling model*: In a complex CPS, there exist multiple controllers. Depending on sensors' data inputs and system control goals, those controllers need to be carefully scheduled to avoid out-of-order event acting. For example, in a medical surgery CPS, different medical devices have strict response time order. An insulin pump cannot work without stable heart beats and normal glucose level. A more complex issue is that different controllers work in different time granularity levels: some work in seconds level, some works in minutes level, etc. A comprehensive event scheduling map needs to be established between multiple controllers. The event transition condition depends on both current system state (which can be determined from sensors' readings) and control goals (what is the ultimate control result for current state). A Petri Net model could be a good event dispatching model. The event emulation software needs to be built for certain CPS.

(5) *Internal CPS attacks*: Although external attacks have been studied widely, internal attacks have not been given enough attention. An internal attacker knows the key information as well as communication protocols. It tries to mislead the controller's decision by intelligently changing the sensor data. The data looks normal but deviates from normal state equations. For such an internal attack, a robust state estimation equation is important since a sensitive estimation model can find out the non-smooth transition to a new state. And it can detect any trend that aims to lead the whole system to an unstable status. Proper data statistics methods should be used to detect the statistical attacks.

(6) *A physical dynamics description model that reflects the discrete control nature*: The real-life physical object changes state smoothly and continuously. However, most times it is not possible to find an accurate math model that describes such a continuous physical law. Therefore, we often need to use discrete state estimation model to describe a non-smooth system state change. Moreover, the controller's action is also discrete, that is, we can only generate actions in different time rounds. Therefore, it is important to make sure that the defined state estimation and control equations can well approximate the time-smoothing physical change nature. The sensor sampling rate needs to be determined properly in order to capture the system status with reasonable accuracy.

(7) *Safety vs. security*: CPS safety has not been studied deeply while security issues have been addressed in a large extent. Safety focuses on natural faults such as power drainage, switch breakage, storage full, etc. For a typical CPS—smart grid, the natural faults include numerous factors such as power grid isolation (from the main backbone), generator overheat, communication channel outage due to power line instability, etc. Safety ensures that the system has backup solutions for those faults. Safety also means that the CPS does not have negative impacts on humans' lives. For example, the wireless charger should not cause high radiation in nearby environment with humans or animals. For medical devices, safety issue is the No.1 priority since a patient cannot take any risk for using those medical devices. In national CPS such as natural gas distribution control, safety is especially critical since a mistake could cause the explosion.

(8) *CPS simulation tools*: Although some discrete-event-model based software tools have been designed for CPS simulation [152–154], they still cannot accurately reflect the coupling relationship between sensor data and control models. A larger scale CPS platform needs more considerations in the simulation designs, such as the network congestion issues, information aggregation, queueing delay, and so on. A friendly graphical user interface (GUI) is needed for easy operations of the tools. An advanced CPS simulation tool should allow the users to change the core codes in order to re-program some components (such as sensor types, data formatting, networked control models, and action types).

(9) *CPS interfacing to internet-of-things*: CPS eventually needs to be connected to Internet-of-Things (IoT) due to the requirement of remote control of sensors and actuators [155,156]. Many new research issues rise up when such a system is built. For example, how does the IoT use suitable sensor fusion to reduce the data redundancy? How does Internet efficiently route those data without much delay? How does Internet use unicast or multicast protocols to control the actuators? How does Internet reliably deliver the control commands to the actuators? And many other issues.

(10) *CPS for future healthcare*: Although healthcare systems have been improved from wireless networks, their performance enhancement based on CPS has not been studied quantitatively. How do different medical sensors interact with medical actuators, such as the interaction between glucose sensors and insulin pump? How does an implanted medical device (IMD) use CPS algorithms to achieve accurate organ treatment? How does a medical CPS protect its system from authorized access? How do we build a medical CPS with accurate patient data collection and diagnosis? And so on.

(11) *The embedding of cyber components into physical objects*: New approaches are needed in order to embed the computer hardware (such as sensors) and software units into the physical objects. The cyber units should be able to detect the entire physical object's status, instead of just part of its system. The sensors may need long-term battery charging (such as wireless power charge) circuit from solar, electromagnetic waves, and other sources. The sensors may need to communicate with the actuators wirelessly. The actuators should be able to control the whole object well based on the sensor data.

There are also many other critical research issues unsolved in terms of building a resilient CPS. The above issues are especially urgent since they are not paid enough attentions in academia.

8. Conclusions

In this paper, we have comprehensively surveyed the principle of building a resilient CPS. We discussed the three important features of CPS resilience: stability, security, and systematicness. We pointed out that networked control system can be used to describe the relationship between CPS sensors and actuators. The sensors provide inputs, and the actuators make the decision. We used some typical examples (such as smart grid, water distribution) to illustrate the principles. Especially, we provided two detailed CPS design case studies—virtual rehabilitation and pacemaker design, in order to show the systematic design process. Those two case studies also have security (through information-to-analog conversion) and stability considerations.

Acknowledgments

We thank the following people for their valuable comments and inputs: Tony Huynh, Ahmed Alsadah, Michael Johnson, Tony Randolph, Steven Guy, Erica Boyle, Rebecca Landrum, and Sarah Pace. We also thank US National Science Foundation (NSF) for their support of our CPS development under the grant No. DUE-1315328. Any ideas presented here do not necessarily represent NSF's opinions. We also thank the editor and reviewers' effort to review this paper.

References

[1] Kyoung-Dae Kim, P.R. Kumar, Cyber-physical systems: A perspective at the centennial, Proc. IEEE 100 (2012) 1287–1308. no. Special Centennial Issue.

[2] Davide Quaglia, Communications in cyber-physical systems, in: 2013 2nd Mediterranean Conference on Embedded Computing, MECO, 15–20 June 2013, pp. 1–1.

[3] Insup Lee, O. Sokolsky, Sanjian Chen, J. Hatcliff, Eunkyoung Jee, BaekGyu Kim, A. King, M. Mullen-Fortino, Soojin Park, A. Roederer, K.K. Venkatasubramanian, Challenges and research directions in medical cyber–physical systems, Proc. IEEE 100 (1) (2012) 75–90.

[4] Ivan Stojmenovic, Large scale cyber-physical systems: Distributed actuation, in-network processing and Machine-to-Machine communications, in: 2013 2nd Mediterranean Conference on Embedded Computing, MECO, 15–20 June 2013, pp. 21–24.

[5] K. Sampigethaya, R. Poovendran, Cyber-physical integration in future aviation information systems, in: Digital Avionics Systems Conference, DASC, 2012 IEEE/AIAA 31st 14–18 October 2012, pp. 7C2-1–7C2-12.

[6] I.S. Sacala, M.A. Moisescu, D. Repta, Towards the development of the future internet based enterprise in the context of cyber-physical systems, in: 2013 19th International Conference on Control Systems and Computer Science, CSCS, 29–31 May 2013, pp. 405–412.

[7] Marcin Szczodrak, Yong Yang, Dave Cavalcanti, Luca P. Carloni, An open framework to deploy heterogeneous wireless testbeds for Cyber-Physical Systems, in: 2018 8th IEEE International Symposium on Industrial Embedded Systems, SIES, 19–21 June 2013, pp. 215–224.

[8] Z. Zhang, H. Wang, C. Wang, H. Fang, Interference mitigation for cyber-physical wireless body area network system using social networks, IEEE Trans. Emerging Top. Comput. 1 (1) (2013) 121–132.

[9] J. Esch, Prolog to "Aviation cyber–physical systems: Foundations for future aircraft and air transport", Proc. IEEE 101 (8) (2013) 1831–1833.

[10] A. Banerjee, K.K. Venkatasubramanian, T. Mukherjee, S.K.S. Gupta, Ensuring safety, security, and sustainability of mission-critical cyber–physical systems, Proc. IEEE 100 (1) (2012) 283–299.

[11] C.W. Axelrod, Managing the risks of cyber-physical systems, in: 2013 IEEE Long Island Systems, Applications and Technology Conference, LISAT, 3–3 May 2013, pp. 1–6.

[12] M.J. Stanovich, I. Leonard, K. Sanjeev, M. Steurer, T.P. Roth, S. Jackson, M. Bruce, Development of a smart-grid cyber-physical systems testbed, in: 2013 IEEE PES Innovative Smart Grid Technologies, ISGT, 24–27 February 2013, pp. 1–6.

[13] J. Taneja, R. Katz, D. Culler, Defining CPS challenges in a sustainable electricity grid, in: 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, ICCPS, 17–19 April 2012, pp. 119–128.

[14] C. Sankavaram, A. Kodali, K. Pattipati, An integrated health management process for automotive cyber-physical systems, in: 2013 International Conference on, Computing, Networking and Communications, ICNC, 28–31 January 2013, pp. 82–86.

[15] Ayan Banerjee, Sandeep K.S. Gupta, Spatio-temporal hybrid automata for safe cyber-physical systems: A medical case study, in: 2013 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS, 8–11 April 2013, pp. 71–80.

[16] Hongan Wang, Xiaoming Deng, Feng Tian, WiP abstract: A human-centered cyber-physical systematic approach for post-stroke monitoring, in: 2012 IEEE/ACM Third International Conference on, Cyber-Physical Systems, ICCPS, 17–19 April 2012, pp. 209–209.

[17] I.H. Rao, N.A. Amir, H. Dagale, J. Kuri, e-SURAKSHAK: A cyber-physical healthcare system with service oriented architecture, in: 2012 International Symposium on Electronic System Design, ISED, 19–22 December 2012, pp. 177–182.

[18] M. Lukasiewycz, S. Steinhorst, F. Sagstetter, Wanli Chang, P. Waszecki, M. Kauer, S. Chakraborty, Cyber-physical systems design for electric vehicles, in: 2012 15th Euromicro Conference on Digital System Design, DSD, 5–8 September 2012, pp. 477–484.

[19] Xu Li, Chunming Qiao, A. Wagh, R. Sudhaakar, S. Addepalli, Changxu Wu, A. Sadek, A holistic approach to service delivery in driver-in-the-loop vehicular CPS, IEEE J. Sel. Areas Commun. 31 (9) (2013) 513–522.

[20] G. Hackmann, W. Guo, G. Yan, Z. Sun, C. Lu, S. Dyke, Cyber-physical co-design of distributed structural health monitoring with wireless sensor networks, IEEE Trans. Parallel Distrib. Syst. 25 (1) (2014) 63–72.

[21] Y.P. Fallah, Raja Sengupta, A cyber-physical systems approach to the design of vehicle safety networks, in: 2012 32nd International Conference on Distributed Computing Systems Workshops, ICDCSW, 18–21 June 2012, pp. 324–329.

[22] B. Syed, A. Pal, K. Srinivasarengan, P. Balamuralidhar, A smart transport application of cyber-physical systems: Road surface monitoring with mobile devices, in: 2012 Sixth International Conference on Sensing Technology, ICST, 18–21 December 2012, pp. 8–12.

[23] G. Schirner, D. Erdogmus, K. Chowdhury, T. Padir, The future of human-in-the-loop cyber-physical systems, Computer 46 (1) (2013) 36–45.

[24] M. Franke, C. Seidl, T. Schlegel, A seamless integration, semantic middleware for cyber-physical systems, in: 2013 10th IEEE International Conference on Networking, Sensing and Control, ICNSC, 10–12 April 2013, pp. 627–632.

[25] S. El-Tawab, S. Olariu, Communication protocols in FRIEND: A cyber-physical system for traffic Flow Related Information Aggregation and Dissemination, in: 2013 IEEE International Conference on Pervasive Computing and Communications Workshops, PERCOM Workshops, 18–22 March 2013, pp. 447–452.

[26] Amir Aminifar, Petru Eles, Zebo Peng, Anton Cervin, Control-quality driven design of cyber-physical systems with robustness guarantees, in: Design, Automation & Test in Europe Conference & Exhibition, DATE, 2013, 18–22 March 2013, pp. 1093–1098.

[27] S. Mitra, T. Wongpiromsarn, R.M. Murray, Verifying cyber-physical interactions in safety-critical systems, IEEE Secur. Privacy 11 (4) (2013) 28–37.

[28] Leon Wu, G. Kaiser, An autonomic reliability improvement system for cyber-physical systems, in: 2012 IEEE 14th International Symposium on High-Assurance Systems Engineering, HASE, 25–27 October 2012, pp. 56–61.

[29] Husheng Li, Lifeng Lai, H.V. Poor, Multicast routing for decentralized control of cyber physical systems with an application in smart grid, IEEE J. Sel. Areas Commun. 30 (6) (2012) 1097–1107.

[30] Xianghui Cao, Peng Cheng, Jiming Chen, Youxian Sun, An online optimization approach for control and communication codesign in networked cyber-physical systems, IEEE Trans. Ind. Inf. 9 (1) (2013) 439–450.

[31] Jing Lin, S. Sedigh, A. Miller, Towards integrated simulation of cyber-physical systems: A case study on intelligent water distribution, in: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009. DASC'09. 12–14 December 2009, pp. 690–695.

[32] R. Mitchell, I. Chen, Effect of intrusion detection and response on reliability of cyber physical systems, IEEE Trans. Reliab. 62 (1) (2013) 199–210.

[33] Yilin Mo, T.H.-H. Kim, K. Brancik, D. Dickinson, Heejo Lee, A. Perrig, B. Sinopoli, Cyber–physical security of a smart grid infrastructure, Proc. IEEE 100 (1) (2012) 195–209.

[34] A. Hahn, A. Ashok, S. Sridhar, M. Govindarasu, Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid, IEEE Trans. Smart Grid 4 (2) (2013) 847–855.

[35] K. Ravindran, M. Rabby, Cyber-physical systems based modeling of adaptation intelligence in network systems, in: 2011 IEEE International Conference on Systems, Man, and Cybernetics, SMC, 9–12 October 2011, pp. 2737–2742.

[36] Akshay Rajhans, Shang-Wen Cheng, Bradley Schmerl, David Garlan, Bruce H. Krogh, Clarence Agbi, Ajinkya Bhave, An architectural approach to the design and analysis of cyber-physical systems, in: Proceedings of the 3rd International Workshop on Multi-Paradigm Modeling, MPM 2009.

[37] J. Rajamaki, P. Rathod, A. Ahlgren, J. Aho, M. Takari, S. Ahlgren, Resilience of cyber-physical system: A case study of safe school environment, in: 2012 European Intelligence and Security Informatics Conference, EISIC, 22–24 August 2012, pp. 285–285.

[38] S. Deshmukh, B. Natarajan, A. Pahwa, State estimation in spatially distributed cyber-physical systems: Bounds on critical measurement drop rates, in: 2013 IEEE International Conference on Distributed Computing in Sensor Systems, DCOSS, 20–23 May 2013, pp. 157–164.

[39] M. Li, P. Li, Crowdsourcing in cyber-physical systems: Stochastic optimization with strong stability, IEEE Trans. Emerging Top. Comput. 1 (2) (2013) 63–72.

[40] Kelly O'Connell, CIA report: Cyber extortionists attacked foreign power grid, disrupting delivery, Internet Business Law Services, 2008. See the following site for details: http://www.ibls.com/internet_law_news_portal_view.aspx?id=1963&s=latestnews.

[41] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, Experimental security analysis of a modern automobile, in: Proceedings of the 31st IEEE Symposium on Security and Privacy, May 2010.

[42] Elinor Mills, Hackers broke into FAA air traffic control system, Wall Street J. (2009) A6.

[43] Vanessa Fuhrmans, Virus attacks siemens plant-control systems, Wall Street J. (2010).

[44] A.A. Cárdenas, S. Amin, B. Sinopoli, A. Giani, A.A. Perrig, S.S. Sastry, Challenges for securing cyber physical systems, in: Workshop on Future Directions in Cyber-physical Systems Security, Newark, NJ, USA, July 2009.

[45] C.L. DeMarco, J.V. Sariashkar, F. Alvarado, The potential for malicious control in a competitive power systems environment, in: IEEE Int. Conf. on Control Applications, Dearborn, MI, USA, 1996, pp. 462–467.

[46] Davide Quaglia, Cyber-physical systems: Modeling, simulation, design and validation, in: 2013 2nd Mediterranean Conference on Embedded Computing, MECO, 15–20 June 2013, pp. 1–2.

[47] J. Moreno, M. Damm, J. Haase, C. Grimm, E. Holleis, Unified and comprehensive electronic system level, network and physics simulation for wirelessly networked cyber physical systems, in: 2012 Forum on Specification and Design Languages, FDL, 18–20 September 2012, pp. 68–74.

[48] Lei Bu, Dingbao Xie, Xin Chen, Linzhang Wang, Xuandong Li, Demo abstract: BACHOL—modeling and verification of cyber-physical systems online, in: 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, ICCPS, 17–19 April 2012, pp. 222–222.

[49] S. Gao, H. Luo, D. Chen, S. Li, P. Gallinari, Z. Ma, J. Guo, A cross-domain recommendation model for cyber-physical systems, IEEE Trans. Emerging Top. Comput. 1 (2) (2013) 384–393.

[50] Xiaoxiang Zhai, Qiaoqiao Chen, Shunhui Ji, Bixin Li, A unified modeling and verifying framework for cyber physical systems, in: 2012 12th International Conference on Quality Software, QSIC, 27–29 August 2012, pp. 128–131.

[51] Zhiqiang Ma, Xiao Fu, Zhenhua Yu, Object-oriented petri nets based formal modeling for high-confidence cyber-physical systems, in: 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM, 21–23 September 2012, pp. 1–4.

[52] Sheng-Tzong Cheng, Tun-Yu Chang, A cyber physical system model using genetic algorithm for actuators control, in: 2012 2nd International Conference on Consumer Electronics, Communications and Networks, CECNet, 21–23 April 2012, pp. 2269–2272.

[53] Marc Geilen, Stavros Tripakis, Maarten Wiggers, The earlier the better: A theory of timed actor interfaces Technical Report No. UCB/EECS-2010-130 October 7, 2010. EECS Department University of California, Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-130.html.

[54] P.A. Vicaire, E. Hoque, Xie Zhiheng, J.A. Stankovic, Bundle: A group-based programming abstraction for cyber-physical systems, IEEE Trans. Ind. Inf. 8 (2) (2012) 379–392.

[55] Arquimedes Canedo, Eric Schwarzenbach, Ai Faruque, Mohammad Abdullah, Context-sensitive synthesis of executable functional models of cyber-physical systems, in: 2013 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS, 8–11 April 2013, pp. 99–108.

[56] Zhenkai Zhang, Emeka Eyisi, Xenofon Koutsoukos, Joseph Porter, Gabor Karsai, Janos Sztipanovits, Co-simulation framework for design of time-triggered cyber physical systems, in: 2013 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS, 8–11 April 2013, pp. 119–128.

[57] P. Bogdan, S. Jain, K. Goyal, R. Marculescu, Implantable pacemakers control and optimization via fractional calculus approaches: A cyber-physical systems perspective, in: 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, ICCPS, 17–19 April 2012, pp. 23–32.

[58] Ying Tan, Mehmet C. Vuran, Steve Goddard, Yue Yu, Miao Song, Shangping Ren, A concept lattice-based event model for Cyber-Physical Systems, in: Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, (ICCPS'10), ACM, New York, NY, USA, 2010, pp. 50–60.

[59] Marija D. Ilie, Le Xie, Usman A. Khan, Jose M.F. Moura, Modeling of future cyber-physical energy systems for distributed sensing and control, IEEE Trans. Syst. Man Cybern. Part A 40 (4) (2010).

[60] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, Pan Shengyi, U. Adhikari, Modeling cyber-physical vulnerability of the smart grid with incomplete information, IEEE Trans. Smart Grid 4 (1) (2013) 235–244.

[61] M. Lin, Y. Pan, L. Yang, M. Guo, N. Zheng, Scheduling co-design for reliability and energy in cyber-physical systems, IEEE Trans. Emerging Top. Comput. 1 (2) (2013) 353–365.

[62] R. Maas, E. Maehle, K.-E. Grosspietsch, Applying the organic robot control architecture ORCA to cyber-physical systems, in: 2012 38th EUROMICRO Conference on Software Engineering and Advanced Applications, SEAA, 5–8 September 2012, pp. 250–257.

[63] John C. Eidson, Edward A. Lee, Slobodan Matic, Sanjit A. Seshia, Jia Zou, Time-centric models for designing embedded CPSs. Technical Report Identifier: EECS-2009-135, October 9, 2009. Electrical Engineering and Computer Sciences University of California at Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-135.html.

[64] Jaeyong Park, Arda Kurt, Omit Ozquner, Poster abstract: A game theoretic approach to controller design for cyber-physical systems: Collision avoidance, in: 2013 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS, 8–11 April 2013, pp. 254–254.

[65] Zhilin Qian, Huiqun Yu, A TAOPN approach to modeling and scheduling cyber-physical systems, in: 2013 International Conference on Information Science and Applications, ICISA, 24–26 June 2013, pp. 1–7.

[66] Cong Xinyu, Yu Huiqun, Xu Xin, Verification of hybrid chi model for cyber-physical systems using PHAVer, in: 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS, 3–5 July 2013, pp. 122–128.

[67] Li Ye-jing, Chen Ming-cai, Zhang Guang-quan, Shao Yu-zhen, Feng Fei, Hou Xing-hua, A model for vehicular Cyber-Physical System based on extended hybrid automaton, in: 2013 8th International Conference on Computer Science & Education, ICCSE, 26–28 April 2013, pp. 1305–1308.

[68] Patricia Derler, Edward A. Lee, Alberto sangiovanni vincentelli. Modeling CPSs', Proc. IEEE 100 (1) (2012).

[69] Junsung Kim, Hyoseung Kim, Karthik Lakshmanan, Ragunathan Rajkumar, Parallel scheduling for cyber-physical systems: Analysis and case study on a self-driving car, in: 2013 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS, 8–11 April 2013, pp. 31–40.

[70] E. Palachi, C. Cohen, S. Takashi, Simulation of cyber physical models using SysML and numerical solvers, in: 2013 IEEE International Systems Conference, SysCon, 15–18 April 2013, pp. 671–675.

[71] see: http://www.isis.vanderbilt.edu/research/MIC.

[72] L. Parolini, et al., A cyber-physical systems approach to data center modeling and control for energy efficiency, Proc. IEEE 100 (2012) 251–268.

[73] Rock-Hyun Choi, Sang-Cheol Lee, Dong-Ha Lee, Joonhyuk Yoo, WiP abstract: Packet loss compensation for cyber-physical control systems, in: 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, ICCPS, 17–19 April 2012, pp. 205–205.

[74] Kailong Zhang, Jiwei Li, Arnaud de la Fortelle, Xingshe Zhou, Agent based adaptive cooperative models and mechanisms of multiple autonomous cyber-physical systems, in: 2013 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD, 1–3 July 2013, pp. 159–164.

[75] M.M. Jamshidi, Sustainable energy systems: Cyber-physical based intelligent mangement of micro-grids, in: 2012 4th IEEE International Symposium on Logistics and Industrial Informatics, LINDI, 5–7 September 2012, pp. 11–12.

[76] M. Wooldridge, An Introduction to Multiagent Systems, John Wiley & Sons, Ltd., 2002.

[77] P.J. Modi, P. Scerri, W.-M. Shen, M. Tambe, Distributed Sensor Networks: A Multiagent Perspective, Kluwer Academic Publishers, 2003, (Chapter) Distributed Resource Allocation: A Distributed Constraint Reasoning Approach.

[78] Nguyen-Thinh Le, L. Martin, C. Mumme, N. Pinkwart, Communication-free detection of resource conflicts in multi-agent-based cyber-physical systems, in: 2012 6th IEEE International Conference on Digital Ecosystems Technologies, DEST, 18–20 June 2012, pp. 1–6.

[79] T. oshimoto, T. Ushio, Poster abstract: Design of modified observer to reduce state estimation error caused by job skipping in cyber-physical systems, in: 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, ICCPS, 17–19 April 2012, pp. 236–236.

[80] Ashish Choudhari, Harini Ramaprasad, Tamal Paul, Jonathan W. Kimball, Maciej Zawodniok, Bruce McMillin, Sriram Chellappan, WiP abstract: Stability of a cyber-physical smart grid system using cooperating invariants, in: 2013 ACM/IEEE International Conference on Cyber-Physical Systems, ICCPS, 8–11 April 2013, pp. 240–240.

[81] P. Tabuada, S.Y. Caliskan, M. Rungger, R. Majumdar, Towards robustness for cyber-physical systems, IEEE Trans. Automat. Control 59 (12) (2014) 3151–3163.

[82] J.L. Jerez, P.J. Goulart, S. Richter, G.A. Constantinides, E.C. Kerrigan, M. Morari, Embedded online optimization for model predictive control at megahertz rates, IEEE Trans. Automat. Control 59 (12) (2014) 3238–3251.

[83] D.E. Quevedo, V. Gupta, W.-J. Ma, S. Yuksel, Stochastic stability of event-triggered anytime control, IEEE Trans. Automat. Control 59 (12) (2014) 3373–3379.

[84] P. Tabuada, Event-triggered real-time scheduling of stabilizing control tasks, IEEE Trans. Automat. Control 52 (2007) 1680–1685.

[85] L. Greco, D. Fontanelli, A. Bicchi, Almost sure stability of anytime controllers via stochastic scheduling, in: Proc. IEEE Conf. Decis. Contr., New Orleans, LA, USA, December 2007, pp. 5640–5645.

[86] S. Caliskan, M. Rungger, R. Majumdar, Towards robustness for cyber-physical systems, IEEE Trans. Automat. Control 59 (12) (2014) 3151–3163.

[87] Arnaldo Pereira, Nelson Rodrigues, Jose Barbosa, Paulo Leitao, Trust and risk management towards resilient large-scale Cyber-Physical Systems, in: 2013 IEEE International Symposium on Industrial Electronics, ISIE, 28–31 May 2013, pp. 1–6.

[88] F. Pasqualetti, F. Dorfler, F. Bullo, Attack detection and identification in cyber-physical systems, IEEE Trans. Automat. Control 58 (11) (2013) 2715–2729.

[89] Björn Andersson, Nuno Pereira, Eduardo Tovar, How a cyber-physical system can efficiently obtain a snapshot of physical information even in the presence of sensor faults, in: WISES, 2008, pp. 1–10.

[90] Jing Lin, Sahra Sedigh, Ann Miller, A general framework for quantitative modeling of dependability in cyber-physical systems: A proposal for doctoral research, in: Proceedings of the 2009 33rd Annual IEEE International Computer Software and Applications Conference—Volume 01, (COMPSAC'09), IEEE Computer Society, Washington, DC, USA, 2009, pp. 668–671.

[91] E.J. Candès, T. Tao, The Dantzig selector: Statistical estimation when p is much larger than n, Ann. Statist. 35 (6) (2007) 2313–2351.

[92] YuLun Huang, Alvaro Cardenas, Saurabh Amin, Song-Zyun Lin, Hsin-Yi Tsai, Shankar Sastry, Understanding the physical and economic consequences of attacks against control systems, Int. J. Crit. Infrastruct. Prot. 2 (3) (2009) 72–83.

[93] Aditya Ashok, Adam Hahn, Manimaran Govindarasu, A cyber-physical security testbed for smart grid: system architecture and studies, in: Frederick T. Sheldon, Robert Abercrombie, Axel Krings (Eds.), Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, (CSIIRW'11), ACM, New York, NY, USA, 2011, p. 1. Article 20.

[94] H. Qi, X. Wang, L. Tolbert, A resilient real-time system design for a secure and reconfigurable power grid, IEEE Trans. Smart Grid 2 (4) (2011) 770–781.

[95] F. Pasqualetti, F. Dorfler, F. Bullo, Cyber-physical attack in power networks: Models, fundamental limitations and monitor design, Technique Report, UC Santa Barbara, Santa Barbara, CA 93106, 1103.2795v1, March 14, 2011. See: http://motion.me.ucsb.edu/pdf/2011i-pdb.pdf.

[96] C.M. Krishna, I. Koren, Adaptive fault-tolerance for cyber-physical systems, in: 2013 International Conference on Computing, Networking and Communications, ICNC, 28–31 January 2013, pp. 310–314.

[97] D. Macdonald, S.L. Clements, S.W. Patrick, C. Perkins, G. Muller, M.J. Lancaster, W. Hutton, Cyber/physical security vulnerability assessment integration, in: 2013 IEEE PES Innovative Smart Grid Technologies, ISGT, 24–27 February 2013, pp. 1–6.

[98] B. Stelte, G.D. Rodosek, Assuring trustworthiness of sensor data for cyber-physical systems, in: 2013 IFIP/IEEE International Symposium on Integrated Network Management, IM 2013, 27–31 May 2013, pp. 395–402.

[99] Saurabh Amin, On cyber security for networked control systems (Ph.D. dissertation), University of California, Berkeley, 2011, p. 198.

[100] B. McMillin, Privacy and confidentiality in cyber-physical power systems, in: Power and Energy Society General Meeting, 2012 IEEE, 22–26 July 2012, pp. 1–3.

[101] Cheolhyeon Kwon, Weiyi Liu, Inseok Hwang, Security analysis for Cyber-Physical Systems against stealthy deception attacks, in: American Control Conference, ACC, 2013, 17–19 June 2013, pp. 3344–3349.

[102] X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, W. Zhao, A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems, IEEE Trans. Comput. 64 (1) (2015) 4–18.
[103] Alvaro A. Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, Shankar Sastry, Attacks against process control systems: risk assessment, detection, and response, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, (ASIACCS'11), ACM, New York, NY, USA, 2011, pp. 355–366.
[104] T.J.H.M. Eggen, Item selection in adaptive testing with the sequential probability ratio test, Appl. Psychol. Meas. 23 (3) (1999) 249–261.
[105] M. He, J. Zhang, Fault Detection and Localization in Smart Grid: A Probabilistic Dependence Graph Approach, IEEE, 2010, pp. 43–48.
[106] Marco A.R. Ferreira, Victor De Oliveira, Bayesian reference analysis for Gaussian Markov random fields, J. Multivariate Anal. 98 (4) (2007) 789–812.
[107] J.E. Besag, C. Kooperberg, On conditional and intrinsic autoregressions, Biometrika 82 (1995) 733–746.
[108] C. Ten, J. Hong, C. Liu, Anomaly detection for cybersecurity of the substations, IEEE Trans. Smart Grid 2 (4) (2011) 865–873.
[109] Power system test case archive, Available at: http://www.ee.washington.edu/research/pstca/.
[110] S. Sridhar, A. Hahn, M. Govindarasu, Cyber-physical system security for the electric power grid, Proc. IEEE 100 (1,) (2012) 210–224.
[111] P. Mohajerin Esfahani, M. Vrakopoulou, G. Andersson, J. Lygeros, A tractable nonlinear fault detection and isolation technique with application to the cyber-physical security of power systems, in: 2012 IEEE 51st Annual Conference on Decision and Control, CDC, 10–13 December 2012, pp. 3433–3438.
[112] Joerg Haehner, Stefan Rudolph, Sven Tomforde, Dominik Fisch, Bernhard Sick, Nils Kopal, Arno Wacker, A concept for securing cyber-physical systems with organic computing techniques, in: Proceedings of 2013 26th International Conference on Architecture of Computing Systems, ARCS, 19–22 February 2013, pp. 1–13.
[113] W. Shen, L. Liu, X. Cao, Y. Hao, Y. Cheng, Cooperative message authentication in vehicular cyber-physical systems, IEEE Trans. Emerging Top. Comput. 1 (1) (2013) 84–97.
[114] Feng Tan, Yufei Wang, Qixin Wang, Lei Bu, Rong Zheng, N. Suri, Guaranteeing proper-temporal-embedding safety rules in wireless CPS: A hybrid formal modeling approach, in: 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN, 24–27 June 2013, pp. 1–12.
[115] S. Amin, G.A. Schwartz, A. Hussain, In quest of benchmarking security risks to cyber-physical systems, IEEE Netw. 27 (1) (2013) 19–24.
[116] D. Goswami, R. Schneider, S. Chakraborty, Re-engineering cyber-physical control applications for hybrid communication protocols, in: 14th Conference for Design, Automation and Test in Europe, DATE, Grenoble, France, 2011.
[117] W. Zhang, M.S. Branicky, S.M. Phillips, Stability of networked control systems, IEEE Control Syst. Mag. 21 (1) (2001) 84–99.
[118] D. Goswami, R. Schneider, S. Chakraborty, Co-design of cyber-physical systems via controllers with flexible delay constraints, in: 16th Asia and South Pacific Design Automation Conference, ASP-DAC, Yokohama, Japan, 2011.
[119] H. Voit, R. Schneider, D. Goswami, A. Annaswamy, S. Chakraborty, Optimizing hierarchical schedules for improved control performance, in: 5th International Symposium on Industrial Embedded Systems, SIES, Trento, Italy, 2010.
[120] R. Schneider, U. Bordoloi, D. Goswami, S. Chakraborty, Optimized schedule synthesis under real-time constraints for the dynamic segment of flexray, in: 8th International Conference on Embedded and Ubiquitous Computing, EUC, Hong Kong SAR, China, 2010.
[121] F. Zhang, K. Szwaykowska, W. Wolf, V.J. Mooney III, Task scheduling for control oriented requirements for cyber-physical systems, in: IEEE Real-Time Systems Symposium, 2008, pp. 47–56.
[122] M. Chow, Y. Tipsuwan, Network-based control systems, in: Proceedings of IEEE IECon 2001 Tutorial, Denver, CO, November 28–December 2, 2001, pp. 1593–1602.
[123] An introduction to Kalman filters: http://www.cs.unc.edu/~welch/kalman/kalmanIntro.html.
[124] P. Dagum, R. Karp, M. Luby, S. Ross, An optimal algorithm for Monte Carlo estimation, SIAM J. Comput. 29 (5) (2000) 1484–1496.
[125] Bernd A. Berg, Markov Chain Monte Carlo Simulations and their Statistical Analysis (With Web-Based Fortran Code), World Scientific, ISBN: 981-238-935-0, 2004.
[126] D. Li, et al., A Cyber Physical Networking System for Monitoring and Cleaning up Blue-Green Algae Blooms with Agile Sensor and Actuator Control Mechanism on Lake Tai, Chinese Academy of Sciences, Beijing, China, 2011, 978-1-4577-0248/11.
[127] A. Nasir, Boon-Hee Soong, PipeSense: A framework architecture for in-pipe water monitoring system, in: 2009 IEEE 9th Malaysia International Conference on Communications, MICC, 15–17 December 2009, pp. 703–708.
[128] T. Dillon, V. Potdar, J. Singh, A. Talevski, Cyber-physical systems: Providing Quality of Service (QoS) in a heterogeneous systems-of-systems environment, in: 2011 Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference, DEST, May 31 2011–June 3 2011, pp. 330–335.
[129] Jingyong Liu, Lichen Zhang, QoS modeling for cyber-physical systems using aspect-oriented approach, in: 2011 Second International Conference on Networking and Distributed Computing, ICNDC, 21–24 September 2011, pp. 154–158.
[130] Feng Xia, Longhua Ma, Jinxiang Dong, Youxian Sun, Network QoS management in cyber-physical systems, in: International Conference on Embedded Software and Systems Symposia, 2008. ICESS Symposia'08. 29–31 July 2008, pp. 302–307.
[131] Y.-C. Pai, T.S. Bhatt, Repeated-slip training: An emerging paradigm for prevention of slip-related falls among older adults, Phys. Ther. 87 (2007) 1478–1491.
[132] HDT Robotics—KineAssist: http://devwww.hdtglobal.com/services/robotics/portfolio/KineAssist/ For more detailed materials on KineAssist, see http://www.kineadesign.com/portfolio/kineassist/ Note that Kinea Design Inc. is now renamed as HDT Robotics Inc., a division of HDT Global.
[133] J. Patton, E. Lewis, G. Crombie, M. Peshkin, E. Colgate, J. Santos, A. Makhlin, D.A. Brown, A novel robotic device to enhance balance and mobility training post-stroke, Top. Stroke Rehabil. 15 (2) (2008) 131–139.
[134] K.J. Sullivan, B.J. Knowlton, B.H. Dobkin, Step training with body weight support: effect of treadmill speed and practice paradigms on poststroke locomotor recovery, Arch. Phys. Med. Rehabil. 83 (2002) 683–691.
[135] E. Hsu, K. Pulli, J. Popovi, Style translation for human motion, in: Markus Gross (Ed.), ACM SIGGRAPH 2005, SIGGRAPH'05, ACM, New York, NY, USA, 1082–1089.
[136] W.K. Pratt, Generalized Wiener filtering computation techniques, IEEE Trans. Comput. 21 (7) (1972) 636–641.
[137] Ali H. Sayed, Adaptive Filters, Wiley-IEEE Press, 2008, book.
[138] C. Li, Q. Hao, W. Guo, F. Hu, Compressive neural activity detection with fMR images using graphical model inference, Int. J. Comput. Biol. Drug Des. (InderScience) 3 (3) (2010) 187–200. December of.
[139] M. Liu, H. Ji, C. Zhao, Event related potentials extraction from EEG using artificial neural network, in: Proceedings of the 2008 Congress on Image and Signal Processing, Volume 01, (CISP'08), IEEE Computer Society, Washington, DC, USA, 2008, pp. 213–215.
[140] A. Villringer, J. Planck, C. Hock, L. Schleinkofer, U. Dirnagl, Near infrared spectroscopy (NIRS): A new tool to study hemodynamic changes during activation of brain function in human adults, Neurosci. Lett. 154 (1993) 101–104.
[141] H. Choi, S. Choi, A. Katake, Y. Kang, Y. Choe, Manifold Alpha-Integration, in: Lecture Notes in Computer Science, vol. 6230/2010, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 397–408.
[142] D.A. Cesario, G. William, Implantable cardioverter defibrillator therapy in clinical practice, J. Am. Coll. Cardiol. 47 (2006) 1507–1517.
[143] S. O'Driscoll, Adaptive signal acquisition and power delivery for implanted medical devices (Ph.D. dissertation), Electrical Engineering, Stanford University, 2009.
[144] A.K.R. Rakhyani, Design of efficient wireless power-transfer system and piezoelectric transducer for sonoporation-based drug-delivery implants (M.s. thesis), Electrical and Computer Engineering, The University of British Columbia, Vancouver, 2010.
[145] M.H. Schoenfeld, S.J. Compton, R.H. Mead, D.N. Weiss, L. Sherfesee, J. Englund, et al., Remote monitoring of implantable cardioverter defibrillators: a prospective analysis, Pacing Clin. Electrophysiol. 27 (2004) 757–763.
[146] J.C. Res, D.A. Theuns, L. Jordaens, The role of remote monitoring in the reduction of inappropriate implantable cardioverter defibrillator therapies, Clin. Res. Cardiol. 95 (2006) III17–III21.
[147] G. Liu, A high quality PN sequence generator based on chaotic maps, in: 2009 Fifth International Conference on Natural Computation, ICNC, Vol. 5, 2009, pp. 432–436.
[148] H. Jiang, C. Fu, A chaos-based high quality PN sequence generator, in: 2008 International Conference on Intelligent Computation Technology and Automation, ICICTA, Issue Date: 20–22 October 2008, pp. 60–64.
[149] S. Zhu, S. Setia, S. Jajodia, LEAP: efficient security mechanisms for large-scale distributed sensor networks, in: Proceedings of the 10th ACM Conference on Computer and Communications Security, (CCS'03), ACM, New York, NY, USA, 2003, pp. 62–72.
[150] Q. Hao, F. Hu, Y. Xiao, Multiple human tracking and identification with wireless distributed pyroelectric sensors, IEEE Syst. J. 3 (4) (2009) 428–439. special issue on Biometrics.
[151] D. Donoho, Compressed sensing, IEEE Trans. Inform. Theory 52 (4) (2006) 1289–1306.
[152] Ahmad T. Al-Hammouri, A comprehensive co-simulation platform for cyber-physical systems, Comput. Commun. 36 (1) (2012) 8–19. 1 December.
[153] Weilin Li, Xiaobin Zhang, Huimin Li, Co-simulation platforms for co-design of networked control systems: An overview, Control Eng. Pract. 23 (2014) 44–56.
[154] Jing Lin, S. Sedigh, A. Miller, Towards integrated simulation of cyber-physical systems: A case study on intelligent water distribution, in: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009. DASC'09, 12–14 December 2009, pp. 690–695.
[155] J. Wan, et al., From machine-to-machine communications towards cyber-physical systems, Comput. Sci. Inf. Syst. 10 (3) (2013) 1105–1128.
[156] J. Wan, et al., Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges and solutions, IEEE Commun. Mag. 52 (8) (2014) 106–113.

Fei Hu is currently a professor in the Department of Electrical and Computer Engineering at the University of Alabama (main campus), Tuscaloosa, Alabama, USA. He obtained his Ph.D. degrees at Tongji University (Shanghai, China) in the field of Signal Processing (in 1999), and at Clarkson University (New York, USA) in the field of Electrical and Computer Engineering (in 2002). He has published over 200 journal/conference papers, books, and book chapters. Dr. Hu's research has been supported by US National Science Foundation (NSF), US Department of Defense (DoD), Cisco, Sprint, and other sources. He has chaired a few international conferences. His research interests are *3S—Security, Signals, Sensors*: (1) Security: This is about how to overcome different cyber attacks in a complex wireless or wired network. Recently he focuses on cyber–physical system security and medical security issues. (2) Signals: This mainly refers to *intelligent signal* processing, that is, using machine learning algorithms to process sensing signals in a smart way in order to extract patterns (i.e., achieve pattern recognition). (3) Sensors: This includes micro-sensor design and wireless sensor networking issues.

Yu Lu received his B.E. degree in electronic engineering from Chongqing University, Chongqing, China in 2014. He is now working toward his M.E degree in the Department of Electrical and Computer Engineering, The University of Alabama, Tuscaloosa, AL, USA. His research interests are wireless sensor network, Cyber–physical system security and big data.

Athanasios V. Vasilakos is currently Professor at the University of Western Macedonia, Greece and Visiting Professor National Technical University of Athens (NTUA), Athens, Greece. He has authored or co-authored over 200 technical papers in major international journals and conferences. He is author/coauthor of five books and 20 book chapters in the areas of communications. Prof. Vasilakos has served as General Chair, Technical Program Committee Chair for many international conferences. He served or is serving as an Editor or/and Guest Editor for many technical journals, such as the *IEEE Transactions on Network and Services Management*, *IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics*, the *IEEE Transactions on Information Technology in Biomedicine*, *ACM Transactions on Autonomous and Adaptive Systems*, the IEEE JSAC special issues of May 2009, Jan 2011, March 2011, the I*EEE Communications Magazine*, ACM/Springer Wireless Networks (WINET), ACM/Springer Mobile Networks and Applications (MONET). He is founding Editor-in-Chief of the *International Journal of Adaptive and Autonomous Communications Systems* (IJAACS, http://www.inderscience.com/ijaacs) and the *International Journal of Arts and Technology* (IJART, http://www.inderscience.com/ijart). He is General Chair of the Council of Computing of the European Alliances for Innovation.

Qi Hao received the B.E. and M.E. degrees from Shanghai Jiao Tong University, Shanghai, China, in 1994 and 1997, respectively, and the Ph.D. Degree from Duke University, Durham, NC, USA, in 2006, all in electrical engineering. His postdoctoral training in the Center for Visualization and Virtual Environment, The University of Kentucky, Lexington, KY, USA was focused on 3-D computer vision for human tracking and identification. From 2007 to 2014, he was an Assistant Professor with the Department of Electrical and Computer Engineering, the University of Alabama, Tuscaloosa, AL, USA. He is currently an Associate Professor with South University of Science and Technology of China, Shenzhen, China. His research has been supported by the US NSF and other sources. His current research interests include smart sensors, intelligent wireless sensor networks, and distributed information processing.

Rui Ma received the B.S. degree in physics from Beijing Normal University in 2008, and the M.S. degree in Microelectronics from Institute of Semiconductors, Chinese Academy of Sciences in 2011. He is now working toward the Ph.D. degree in Electrical Engineering at the University of Alabama. His research interests include wireless sensor network, intelligent sensing system, machine learning for human activity recognition, and time series analysis.

Yogendra Patil received the Bachelors degree in engineering in the field of electronics and telecommunications. He completed his Master's degree from Wright State University, OH, USA, in the field of electrical engineering. He is currently working toward the Ph.D. degree from the University of Alabama, Tuscaloosa, USA. He is currently a Research Assistant in the area of Pattern Recognition and Machine Learning.

Ting Zhang is a Ph.D. student in Department of Electrical and Computer Engineering of University of Alabama. She got her B.E. in Computer Engineering in Tianjin University in China and got her M.S. in Computer Science in University of Texas at Brownsville. Her research interests focus in the area of data mining & classification algorithms, computer vision & computer graphics. Ting enjoys writing code, playing piano, cooking and shopping.

Jiang Lu received the B.E. degree in electrical engineering from Shanghai Maritime University, Shanghai, China in 2007, and the M.S. degree in electrical and computer engineering from University of Florida, Gainesville, FL in 2008. He is currently working toward the Ph.D. degree in the electrical and computer engineering at The University of Alabama. His research interests include machine learning and pattern recognition, intelligent sensor systems, tele-healthcare, and mobile computing.

Xin Li received his B.E. degree in electronic engineering from University of Electronic Science and Technology of China (UESTC), Chengdu, China in 2011 and M.E degree in communication and information system from University of Science and Technology of China (USTC), Hefei, China in 2014. He is now working toward his Ph.D. degree in the Department of Electrical and Computer Engineering, the University of Alabama, Tuscaloosa, AL, USA. His research interests include wireless networks, MAC layer design, and Machine Learning algorithms.

Neal N. Xiong is currently a professor in the School of Computer Science, Colorado Technical University, CO, USA. His research interests are wireless networks, cloud computing, fault tolerance, artificial intelligence, and sensor networks. He obtained his Ph.D. degree in 2012 at George State University. He has over 50 international publications.