2015 20th IEEE European Test Symposium (ETS)

# Cyber-Physical Systems: A Security Perspective

Charalambos Konstantinou*, Michail Maniatakos*, Fareena Saqib†, Shiyan Hu‡, Jim Plusquellic§ and Yier Jin¶
*Department of Electrical and Computer Engineering, New York University - Abu Dhabi
†Department of Electrical and Computer Engineering, Florida Institute of Technology, USA
‡Department of Electrical and Computer Engineering, Michigan Technological University, USA
§Department of Electrical and Computer Engineering, University of New Mexico, USA
¶Department of Electrical Engineering and Computer Science, University of Central Florida, USA
{ckonstantinou@nyu.edu, michail.maniatakos@nyu.edu, fsaqib@fit.edu, shiyan@mtu.edu, jimp@ece.unm.edu, yier.jin@eecs.ucf.edu}

***Abstract*—A cyber-physical system (CPS) is a composition of independently interacting components, including computational elements, communications and control systems. Applications of CPS institute at different levels of integration, ranging from nation-wide power grids, to medium scale, such as the smart home, and small scale, e.g. ubiquitous health care systems including implantable medical devices. Cyber-physical systems primarily transmute how we interact with the physical world, with each system requiring different levels of security based on the sensitivity of the control system and the information it carries. Considering the remarkable progress in CPS technologies during recent years, advancement in security and trust measures is much needed to counter the security violations and privacy leakage of integration elements. This paper focuses on security and privacy concerns at different levels of the composition and presents system level solutions for ensuring the security and trust of modern cyber-physical systems.**

## I. Introduction

The research relating to cyber-physical systems (CPS) has recently drawn the attention of academia, industry, and the government because of its wide impact to society, economy, and environment [1]. While still lacking in formal definition, cyber-physical systems are largely referred to as the next generation of engineered systems with the integration of communication, computation, and control to achieve the goals of stability, performance, robustness, and efficiency for physical systems [2]. While ongoing research work focuses on achieving these goals, security within CPS is largely ignored [1]. As cyber-physical systems are being widely integrated in various critical infrastructures, however, any security breaches to these systems could have catastrophic consequences. For example, if a vehicle-to-vehicle communication network is compromised, accidents would occur when wrong distance information is transmitted. In fact, the emergence of autonomous cars has further deteriorated the problem since passengers have to trust all decisions made by the vehicles.

Besides security concerns, CPS privacy is another serious issue. Cyber-physical systems are often distributed broadly across wide geographic areas and typically collect huge amounts of information for data analysis and decision making. The collection of information helps the system make smart decisions through sophisticated machine learning algorithms. Data breach, however, could potentially happen in any part of the system, including the stages of data collection, data transmission, data operation, and data storage. Again, most of the current CPS design methodologies do not consider data protection, leaving the collected data in jeopardy.

In this survey paper, we discuss a diverse set of cyber-physical systems with different complexity and integration scale. The massive deployment of advanced metering infrastructure (AMI) and home energy management system has mandated a transformative shift of the classical grid into a more reliable and secure grid, resulting in the so called *smart grid*. This emerging infrastructure consists of four parts, namely power generation, transmission, distribution, and end use. The latter part, end usage, has also been enjoying a shift towards the integration of intelligent control systems, creating the notion of *home automation systems*. Such systems will also be extensively discussed in this survey paper. Finally, the last part introduces the smallest scale of CPS, namely *health care systems*, such as wearable and implantable medical devices (IMDs). Health care devices can be wore or implanted to control and regulate functions of many organs inside the body. Health care devices communicate via wireless sensor networks They are vulnerable to networks attacks and may also be compromised at the device level.

A plethora of security and privacy solutions exist for the three aforementioned categories of cyber-physical systems. Solutions discussed in this paper include network level security, physical unclonable functions (PUFs), machine learning approaches and firmware diversity. The rest of the paper is organized as follows: Section II presents challenges and solutions for smart-grid security, while Section III focuses on home automation systems. Finally, Section IV discusses the lowest level of integration, health-care systems, followed by conclusions in Section V.

## II. Smart Grid Security

A prominent example of a nation-wide CPS is the power grid. The structure of power grid indicates a complex cyber-physical system, designed to support the needs of a growing population. For example, in 2013, U.S. grid could carry over 1,063 gigawatts of power while continuously balancing supply with fluctuating demand [3]. Figure 1 illustrates the cyber-physical perspective of power grid. The power grid components (generation, transmission, distribution and consumption) are equipped with cyber-systems including communication networks, control automation systems and centers, and Intelligent Electronic Devices (IEDs). Utilities participate in energy

978-1-4799-7603-4/15/$31.00 ©2015 IEEE

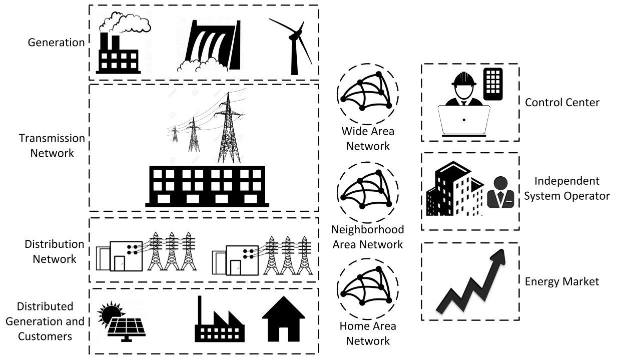

Figure 1: Cyber-physical infrastructure of power grid.

markets and coordinate with independent system operators which monitor the operation of smart grid.

During the last few years, there has been an effort to modernize the current grid by establishing dynamic and interactive power equipment communication. In addition, advanced smart grid applications are deployed in order to enhance grid efficiency and resiliency. The inadequate level of security measures prior to the implementation of those technologies, however, has led to a greater threat landscape. Therefore, this section focuses on the challenges that arise due to the deployment of smart grid technologies, as well as fundamental countermeasures towards enhancing the security of the grid.

### A. *Challenges for a Secure and Resilient Smart Grid*

Successful smart grid integration requires the establishment of security mechanisms in order to face persistent challenges. In the past, several real world examples have shown that the power grid is exposed to various threats that can lead to severe consequences. The Stuxnet incident (discovered in 2010) and its cousins Duqu, Flame and Gauss are few of the most significant cases of targeted attacks [4]. Duqu, Flame and Gauss focused on traditional espionage scopes. On the other hand, Stuxnet [5] presented a foundational shift in malware with its ability to usurp the operation of an Industrial Control System (ICS) and manipulate Programmable Logic Controllers (PLC) while spreading through injected portable media drives using four zero-day vulnerabilities.

Existing research on smart grid cyber-security challenges is mainly categorized into two major groups: Methods that could compromise systems and devices, and methods that could impact the communication of the smart grid.

*1) Systems and Devices:* The coupling between the power control applications and embedded cyber-systems expanded the attack surface. Many integrated control devices are running firmware and operating systems with published bugs and vulnerabilities (e.g. buffer overflows) making them vulnerable to attacks [6]. Adversaries can develop malicious software and spread it on Supervisory Control And Data Acquisition (SCADA) systems, PLCs and IEDs [7]. In addition, many devices lack authentication support, allowing unauthorized users to gain access and manipulate system settings and operations [8]. Furthermore, malware might be installed on devices prior the shipment to the target location [9] or devices might be infiltrated inside the trusted perimeter, deliberately or not, by personnel.

*2) Communications:* The modernization of power grid leads to a tightly interconnected system, increasing the number of connections and resulting in the creation of new paths to potentially undermine communication systems. Virtual Private Networks (VPNs) and firewalls constitute an essential part of the newly shaped zones. Although VPNs create secure encrypted connections, they do not prevent attacks since they protect only the tunnel and not the client or the server device [10]. Poor firewall configuration settings can also be detected and leveraged by attackers as entry points into the system [11].

The existing smart grid protocols migrate their vulnerabilities to the grid components. For example, Modbus was designed for low-speed serial communication in process control networks; it is not designed to address security issues. Thus, several attacks are possible, such as broadcast message spoofing and response delay attack [12]. In addition, attackers can impersonate authorized users by spoofing their identity [13].

Databases used in industrial control systems are often connected with web-enabled applications located on the business network. Therefore, attackers can exploit the communication channel between the two networks and hence bypass the security mechanisms used to protect the control systems environment [14]. Furthermore, false data injection attacks (e.g. faking meter data - replay attack) can mislead the outcome of state estimation routines [15] causing a huge financial impact on electricity markets [16].

### B. *Security Countermeasures for Smart Grid*

Since threats are constantly evolving, proper defenses require advanced cyber-security mechanisms. In order to maintain the reliability and stability of the smart grid as a system, security technologies related with smart grid devices, networks and management systems are essential, both at the device and at the network level.

*1) Devices:* As discussed previously, the smart grid is an evolved grid system of new and legacy devices. Protecting these devices from adversaries should first focus on securing their executed software. If the underlying binary code is not trusted, then any other mechanisms implemented at the application level cannot be trusted. For example, an IED can be protected using a collection of interdependent routines (e.g. encryption algorithms) embedded into the firmware code of the device [17]. Firmware diversity methods have the ability to significantly slow down a large-scale compromise of smart meters [18]. In addition, remote code verification can be achieved using attestation techniques, enabling an external entity to detect stealthy malware [19]. Intrusion Detection Systems (IDS) are also widely deployed to detect unwanted entities into a system by using signature-based, specification-based, or anomaly-based techniques [20].

The task of providing security services for the smart grid heavily depends on authentication, authorization and message integrity of smart grid devices and systems. As a result, developed authentication schemes adopt public key cryptography concepts. Fouda *et al.* [21] proposed a lightweight two-step mutual authentication protocol. In [22], the authors address the authentication issue from a storage load minimization perspective using a one-time signature scheme. For message integrity, Zhang *et al.* [23] propose a 256-bit AES scheme as a solution for the data transmission between two smart grid devices in ethernet networks.

*2) Network:* The IEC 61850 communication standard intends to replace DNP3 in substation communications and can be potentially used for outside substation communication in future power systems [24]. Towards protocols security, in [25] the authors propose a prototype multicast system using a cross-layer approach to handle and secure substation's intercommunications in IEC 61850 power networks. In order to fulfill authentication requirements, there is a need to incorporate more efficient schemes during the design or upgrade of communication protocols [26]. Furthermore, homomorphic encryption protocols can be used to aggregate smart meter communications to a gateway [27], [28]; due to their performance implications, however, the trade-off between security and efficiency must be examined thoroughly [29].

Due to the bi-directional information flow of smart grid, switches, firewalls and gateway controllers are critical for cyber-security, as they can contribute to the necessary network separation (demilitarized zones (DMZs), traffic control on information flow [30]). The networking of these components for wired, wireless and sensor networks should ensure routing security and improved resiliency against cross-layer traffic injection [31]. Moreover, their communication channel capacity must be appropriately defined to guarantee security against eavesdropping.

*3) Management:* Cryptographic approaches have become primary countermeasures against malicious attacks. In addition to encryption and authentication procedures, key management processes are also part of cryptographic methods. For example, Public Key Infrastructure (PKI) can contribute towards establishing trust between different identities using digital signatures. Despite the constraints regarding cryptography and key management [32], research has shown that PKI technology could be prospectively deployed into the smart grid [33].

The management of data transmission and data access of smart grid equipment exacerbated concerns on data objects security. In response to the concerns, IEC 62351 has proposed role-based access control for substation automation [34]. Implementations of access control models could potentially establish trust and role assignments for users in different smart grid domains [35].

## III. Smart Home Security

Besides the nation-wide aspect of the smart grid, recent work has also highlighted the importance of sophisticated end-use controls of the smart-grid. For example, given a 5% improvement of the energy usage on the residential side, the resulting energy savings and reduction of carbon emission will be similar to removing 53 million cars [36]. The wide adoption of smart home systems also breeds security concerns.

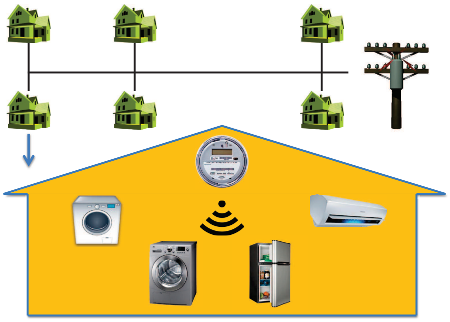

Figure 2: Typical Smart Home infrastructure

### A. Smart Home Infrastructure

The smart home infrastructure features the automatic control of the end usage of electricity. It employs the smart meter in the household of each customer as a controller, which schedules the energy consumption of the home appliances according to the electricity pricing information and the need of the customer. Given the guideline electricity price provided by the utility, the smart meter uses various smart home scheduling techniques to shift the energy consumption from peak pricing hours to the non-peak ones, thus reducing the electricity bill. For the utility, a sophisticated designed guideline electricity price can help balance the energy load of the power grid. This helps mitigate the pressure of the generation, transmission and distribution systems due to peak energy usage and the pollution due to excessive power generation. Figure 2 shows a sample smart home infrastructure.

Various smart home scheduling techniques have been developed, depending on the configuration of the home appliances for a single customer. Among multiple customers, since the customers are always charged based on the total energy consumption of the whole community and the contribution of each customer in the past time window, the electricity bill of each customer depends on the energy consumption of other customers as well as that of their own. Thus, a game theoretic framework is commonly deployed to solve the smart home scheduling problem among multiple customers. Recent research shows that the smart home scheduling technique can reduce the electricity bill of the customers by 34.3% and the peak to average ratio (PAR) of the energy load by 35.9% [36].

### B. Smart Home Cyberattacks

Unfortunately, smart home cybersecurity, which is a very important aspect of the smart home system research, is much less studied despite its criticality. Smart home cybersecurity addresses security challenges at both system and device levels. For the device level hacking, multiple public media have reported the exploration of vulnerabilities in smart devices [37], [38]. Smart meters suffer from similar threats which make them vulnerable to cyberattacks. For example, Texas Instruments provides an all in one smart meter design solution using the AMR/AMI platform [39]. The main focus is to

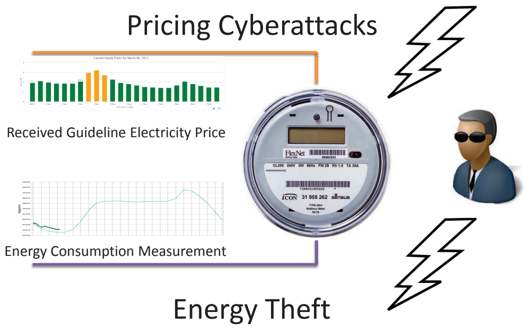
Pricing Cyberattacks
Received Guideline Electricity Price
Energy Consumption Measurement
Energy Theft

Figure 3: Pricing cyberattacks and energy theft.

provide interfacing libraries for these modules and a reference design [40] for reducing the development time and cost. However, the AMR/AMI platform does not take security into consideration and can be easily exploited by various attacks with or without physical access. In fact, an important component in a smart house for HVAC control, the Google Nest Thermostat, has recently proved to be insecure [37]. After identifying and reviewing the components of a Google Nest Thermostat, researchers found vulnerabilities in the device hardware infrastructure, or more specifically, the Texas Instruments Sitara AM3703 processor. Through software code reverse engineering and hardware analysis, the whole toolchain was recovered which was then used to develop malicious filesystem on Nest Thermostats. A compromised Google Nest thermostat enables attackers to remotely control the device.

Similar to the smart thermostat, smart meters can also be compromised so that hackers can remotely control the device. The hacker can choose to manipulate the input guideline electricity price or output energy consumption measurement, which are known as *pricing cyberattack* and *energy theft*, respectively. Figure 3 demonstrates the two types of smart home cyberattacks.

*1) Pricing Cyberattack:* Customers conduct smart home scheduling according to the guideline electricity price received by the smart meter. Thus, the scheduling of the customers will be misled if the guideline electricity price is manipulated. This can impact the energy load in the power grid. Since the customers are charged based on the energy consumption in the past time window, the electricity bills of the customers can also be impacted if the energy load is influenced. Demonstrated in [41], attackers can manipulate the guideline electricity price for two purposes:

- The attacker can manipulate the guideline electricity price to create a peak energy load.
- The attacker can manipulate the guideline electricity price to reduce his/her own electricity bill at the cost of increasing those of others.

*2) Energy Theft:* In addition to pricing cyberattack, adversaries can manipulate the measurement of energy consumption and tune it down. Thus, the electricity bill is significantly reduced since the energy consumption is not totally charged. If the energy theft amount is large, the utility has to shut down the energy supply since the real energy load is much higher than the measurement [42].

### C. Multi-Level Smart House Security Protection

As the first step towards building highly secure hardware infrastructures for cyberattacks defense, hardware platforms within smart devices should be secured with resilient architectures. Considering the unique property of hardware of no/minimal update frequency compared to its firmware/software counterparts, security must be considered from the early stages of the design flow. For example, a cross-boundary security platform is developed that ensures trusted execution of privileged kernel extensions and device drivers [43], [44]. This has been achieved by co-designing a secure Linux kernel running on a security-enhanced SPARC V8 compatible processor. This platform can be used for highly-secure smart meter development which supports customizable, user-friendly security policy and monitoring capabilities in the OS. The platform can also help balance the security and performance for embedded hardware.

Defense techniques are also proposed at the system level, countering cyberattacks in the smart home system. In [45], the long term detection technique is developed based on partially observable Markov decision process (POMDP) and support vector regression (SVR). SVR is used to predict the guideline electricity price from historical data. The cyberattack is reported if the electricity bill and PAR corresponding to the received guideline electricity price are significantly higher than those corresponding to the predicted price. The POMDP is then employed to compute the optimal action (e.g. check the smart meters or ignore the cyberattack report) considering the expected reward and the transient variance of guideline electricity price. Based on that framework, the authors in [46] propose the energy load prediction and defense technique considering the impact of net metering on smart home cybersecurity. In [42], energy theft is detected through inserting feeder remote terminal units (FRTUs). The locations of the FRTUs are computed by the cross entropy method in order to minimize the cost for installing FRTUs while maintaining the detection accuracy. These methods have been proved to effectively detect different cyberattacks to smart home systems.

### D. Future Directions

While single-layer protection methods have been proved successful, more sophisticated and powerful cyberattacks are expected to be launched soon, similar to the StuxNet attack to control systems (discussed in Section II-A). Cross-layer cyberattacks on smart home are expected to be a major threat: Attackers could spread malicious firmware to many of the networked smart devices such that a sophisticated attacking method could be performed. This attack will target the whole smart home system and could be carefully designed to evade existing single-layer protection methods, e.g., one smart device's outputs will still be within the allowed threshold but the cumulative effect will compromise the security of the whole system. As a result, a salient defense technology clearly needs to tackle various cyberattacks in a judiciously integrated way rather than separately. Cross-layer protection schemes will become the default in smart home protection.

## IV. Health Care Security

As the previous sections highlighted, security consideration is largely ignored in high-end complex CPS such as the smart grid and smart home systems. The same problem, regrettably, also exists in low-end networked embedded devices. Fortunately, the increased reliance on remote and embedded electronics as the basis for personal, commercial and military command and control systems is driving the need for improved security and trust in these cyber-physical systems [47]–[49]. Technology has been playing an important role in the area of medical devices for patient diagnosis, monitoring and treatment consisting of x-ray apparatus, magnetic resonance imaging (MRI), surgical and other medical instruments. Given a recent paradigm shift, emerging medical devices are not only composed of passive devices controlled by human but are moving towards more complex cyber-physical systems consisting of active devices [50], [51], including computational embedded systems with sensors and actuators to analyze and control the physical processes. Ultimately, cyber-physical systems transform how we interact with the physical world, where each system requires different level of security based on the sensitivity of the information and control system. Health care related CPS in the areas of implantable medical devices (IMDs), body area networks (BAN) [52] and wearable devices [53] with limited computational capability and communication complexity and challenged battery life requires privacy, security and trust.

Subversion of integrated circuits in the supply chain is just one recent area of security concern, of many, where adversaries can manipulate, sabotage and/or destroy electronic components slated for installation in later commercial electronics, critical infrastructures [54]–[58]. In the case of, for example, IMDs such as pacemakers, defibrillators, and nerve sensors, any effort to remove potentially compromised chip/bug or to have any other security fix would require a surgery. Therefore, security and trust play an extremely critical role.

### A. Challenges in Health Care CPS

In health care, fundamentals enabling privacy, assurance and secure communication of medical device are very important. There are many key factors influencing the development of a robust and autonomous health care CPS, including the proprietary nature of medical-device lacking standard interfaces and communication protocols. Strict HIPAA (Health Insurance Portability and Accountability Act) [59] privacy regulations complicate the information exchange even further. Below we discuss these issues in detail.

*1) Privacy and Quality Assurance:* The networking for distributed sensing and control can range from dedicated networks to wireless sensor networks for monitoring and sharing the information with other facilities. Federal Communications Commission (FCC) has allocated the bandwidth range of 402–405 MHz for medical implant communication services [60].

Networking services include channel arbitration, link establishment, routing, and data transmission. In the ubiquitous embedded devices, with seamless integration with the physical environment, personal wireless communication has become an integral part of communication. All the inherent security threats of wireless communication involving impersonation, eavesdropping and jamming [61] can be exploited in more complex cyber-physical systems and can be used for security threats from passive eavesdroppers, to active adversaries, e.g. to use life threatening attacks like sending electric shocks using the implanted medical devices.

*2) Security and Trust in Abstractions:* An important driver of emerging security and trust problems is globalization. Nearly every step of the modern design process, from architecture, through RTL, layout, manufacturing, packaging, distribution and system integration is farmed out to individual companies located all over the world [62]. This has raised serious concerns over the trustworthiness of components in the supply chain, where substitutions of malicious clones and sub-standard components, are becoming increasingly easier for adversaries because of the lack of component identification information and corresponding tracking mechanisms.

Moreover, tools for the evaluation of security and trust, e.g., those that determine whether large complex 3rd party intellectual property (IP) components do what they are supposed to do and nothing more, are non-existent in modern design and test flows. IP that serves as interface, such as USB driver, opens up additional information leakage vulnerabilities beyond the standard concerns that the IP possesses hidden kill switches or other types of malicious functionality. Compounding the problem is the fact that malicious insertions can occur at any abstraction level including RTL, structural and layout, with each requiring different types of detection methods. Fundamental changes are required in the integrated circuit (IC) design flow and authentication processes to combat these vulnerabilities.

### B. Security Countermeasures for Health Care System

Developing a comprehensive framework for secure IMD design requires knowledge about the possible security and trust issues [63], at the device level as well as the world wide sensor web or other communication crucial in the area of health care. The networks are widespread in many systems, providing connectivity and bringing convenience but on the other hand expose the systems to be easily inspected and probed by attackers. Security at the device level is important to make sure that the correct device is being used (i.e. identification and authentication of device), the device is doing what it is supposed to do, and no Trojans [64]–[68] are configured. We now present both the network and device level security solutions for the health care.

*1) Network Level Security Solutions:* Major concerns in CPS communication include keeping the data private and allowing only authorized access. Network attacks can be implemented at the physical layer as well as the software layer.

Furthermore, attackers may attempt to physically probe the devices, altering their behavior or intercepting the physical properties of power consumption and timing behaviors to analyze the secrets and masquerade them. Proposed solutions include fault recovery mechanisms [69], [70], temper resistant methods [71] and better attack detection to take preventive actions [72]. At software level, several data security solutions have been discussed in wireless sensor networks [73]. Light weight protocols incorporate symmetric mechanisms like SPINS [74] and TinySec [75] providing security using SNEP and Skipjack or RC5 ciphers, respectively. Other security solutions include uTESLA [74] for broadcast authentication, and INSENS [76] for intrusion tolerant protocols.

*2) Device Level Security Solutions:* Device can be identified using a unique label stored in a nonvolatile memory, and later authenticating the device by reading the stored response. This kind of authentication is prone to attacks where adversary can read the memory and can masquerade the identity. Many software solutions exist [52]; and a lot of work has been done at the hardware level where fingerprints are generated using physical unclonable functions (PUFs), utilizing the process variations which are unique to a given device and cannot be cloned. This section focuses on the existing solutions provided in latest research work using PUFs.

Physically unclonable function use for authentication could potentially provide an efficient hardware solution: Each device generates a unique signature/fingerprint by deriving random but reproducible bitstring from the underlying manufacturing variations in the printed and implanted features of wires and transistors on an IC [77]. Since the variations are unique in each device, the bitstrings generated are also unique for different devices. Impersonation is nearly impossible because it would require control over the fabrication process that is well beyond current capabilities.

PUF maps a set of digital challenges to a set of digital responses by exploiting these physical variations in the IC. The analog nature of the entropy sources makes PUFs 'tamper-evident', whereby invasive attacks by adversaries to probe the PUF damages it. PUFs have been proposed that are constructed using variations in transistor threshold voltages [78], delay chains and ROs [79], [80], FPGAs [81], SRAMs [82], leakage current [83], [84], the path delays of core logic macros [85], microprocessors [86] and memristors [87]. Other characteristics of PUFs include uniqueness, randomness and reproducibility. These properties, and PUFs being nonreplicable are very promising primitives for the purpose of producing embedded bitstring used in applications, such as cryptographic keys generation for data encryption, authentication, and hardware metering. PUF can be classified as strong PUF or weak PUF based on the number of random bitstrings it can generate, where strong PUFs are more suitable for authentication.

Some of the recent innovations use path delays of existing logic/macros as a source of entropy, instead of having many copies of identical specialized circuitry to measure the process variations. For example, a hardware-embedded delay PUF called HELP has been described in [85], where hardware-embedded refers to the property that the secret bitstring is derived from the measured path delays in the implementation of an Advanced Encryption Standard (AES) module. The generated bitstring is later used as the key for the AES unit itself when it is run in functional mode. The overhead of the HELP PUF is very low because the source of entropy used to derive the key is the functional unit itself. HELP PUF is thus a good candidate to be incorporated on the secure elements of the cyber-physical systems. Another PUF that can meet the efficiency and resource constraints of devices in health care CPS is NVM PUF [87], which requires no error correction or helper data.

## V. Conclusions

In this paper, we emphasized the importance of protecting cyber-physical systems at various scales, including nation wide CPS, such as the smart-grid, to medium scale CPS, e.g. home automation systems, all the way to minuscule systems such as implantable medical devices. The survey highlighted the security and privacy concerns of various components of such systems, and discussed potential solutions towards enhancing the robustness of critical cyber-physical systems.

## References

[1] Kyoung-Dae Kim and P.R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1287–1308, 2012.

[2] Ragunathan (Raj) Rajkumar, Insup Lee, Lui Sha, and John Stankovic, "Cyber-physical systems: The next computing revolution," in *Proceedings of the 47th Design Automation Conference*, 2010, DAC '10, pp. 731–736.

[3] U.S. Energy Information Administration, U.S. Department of Energy, "International Energy Statitics," [Online]: http://www.eia.gov/.

[4] Boldizsr Bencsth, Gbor Pk, Levente Buttyn, and Mrk Flegyhzi, "The cousins of stuxnet: Duqu, flame, and gauss.," *Future Internet*, vol. 4, no. 4, pp. 971–1003, 2012.

[5] T.M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[6] Industrial Control Systems Cyver Emergency Response Team, Department of Homeland Security, "ICS-CERT Alerts," [Online]: https://ics-cert.us-cert.gov/alerts.

[7] Igor Nai Fovino, Andrea Carcano, Marcelo Masera, and Alberto Trombetta, "An experimental investigation of malware attacks on scada systems," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 139–145, 2009.

[8] Aldar C.-F. Chan and Jianying Zhou, "Cyber-Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 7, pp. 1509–1517, 2014.

[9] Mike Rogers and C.A. Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," in *U.S. House of Representatives, 112th Congress*, 2012.

[10] Sanaz Rahimi and Mehdi Zargham, "Analysis of the security of {VPN} configurations in industrial control environments," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 1, pp. 3 – 13, 2012.

[11] Troy Nash, "Backdoors and holes in network perimeter," [Online]: http://ics-cert.us-cert.gov/control$_systems/$, 2005.

[12] JulianL. Rrushi, "Scada protocol vulnerabilities," in *Critical Infrastructure Protection*, vol. 7130 of *Lecture Notes in Computer Science*, pp. 150–176. Springer Berlin Heidelberg, 2012.

[13] U.K. Premaratne, J. Samarabandu, T.S. Sidhu, R. Beresh, and Jian-Cheng Tan, "An intrusion detection system for iec61850 automated substations," *Power Delivery, IEEE Transactions on*, vol. 25, no. 4, pp. 2376–2383, 2010.

[14] Nektarios Georgios Tsoutsos and Michail Maniatakos, "Trust no one: Thwarting" heartbleed" attacks using privacy-preserving computation," in *VLSI (ISVLSI), 2014 IEEE Computer Society Annual Symposium on*. IEEE, 2014, pp. 59–64.

[15] O. Kosut, Liyan Jia, R.J. Thomas, and Lang Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 220–225.

[16] Le Xie, Yilin Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 226–231.

[17] Hoi Chang and Mikhail J. Atallah, "Protecting software code by guards," in *Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management*, London, UK, UK, 2002, DRM '01, pp. 160–175, Springer-Verlag.

[18] Stephen McLaughlin, Dmitry Podkuiko, Adam Delozier, Sergei Miadzvezhanka, and Patrick McDaniel, "Embedded firmware diversity for smart electric meters," in *5th USENIX Workshop on Hot Topics in Security (HotSec 2010)*, 2010.

[19] Michael LeMay, George Gross, Carl A. Gunter, and Sanjam Garg, "Unified architecture for large-scale attested metering," in *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*. 2007, HICSS '07, IEEE Computer Society.

[20] R. Berthier, W.H. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, Oct 2010, pp. 350–355.

[21] M.M. Fouda, Z.M. Fadlullah, N. Kato, Rongxing Lu, and Xuemin Shen, "A lightweight message authentication scheme for smart grid communications," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 675–685, 2011.

[22] Qinghua Li and Guohong Cao, "Multicast authentication in the smart grid with one-time signature," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 686–696, 2011.

[23] Peng Zhang, O. Elkeelany, and L. McDaniel, "An implementation of secured smart grid ethernet communications using aes," in *IEEE SoutheastCon 2010 (SoutheastCon), Proceedings of the*, 2010, pp. 394–397.

[24] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication protocols and networks for power systems-current status and future trends," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, 2009, pp. 1–9.

[25] Jianqing Zhang and C.A. Gunter, "Application-aware secure multicast for power grid communications," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 339–344.

[26] Qiyan Wang, H. Khurana, Ying Huang, and K. Nahrstedt, "Time valid one-time signature for time-critical multicast data authentication," in *INFOCOM 2009, IEEE*, 2009, pp. 1233–1241.

[27] Nektarios Georgios Tsoutsos and Michail Maniatakos, "HEROIC: Homomorphically EncRypted One Instruction Computer," in *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, 2014, pp. 1–6.

[28] Fenjun Li, Bo Luo, and Peng Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 327–332.

[29] C. Konstantinou, A. Keliris, and M. Maniatakos, "Privacy-preserving functional ip verification utilizing fully homomorphic encryption," in *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2015*, March 2015, pp. 1–6.

[30] Ilan Barda, "Cyber security for advanced smart-grid applications," *ISGF conference*, 2013, [Online]: http://indiasmartgrid.org/en/.

[31] National Institute of Standards and Technology, "Guidelines for smart grid cyber security, NIST," [Online]: http://csrc.nist.gov/, 2014.

[32] S. Iyer, *Cyber Security for Smart Grid, Cryptography, and Privacy*, International Journal of Digital Multimedia Broadcasting, 2011.

[33] H.K.-H. So, S.H.M. Kwok, E.Y. Lam, and King-Shan Lui, "Zero-configuration identity-based signcryption scheme for smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 321–326.

[34] International Electrotechnical Commission, "Iec 62351," [Online]: http://www.iec.ch/smartgrid/standards/.

[35] H. Cheung, A. Hamlyn, T. Mander, Cungang Yang, and R. Cheung, "Role-based model security access control for smart power-grids computer networks," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, 2008, pp. 1–7.

[36] Yang Liu, Shiyan Hu, Han Huang, Rajiv Ranjan, Albert Zomaya, and Lizhe Wang, "Game theoretic market driven smart home scheduling considering energy balancing," *accepted to IEEE System Journal*.

[37] Grant Hernandez, Orlando Arias, Daniel Buentello, and Yier Jin, "Smart Nest Thermostat: A smart spy in your home," in *Black Hat USA*, 2014.

[38] CJ Heres, Amir Etemadieh, Mike Baker, and Hans Nielsen, "Hack all the things: 20 devices in 45 minutes," in *DEFCON*, 2014.

[39] Texas Instruments, "Smart E-Meter: AMR/AMI," http://www.ti.com/solution/docs/appsolution.tsp?appId=407.

[40] Texas Instruments, "Implementation of a three-phase electronic watt-hour meter using the msp430f677x(a)," *Application Report*, 2014.

[41] Yang Liu, Shiyan Hu, and Tsung-Yi Ho, "Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks," in *Proceedings of IEEE/ACM International Conference on Computer-Aided Design*, 2014.

[42] Chen Liao, Chee-Wooi Ten, and Shiyan Hu, "Strategic frtu deployment considering cybersecurity in secondary distribution network," *IEEE Transactions on Smart Grid*, vol. 4, no. 3, pp. 1264–1274, Sept 2013.

[43] Y. Jin and Daniela Oliveira, "Extended abstract: Trustworthy soc architecture with on-demand security policies and hw-sw cooperation," in *5th Workshop on SoCs, Heterogeneous Architectures and Workloads (SHAW-5)*, 2014.

[44] Daniela Oliveira, Jesus Navarro, Nicholas Wetzel, and Max Bucci, "Ianus: Secure and holistic coexistence with kernel extensions - a immune system-inspired approach," in *Proceedings of the 29th Annual ACM Symposium on Applied Computing*, 2014, SAC '14, pp. 1672–1679.

[45] Yang Liu, Shiyan Hu, and Tsung-Yi Ho, "Leveraging strategic defense algorithms for smart home pricing cyberattacks," in *under submission for journal review*.

[46] Yang Liu, Shiyan Hu, Jie Wu, Yiyu Shi, Yier Jin, Yu Hu, and Xiaowei Li, "Impact assessment of net metering on smart home cyberattack detection," in *accepted to IEEE/ACM Design Automation Conference (DAC)*, 2015.

[47] Dean Collins, "TRUST, A Proposed Plan for Trusted Integrated Circuits," [Online]: http://www.stormingmedia.us/.

[48] "TRUST in Integrated Circuits (TIC)," [Online]: http://www.darpa.mil/Our$_{W}ork/MTO/Programs/$.

[49] "National Cyber Leap Year Summit 2009: Co-Chairs Report," [Online]: https://www.nitrd.gov/.

[50] Savage T.S., "The implications of RoHS on active implantable medical devices," in *Reliability Physics Symposium (IRPS), 2011 IEEE International*, 2011, pp. 10–14.

[51] V. Buzduga, D.M. Witters, Jon P. Casamento, and W. Kainz,

"Testing the immunity of active implantable medical devices to cw magnetic fields up to 1 mhz by an immersion method," *Biomedical Engineering, IEEE Transactions on*, vol. 54, 2007.

[52] M. Rushanan, A.D. Rubin, D.F. Kune, and C.M. Swanson, "Sok: Security and privacy in implementable medical devices and body area network," in *IEEE Symposium on Security and Privacy*, 2014, pp. 524–539.

[53] G. Chen and E. Rodriguez-Villegas, "System-level design trade-offs for truly wearable wireless medical devices," in *Annual International Conference of the IEEE on Engineering in Medicine and Biology Society (EMBC), Buenos Aires*, 2010, pp. 1441–1444.

[54] Bureau of Industry and Security, "U.S. Department of Commence. Defense Industrial Base Assessment: Counterfeit Electronics," [Online]: http://www.bis.doc.gov/index.php, 2010.

[55] B. Grow and C.-C. Tschang and C. Edwards and B. Burnsed , "Dangerous Fakes," [Online]: http://www.businessweek.com/stories/2008-10-01/dangerous-fakes, 2008.

[56] L. W. Kessler and T. Sharpe , "Dangerous Fakes," [Online]: http://www.circuitsassembly.com/, 2010.

[57] J. Stradley and D. Karraker, "The electronic part supply chain and risks of counterfeit parts in defense applications," *IEEE Trans. on Components and Packaging Technology*, vol. 29, no. 3, pp. 703–705, 2006.

[58] H. Ke, J. M. Carulli, and Y. Makris, "Counterfeit electronics: A rising threat in the semiconductor manufacturing industry," in *International Test Conference (ITC)*, 2013, pp. 1–4.

[59] "HIPAA: Federal Health Insurance Portability and Accountability Act of 1996 ," [Online]: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.

[60] Networking, Information Technology Research, and Development (NITRD) Group, "High-confidence medical devices:cyber-physical systems for 21 century health care," .

[61] Z.E Ankarali., Q.H. Abbasi, A.F. Demir, E. Serpedin, K. Qaraqe, and H. Arslan, "A comparative review on the wireless implantable medical devices privacy and security," in *IEEE 2014 EAI International Conference on Wireless Mobile Communication and Healthcare (Mobihealth), Athens*, 2014, pp. 246–249.

[62] Senator Joe Lieberman, "National Security Aspects of the Global Migration of the U.S. Semiconductor Industry," .

[63] W.H. Maisel, "Safety issues involving medical devices: implications of recent implantable cardioverter-defibrillator malfunctions," *Journal of American Medical Assoc*, vol. 294, no. 8, pp. 955–958, 2005.

[64] K. Hu, A. N. Nowroz, S. Reda, and F. Koushanfar, "High-sensitivity hardware trojan detection using multimodal characterization," in *Design, Automation Test in Europe Conference Exhibition (DATE)*, 2013, pp. 1271–1276.

[65] R. Rad J. Aarestad, D. Acharyya and J. Plusquellic, "Detecting trojans though leakage current analysis using multiple supply pad iddqs," *IEEE Transactions on Information Forensics and Security*, vol. 5, pp. 893–904, 2010.

[66] wilcox.z.Ian, F. Saqib, and J. Plusquellic, "Gds-ii trojan detection using multiple supply pad vdd and gnd iddqs in asic functional units," in *IEEE International Symposium on Hardware-Oriented Security and Trust*, 2015.

[67] D. Forte, B. Chongxi, and A. Srivastava, "Temperature tracking: An innovative run-time approach for hardware trojan detection," in *International Conference on Computer-Aided Design (ICCAD)*, 2013, pp. 532–539.

[68] Y. Jin, N. Kupp, and Y. Makris, "Experiences in hardware Trojan design and implementation," in *IEEE International Workshop on Hardware-Oriented Security and Trust*, 2009, pp. 50–57.

[69] Jian Wan, Jianrong Wu, and Xianghua Xu, "A novel fault detection and recovery mechanism for zigbee sensor networks," in *IEEE Future Generation Communication and Networking FGCN*, 2008, pp. 270–274.

[70] M. Pooyan, M.R.N. Rad, and R. Kourdy, "Using mpls fault recovery mechanism and bandwidth reservation in network-on-chip," in *Computer and Automation Engineering (ICCAE)*, 2010, pp. 509 – 513.

[71] R Anderson and M Kuhn, "Tamper resistance - a cautionary note.," in *2nd USENIX Workshop On Electronic Commerce*, 1996, pp. 18–20.

[72] G Suh, D Clarke, B Gassend, M van Dijk, and S Devadas, "Aegis: Architecture for tamper-evident and tamper-resistant processing.," in *Int'l Conf. on Supercomputing (ICS)*, 2003, pp. 168–177.

[73] A.D. Wood and J.A. Stankovic, "Security of distributed, ubiquitous, and embedded computing platforms," in *Wiley Handbook of Science and Technology for Homeland Security*, 2010, p. 2888.

[74] A Perrig, R Szewczyk, V Wen, D Culler, and JD Tygar, "Aegis: Architecture for tamper-evident and tamper-resistant processing.," in *7th ACM Mobile Computing and Networks (MobiCom '01)*, 2001, pp. 189–199.

[75] C Karlof, N Sastry, and D Wagner, "Tinysec: A link layer security architecture for wireless sensor networks.," in *Second ACM Conference on Embedded Networked Sensor Systems (SensSys)*, 2004, pp. 162–175.

[76] J Deng, R Han, and S Mishra, "Safety issues involving medical devices: implications of recent implantable cardioverter-defibrillator malfunctions," *Elsevier Journal on Computer Communications*, vol. 29, no. 2, pp. 216–230, 2005.

[77] J. W. Lee, L. Daihyun, B. Gassend, G.E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *Symposium of VLSI Circuits*, 2004, pp. 176–179.

[78] Lang Lin, Dan Holcomb, D.K. Krishnappa, P. Shabadi, and W. Burleson, "Low-power sub-threshold design of secure physical unclonable functions," in *Low-Power Electronics and Design*, 2010, pp. 43 – 48.

[79] G. Qu and C. Yin, "Temperature-aware cooperative ring oscillator puf," in *Workshop on HardwareOriented Security and Trust*, 2009, pp. 36–42.

[80] A. Maiti and P.Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *Conference on Field Programmable Logic and Applications*, 2009, pp. 703–707.

[81] M. Majzoobi, F. Koushanfar, and S. Devadas, "Fpga puf using programmable delay lines," in *Conference on Field Programmable Logic and Applications*, 2010, pp. 1–6.

[82] C. Bohm, M. Hofer, and W. Pribyl, "A microcontroller sram-puf," in *Conference on Network and System Security*, 2011, pp. 25–30.

[83] D. Ganta, V. Vivekraja, K. Priya, and L. Nazhandali, "A highly stable leakage-based silicon physical unclonable functions," in *VLSI Design (VLSI Design), International Conference on*, 2011, pp. 135 – 140.

[84] M. Majzoobi, Golsa Ghiaasi, F. Koushanfar, and S.R. Nassif, "Ultra-low power current-based puf," in *Circuits and Systems (ISCAS), IEEE International Symposium on*, 2011, pp. 2071 – 2074.

[85] F. Saqib, M. Areno, J. Aarestad, and J. Plusquellic, "An asic implementation of a hardware-embedded physical unclonable function," *IET Computers and Digital Techniques*, vol. 8, pp. 288–299, 2014.

[86] A. Maiti and P. Schaumont, "A novel microprocessor-intrinsic physical unclonable function," in *Field Programmable Logic and Applications*, 2012, pp. 380–387.

[87] W. Che, S. Bhunia, and J. Plusquellic, "A non-volatile memory based physically unclonable function without helper data," in *International Conference on Computer-Aided Design*, 2014.