Emerging Challenges in Cyber-Physical Systems: A Balance of Performance, Correctness, and Security

Kelvin Ly, Wei Sun, and Yier Jin
Department of Electrical and Computer Engineering
University of Central Florida
rangertime@knights.ucf.edu, sun@ucf.edu, yier.jin@eecs.ucf.edu

***Abstract*—Cyber-physical sytems (CPS) has seen an expanding implementation in our society facilitating various services from smart grids to smart vehicle network. While traditional criteria in industrial networks and controlling systems are still valid for the emerging CPS, new challenges need to be addressed for the development of future CPS including security, correctness, and resource constraints. These challenges are further elaborated in a case study of modern power grids to demonstrate the impact of such problems and possible solutions.**

I. Introduction

Research relating to cyber-physical systems (CPS) has recently drawn the attention of those in academia, industry, and the government because of the wide impact CPS has on society, the economy, and the environment [1]. Though still lacking a formal definition, cyber-physical systems are largely referred to as the next generation of systems that integrate communication, computation, and control in order to achieve stability, high performance, robustness, and efficiency as it relates to physical systems [2]. More concisely, CPS is also defined as an emerging class of systems that closely couple components of both the physical and cyber world [3]. These systems generally involve the interaction of many interconnected smart devices that may provide sensor data and/or affect the physical system through actuators.

While ongoing research still focuses on traditional criteria, combining a large amount of embedded (often smart) devices with network connections has already resulted in new challenges to CPS development. Among all of these challenges, security concerns are a leading example which has been largely ignored in CPS construction [1]. Cyber-physical systems are in the process of being widely integrated into various critical infrastructures, however given the lack of countermeasures, security breaches could have catastrophic consequences. For example, if communication channels within a power grid are compromised, the whole power grid may become unstable, possibly causing a large-scale cascaded blackout. The emergence of smart grids may further complicate the problem if security is not considered during the smart grid construction process [4]. In fact, the first cyber attack on a national-level power grid has been reported recently [5].

Correctness is another challenge when the CPS systems evolve from large-scale to exascale. The interconnections among all underlying devices and the interconnections between end nodes and the central controller (or the cloud) make it challenging to ensure the correctness of the whole system. New requests rise on how to balance performance overhead and the deployment of correctness checking nodes. The exascale deployment of CPS also raises the problem of total cost. Therefore, end nodes are often equipped with limited resources to save cost. As a result, research has been done in two directions: 1) improve the device calculation efficiency through hardware-software co-optimization; 2) reduce the workload from individual nodes and put the calculation on server side. Figure I shows the overview of technologies involved in cyber-physical systems.

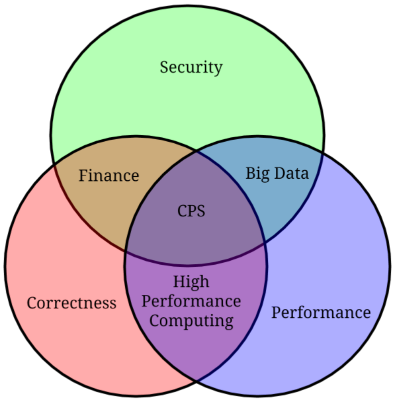

Fig. 1. An overview of the technologies involved in cyber-physical systems

The rest of the paper will discuss these emerging challenges as follows: Section II discusses the security challenges in modern CPS. Section III introduces the problem of correctness in exascale CPS deployment and possible solutions. The problem of resource constraints is briefly introduced in Section IV. A case study on power grid security and resilience is elaborated in Section V. Finally, conclusions are drawn in Section VI.

II. Security

Security has grown to become a major concern in most computing applications. However, it takes a more urgent tone in the field of CPS, where a lack of security has real consequences on the physical security of the system. Security in CPS is complicated by the fact that many CPS devices have lower performance than conventional computing devices, leaving a smaller performance margin within which security and cryptography can be implemented. Security of

978-1-4673-9955-5/16/$31.00 ©2016 IEEE

embedded devices has been examined in every section of the software/hardware stack, from the analysis of network traffic and run time of tasks on CPS devices down to the development of microcontroller extensions to heighten security.

Work on securing the software in CPS can be divided into three main categories, ways to ensure proper program functioning, the development of new secure operating systems running within the performance bounds of CPS devices, and ensuring data integrity. Each of these approaches act mostly orthogonally with the others, allowing a combination of these ideas to be used together to provide the greatest amount of security.

The first category attempts to find ways to validate proper code behavior, most commonly by measuring some metric of the code before it is exploited or modified by the attacker, and detecting an attack by noticing a change in that metric after it is modified by the attacker. Robert Mitchell and Ing-Ray Chen provide an overview of this field, noting that there are many parallels with information and communication technologies that may be useful for further development of this field [6]. For one example, Zimmer et al examine the use of fine and coarse grained execution timings to detect any malicious changes in program software [7].

CPS devices traditionally run either bare metal or on top of a real-time operating system, because the hardware platforms they run on were designed to perform just well enough to provide enough performance to work at the lowest possible price, and consequently a high performance and low overhead operating system was needed. Now that security in CPS is beginning to be examined seriously, new hardened operating systems are beginning to be designed with the low overhead needs of CPS in mind. TyTAN is one example of this new generation of operating systems, being hard real-time while providing security features such as isolated memory and secure tasks while having only 15% overhead over traditional real-time operating systems [8]. Qduino is another example, where the Arduino runtime and API are adapted to work efficiently in multicore environments [9].

Data integrity is resolved through similar cryptographic methods as in traditional hardware, but the limitations of CPS device performance requires more thought into the tradeoffs between computation cost and cryptographic strength. For instance, Xu et al have collaborated to develop a certificateless signing scheme that outperformed prior attempts at certificateless signing, and consequently made it practical to use on CPS devices [10]. Newer, more lightweight ciphers are also being developed, where the goal is to reduce the complexity of the software or hardware needed to implement it without overly compromising cryptographic security. PRESENT is one example of one such cipher suite, and its performance on reconfigurable hardware has been examined [11].

Hardware modifications are a somewhat rarer approach, as hardware modification inevitably entails cost, which is counter to their use in industry, especially in a field such as CPS where low costs are one of the major factors to its success. However, papers have been developed around the premise of using an FPGA in the device, which would reduce the modification cost substantially, or around instruction set modification to improve device security in general. Peterson and Farag produced an FPGA security scheme that monitored untrusted FPGA modules to stop them if they violated any features of their interface contracts with other components [12]. Chilivuri et al produced a similar scheme, called TAIGA, that works on a higher level by monitoring the network I/O and ensuring the physical plant was behaving correctly, while also providing the criteria for producing a trustable hardware module [13]. SMART is another hardware modification, providing a method for verifying the correct execution of code on a microcontroller [14].

III. Correctness

The correctness of CPS has been the traditional focal point of CPS research. As these systems become larger and are allowed more automation with less human oversight, the need to ensure proper functioning under all conditions becomes ever more paramount. The main focus appears to be on the ideas of contract programming and the generation of code from formally verified models, or the use of formal verification on existing code.

Contract based design, where the system is designed with an emphasis on ensuring contracts at the interfaces between devices, appears to be a major topic of research in the field of CPS design, led primarily by the CPS group in Berkeley. They have examined the efficacy of such an approach in safety-crucial portions of CPS design, and have also developed proof systems to verify that the contracts are providing the expected safety guarantees [15] [16]. Nuzzo and Sangiovanni-Vincentelli provide an excellent overview of the use of formal contracts in CPS design, focusing on the most commonly used formally verifiable form known as assume-guarantee contracts [17]. One recent practical application of contracts in design is SafetyADD, which was developed in 2014. SafetyADD allows contracts and guarantees to be automatically checked during the design of system and acts as an extension of Eclipse [18].

Berkeley has also developed a modelling framework called Ptolemy II, which is meant to model concurrent systems in general, and there has success in using this model to work on CPS systems [19] [20]. The model supports a wide variety of programming paradigms, allowing it to be used effectively in the multidomain systems prevalent in CPS design.

Generating code from models has also become a big area of research to ensure the safety of CPS devices. The use of models often allows failures that would be revealed far later during integration to be found much earlier through simulation [21]. Models are commonly used to simulate different parts of complicated designs to verify the integration of the whole design, and consequently being able to use the model itself to generate the logic would improve the overall reliability of the code. One example is of Farag's use of CoRaL, a cognitive radio policy language, to generate HDL code that would create a module that followed those policies [22]. Ptolemy II has been translated into multicore Java code by Telez and Pla [23]. A less extreme approach that is also gaining traction is the use of models to generate test cases with which to test code.

Formal verification appears to be a widespread approach towards verifying the design of highly critical components. There are many papers published showing the verification of components as diverse as automobile gearbox shifters, microcontrollers, and train controls [24] [25] [26]. This field tries to prove either that the component is working correctly, or that it will work fast enough to meet its execution time requirements. Kumar et al has contributed to the latter, providing a methodology that allows for more accurate timing proofs [27].

IV. Physical constraints

Being embedded devices, CPS devices are often constrained in time, energy, and performance due to their use of low cost computing units in environments where quick response is vital and where power often comes from a small battery. Thus, CPS design shares the same challenges as embedded system design, i.e. determining the appropriate trade offs between these three quantities. However, this is not as large a field of research as the others discussed, because many of these challenges are already being worked on in embedded systems research and industry, and the problem of performance itself will somewhat rectify itself with time due at least in part to Moore's law. Most research fits into the above categories, where the challenge is in fitting the software to the available hardware rather than attempting to improve the hardware itself.

One of the most defining features of CPS is their need for real-time systems. Not all CPS require hard real-time to function, but many do due to how they form part of a feedback loop that requires reliable sensing or actuation to function in a reliably stable manner. Consequently, the development of low overhead real-time operating systems capable of running on the small memory spaces and slow processors commonly used in CPS devices is an important point of research. TyTAN is a good example of research in this direction [8].

V. Cyber-physical security and resilience of power grid

As a critical infrastructure, the electric power grid is required for almost all business and consumer activities. The electric power critical infrastructure supports all 17 other critical infrastructures and is required for almost all business and consumer activities. The emerging smart grid concept introduces more cyber components into the existing power grid for billing, monitoring, and control [28]. Smart grids leverage advanced information and communication technologies to improve the reliability and efficiency of power systems. This increased cyber dependency brings higher risks from cyber-attacks which could have catastrophic consequences, thus making it of vital importance to secure the grid. This challenge is interdisciplinary in nature, requiring knowledge of electrical engineering as well as computer science, computer networking, and cyber security [29].

With the development of communication technologies and advanced information in power systems, cyber parts and physical power systems construct a complicated cyber-physical power system that can ensure higher reliable power supplies to customers. However, some devices may be out of service due to malicious cyber-attacks. Cyber-attacks have increased dramatically over the last decade, exposing sensitive information, disrupting critical operations, and imposing high costs on economy. Under cyber-attacks, emergency controls, e.g., load shedding and system separation, should be performed to guarantee the steady-state and transient stability [30] [31]. After cyber-attack, if the emergency control cannot maintain power system integrity or several electrical islands are formed, restoration strategy will assist system operators to return the system to normal operating conditions [32] [33].

In the smart grid, there are emerging challenges, as well as new definitions of cyber-physical vulnerability, security, and resilience.

Vulnerability: Physical vulnerabilities focus on the disruption of transmission and distribution lines, transformers, and other equipment. And power grid components' communication abilities and information technologies result in more cyber vulnerabilities. Cyber-attacks can be classified into reconnaissance, denial of service, command injection, and measurement injection [34] [35]. The link between physical and cyber components in power grid, e.g., supervisory control and data acquisition (SCADA) systems, intelligent electronic devices (IEDs), advanced metering infrastructure (AMI), distributed energy resource (DER) control systems, bring more cyber-physical vulnerabilities from cyber-attacks to cause physical damage to power grid components.

Security: Power grid security is defined as the risk of the ability to survive disturbances without interruption of customer service [36]. The cyber-security of SCADA and AMI has been investigated by many power researchers [37] [38] [39]. However, more research is desired in the intelligent detection of cyber-physical disturbance and the impact analysis of IEDs and DER on cyber-physical security [35].

Resilience: Power system resilience focuses on the ability to anticipate, absorb, and rapidly recover from a disturbance or extreme event (natural disaster, cyber-attack, etc.). To compare with another important power system index – reliability, the cyber-physical resilience looks at the high-impact and low-probability event, evaluates power system states and transition times between states, and also concerns with customer interruption time and the infrastructure recovery time [30]. Cyber-physical resilience assessment is based on risk assessment, but takes it one step further by quickly reacting to damage and attacks with the goal of maintaining system functionality [35].

To enhance the cyber-physical security and resilience of power grid, a strategic defense and recovery systems using smart grid technology would be of great interest to power grids and other critical infrastructures. This system should provide the following functions: 1) *Prevention*: identifying vulnerable cyber components is the key to preventing potential cyber-attacks. The vulnerability of major cyber components in smart grids can be assessed, and the resulting impact will be quantified by a vulnerability index composed of system voltage and frequency stability, as well as islanding and recovery time. 2) *Detection*: the intrusion detection algorithm exploiting the phasor measurement units (PMUs) data can be designed to monitor malicious activities. 3) *Mitigation*: different control actions could be considered to protect the system, including, generation rescheduling, system topology reconfiguration, isolation, and controlled system separation. 4) *Restoration*: An adaptive restoration tool can be developed to guide system operators to restore attack-affected area back to the normal condition reliably and efficiently.

VI. Conclusion

In this paper, we discussed three emerging challenges of the modern cyber-physical systems. A case study on power grids is also discussed to introduce the impact of these problems and the possible solutions. The paper will serve as a starting point for CPS researchers to better understand the new challenges and to develop more efficient CPS balancing performance, correctness and security.

Acknowledgement

This work was supported in part by the Florida Cybersecurity Center (FC2) 2015 Collaborative Seed Grant Program and the Southeastern Center for Electrical Engineering Education (SCEEE 15-001).

References

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

[2] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, “Cyber-physical systems: The next computing revolution,” in *Proceedings of the 47th Design Automation Conference*, ser. DAC ’10, 2010, pp. 731–736.

[3] S. Khaitan and J. McCalley, “Design techniques and applications of cyberphysical systems: A survey,” *Systems Journal, IEEE*, vol. 9, no. 2, pp. 350–365, 2015.

[4] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, and Y. Jin, “Cyber-physical systems: A security perspective,” in *Test Symposium (ETS), 2015 20th IEEE European*, 2015, pp. 1–8.

[5] K. Zetter, “Everything we know about the ukraine’s power plant hack,” *Wired*, 2016, [Online]. http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

[6] R. Mitchell and I.-R. Chen, “A survey of intrusion detection techniques for cyber-physical systems,” *ACM Comput. Surv.*, vol. 46, no. 4, pp. 55:1–55:29, Mar. 2014.

[7] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, “Intrusion detection for cps real-time controllers,” in *Cyber Physical Systems Approach to Smart Electric Power Grid*, ser. Power Systems. Springer Berlin Heidelberg, 2015, pp. 329–358.

[8] F. Brasser, B. El Mahjoub, A.-R. Sadeghi, C. Wachsmann, and P. Koeberl, “Tytan: Tiny trust anchor for tiny devices,” in *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, 2015, pp. 1–6.

[9] Z. Cheng, Y. Li, and R. West, “Qduino: A multithreaded arduino system for embedded computing,” in *Real-Time Systems Symposium (RTSS), 2015 IEEE*, 2015, pp. 261–272.

[10] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai, and W. Shu, “A certificateless signature scheme for mobile wireless cyber-physical systems,” in *Distributed Computing Systems Workshops, 2008. ICDCS ’08. 28th International Conference on*, June 2008, pp. 489–494.

[11] J. Pospiil and M. Novotny, “Evaluating cryptanalytical strength of lightweight cipher present on reconfigurable hardware,” in *Digital System Design (DSD), 2012 15th Euromicro Conference on*, Sept 2012, pp. 560–567.

[12] M. M. Farag, “Architectural enhancements to increase trust in cyber-physical systems containing untrusted software and hardware,” Ph.D. dissertation, 2012, aAI3585744.

[13] N. T. Chiluvuri, O. A. Harshe, C. D. Patterson, and W. T. Baumann, “Using heterogeneous computing to implement a trust isolated architecture for cyber-physical control systems,” in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, ser. CPSS ’15. ACM, 2015, pp. 25–35. [Online]. Available: http://doi.acm.org/10.1145/2732198.2732199

[14] K. Eldefrawy, A. Francillon, D. Perito, and G. Tsudik, “SMART: Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust,” in *NDSS 2012, 19th Annual Network and Distributed System Security Symposium, February 5-8, San Diego, USA*, San Diego, UNITED STATES, 02 2012. [Online]. Available: http://www.eurecom.fr/publication/3536

[15] P. Nuzzo, J. Finn, A. Iannopollo, and A. Sangiovanni-Vincentelli, “Contract-based design of control protocols for safety-critical cyber-physical systems,” in *Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, March 2014, pp. 1–4.

[16] A. Cimatti and S. Tonetta, “A property-based proof system for contract-based design,” in *Software Engineering and Advanced Applications (SEAA), 2012 38th EUROMICRO Conference on*, Sept 2012, pp. 21–28.

[17] P. Nuzzo and A. Sangiovanni-Vincentelli, *From Programs to Systems. The Systems perspective in Computing: ETAPS Workshop, FPS 2014, in Honor of Joseph Sifakis, Grenoble, France, April 6, 2014. Proceedings*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, ch. Let’s Get Physical: Computer Science Meets Systems, pp. 193–208. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-54848-2_13

[18] F. Warg, B. Vedder, M. Skoglund, and A. Soderberg, “Safety add: A tool for safety-contract based design,” in *Software Reliability Engineering Workshops (ISSREW), 2014 IEEE International Symposium on*, Nov 2014, pp. 527–529.

[19] J. Eker, J. Janneck, E. Lee, J. Liu, X. Liu, J. Ludvig, S. Neuendorffer, S. Sachs, and Y. Xiong, “Taming heterogeneity - the ptolemy approach,” *Proceedings of the IEEE*, vol. 91, no. 1, pp. 127–144, Jan 2003.

[20] A. Kanduri, A.-M. Rahmani, P. Liljeberg, K. Wan, K. L. Man, and J. Plosila, “A multicore approach to model-based analysis and design of cyber-physical systems,” in *SoC Design Conference (ISOCC), 2013 International*, Nov 2013, pp. 278–281.

[21] A. Sangiovanni-Vincentelli, W. Damm, and R. Passerone, “Taming dr. frankenstein: Contract-based design for cyber-physical systems*,” *European Journal of Control*, vol. 18, no. 3, pp. 217 – 238, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0947358012709433

[22] M. M. Farag, “Architectural enhancements to increase trust in cyber-physical systems containing untrusted software and hardware,” Ph.D. dissertation, Blacksburg, VA, USA, 2012, aAI3585744.

[23] A. Tellez and M. Pla, “Multithreaded translation of ptolemy ii designs on multicore platforms,” in *Complex, Intelligent and Software Intensive Systems, 2008. CISIS 2008. International Conference on*, March 2008, pp. 607–612.

[24] H. Chen and S. Mitra, “Synthesis and verification of motor-transmission shift controller for electric vehicles,” in *ICCPS ’14: ACM/IEEE 5th International Conference on Cyber-Physical Systems (with CPS Week 2014)*, ser. ICCPS ’14. Washington, DC, USA: IEEE Computer Society, 2014, pp. 25–35.

[25] J. Espinosa, C. Hernandez, J. Abella, D. de Andres, and J. Ruiz, “Analysis and rtl correlation of instruction set simulators for automotive microcontroller robustness verification,” in *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, June 2015, pp. 1–6.

[26] A. Platzer and J.-D. Quesel, “European train control system: A case study in formal verification,” in *Formal Methods and Software Engineering*, ser. Lecture Notes in Computer Science, K. Breitman and A. Cavalcanti, Eds. Springer Berlin Heidelberg, 2009, vol. 5885, pp. 246–265.

[27] P. Kumar, D. Goswami, S. Chakraborty, A. Annaswamy, K. Lampka, and L. Thiele, “A hybrid approach to cyber-physical systems verification,” in *Design Automation Conference (DAC), 2012 49th ACM/EDAC/IEEE*, June 2012, pp. 688–696.

[28] Y. Mo, T.-H. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, “Cyber-physical security of a smart grid infrastructure,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, Jan 2012.

[29] W. Wang and Z. Lu, “Survey cyber security in the smart grid: Survey and challenges,” *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2012.12.017

[30] C.-W. Ten, G. Manimaran, and C.-C. Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling,” *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 40, no. 4, pp. 853–865, July 2010.

[31] C.-W. Ten, C.-C. Liu, and G. Manimaran, “Vulnerability assessment of cybersecurity for scada systems,” *Power Systems, IEEE Transactions on*, vol. 23, no. 4, pp. 1836–1846, Nov 2008.

[32] W. Sun, C.-C. Liu, and L. Zhang, “Optimal generator start-up strategy for bulk power system restoration,” *Power Systems, IEEE Transactions on*, vol. 26, no. 3, pp. 1357–1366, Aug 2011.

[33] Y. Hou, C.-C. Liu, K. Sun, P. Zhang, S. Liu, and D. Mizumura, “Computation of milestones for decision support during system restoration,” *Power Systems, IEEE Transactions on*, vol. 26, no. 3, pp. 1399–1409, Aug 2011.

[34] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, “Modeling cyber-physical vulnerability of the smart grid with incomplete information,” *Smart Grid, IEEE Transactions on*, vol. 4, no. 1, pp. 235–244, March 2013.

[35] R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili, “On the definition of cyber-physical resilience in power systems,” *CoRR*, vol. abs/1504.05916, 2015. [Online]. Available: http://arxiv.org/abs/1504.05916

[36] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, and V. Vittal, “Definition and classification of power system stability ieee/cigre joint task force on stability terms and definitions,” *Power Systems, IEEE Transactions on*, vol. 19, no. 3, pp. 1387–1401, Aug 2004.

[37] F. Cleveland, “Cyber security issues for advanced metering infrasttructure (ami),” in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, July 2008, pp. 1–5.

[38] C. Neuman and K. Tan, “Mediating cyber and physical threat propagation in secure smart grid architectures,” in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, Oct 2011, pp. 238–243.

[39] Z. Vale, H. Morais, P. Faria, H. Khodr, J. Ferreira, and P. Kadar, “Distributed energy resources management with cyber-physical scada in the context of future smart grids,” in *MELECON 2010 - 2010 15th IEEE Mediterranean Electrotechnical Conference*, April 2010, pp. 431–436.