Design Methodologies for Securing Cyber-Physical Systems

Mohammad Al Faruque
Dept. of Electrical Engineering & Computer Science
University of California
Irvine, CA, USA
alfaruqu@uci.edu

Francesco Regazzoni
ALaRI Institute
University of Lugano
Lugano, Switzerland
regazzoni@alari.ch

Miroslav Pajic
Dept. of Electrical and Computer Engineering
Duke University
Durham, NC, USA
miroslav.pajic@duke.edu

ABSTRACT

Cyber-Physical Systems (CPS) are in most cases safety- and mission-critical. Standard design techniques used for securing embedded systems are not suitable for CPS due to the restricted computation and communication budget available in the latter. In addition, the sensitivity of sensed data and the presence of actuation components further increase the security requirements of CPS. To address these issues, it is necessary to provide new design methods in which security is considered from the beginning of the whole design flow and addressed in a holistic way. In this paper, we focus on the design of secure CPS as part of the complete CPS design process, and provide insights into new requirements on platform-aware design of control components, design methodologies and architectures posed by CPS design. We start by discussing methods for the multi-disciplinary modeling, simulation, tools, and software synthesis challenges for CPS. We also present a framework for design of secure control systems for CPS, while taking into account properties of the underlying computation and communication platforms. Finally, we describe the security challenges in the computing hardware that is used in CPS.

1. INTRODUCTION

Cyber-Physical Systems (CPS) feature tight integration of computational nodes, communication networks, and physical environment that might include human users. CPS have to fulfill a number of strict requirements in terms of power and energy consumption, while providing real-time interaction with (i.e., control of) the physical world using reduced communication and computation resources. Nevertheless, the sensitivity of sensed data and the presence of actuation components further increase the security requirements of CPS. Standard design techniques used for securing embedded systems are not suitable for CPS, due to the constrained computation and communication budget available in the latter. To address these issues, we require a new design approach in which security is considered from the beginning of the whole design flow and addressed in a holistic way.

Recently, there have been high-profile attacks against CPS, exploiting the tight integration between physical, computational, and networking aspects of CPS, and illustrating vulnerabilities of these systems. In [24, 12], several simple methods to disrupt the operation of a vehicle were presented. Additional incidents that have raised the attention about security problems in CPS, include Maroochy Water incident [49] and Stuxnet virus attack on a SCADA system used in industrial processes control [13, 25, 14]. Furthermore, recent studies have found that a large number of widely-used software based medical devices have been compromised [52]. For example, in a VA hospital a virus infected 104 medical devices such as X-rays, causing interruption of patient care [61]. Also, methods to perform attacks on a widely used glucose monitoring and insulin delivery system [26] and attack vectors on a networked PCA pump in a system of interoperable medical devices [53] have been reported.

In this paper, we address the issues related to the design of secure CPS. Existing methods for securing embedded systems have proven to not be completely effective in this domain. For instance, recent attacks demonstrated that considering security as an afterthought has not been the best way to address physical attacks, such as sensor spoofing; recent examples include GPS spoofing attacks to misguide a yacht off route [2], while [59, 16, 55] present steps and equipment required for GPS spoofing.

It is thus of crucial importance that designers of future CPS are aware of the most important security challenges which needs to be addressed during the design. In addition, they have to have the proper basic blocks and tools to solve them in a correct and reliable way. We describe the main challenges and opportunities related to security of CPS and provide an updated overview of design tools, methodologies, and basic blocks currently used to address them. Note that we present the design of secure CPS as part of the complete design process for CPS, in order to provide a better insight into the new requirements on platform-aware design of control components, design methodologies and architectures posed by CPS design.

Specifically, we start by discussing challenges in the multi-disciplinary modeling, simulation, tools, and software synthesis for secure CPS (Section 2). We then present a design framework for secure control of CPS, which takes into account properties of the underlying computation and com-

munication platforms. Finally, we describe the security challenges in the computing hardware used in CPS.

2. FUNCTIONAL LEVEL DESIGN FOR SECURITY

The increasing deployment of software and communication is making CPS more vulnerable to cyber attacks [21, 42]. However, there lacks the design automation support for the CPS security. For this reason, researchers are currently trying to solve the CPS security challenge at the system level. In [60], the authors propose a Model-Based Design (MBD) method to assess the security of CPS with four architecture-level attack models. Authors in [34] have discussed a MBD technique to quantify the security metrics at the early design stage. Some researchers have proposed and used graph-based modeling methods to solve many security problems. Authors in [62] have proposed a systematic method for analyzing cyber-attacks on CPS using an extended Data Flow Diagram (xDFD) approach. Lastly, in [31] the authors have offered an attack tree-based approach for system level security design. Unfortunately, the majority of these existing approaches to CPS security are limited to modeling the software used in security analysis. For this reason, the group at UCI has proposed a design automation model and tool to formulate and solve the security problem(s) before the system is built.

The work proposed by the UCI group exploits the observation that identifying and fixing problems at the early stages is economically beneficial. They proposes to formulate the security problem *before* the system is built. They model cybersecurity attacks and countermeasure functionalities using a novel *security-aware functional modeling* language implemented in the commercial design and simulation tools. And they create a design automation tool that uses simulation to validate cybersecurity vulnerabilities at the system-level.

Existing functional models include two types of functions: physical and cyber [9, 10, 11, 57]. Functions interact with each other through energy, material, and signal flows. These flows carry real physical and cyber properties such as mechanical, electrical, thermal energy, and data. Thus, existing functional models naturally *leak* information that can be used to attack the system via the signal flows in the cyber domain or energy/material flows in the physical domain. The UCI group extends the functional modeling concept with cybersecurity functions. Their proposed *security-aware functional models* provide the means to both analyze the effect of cybersecurity attack functions on the system, and refine the design using cybersecurity countermeasure functions.

An example of a security aware functional model for a car is shown in Figure 1. In this example, both cyber and physical attacks are modeled. The blue arrows in the flows represent the cyber attack vectors, while the red arrows represent the physical attack vectors. The purpose of the analysis is to quantify the effects of these attacks to the `Export TME` function that maps to the velocity of the car. In other words, we want to determine if the velocity controls are vulnerable to any cyber physical attacks.

In order to evaluate the security level of the `Export TME` function, we simulate the model and analyze the impact of the attack at the system-level. This step is important to identify functions that are vulnerable to attacks. These low-security functions can then be protected by refining the functional model and adding cybersecurity countermeasure functions. This iterative approach facilitates the analysis of different scenarios. An important benefit of the iterative approach is that more complex scenarios can be modeled.

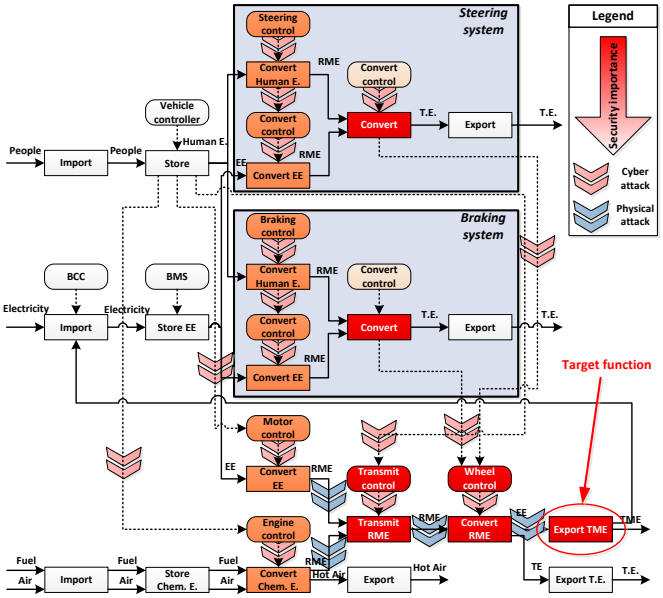

Figure 1: Security aware functional level model of automotive [58].

From the analysis of this security-aware functional model, a system-level simulation model can be directly generated using the synthesis technology provided in the existing works [9, 10, 11, 57].

To validate the presented methodology, we implemented a design automation tool using commercial off-the-shelf software as shown in Figure 2. Taking advantage of its subsystem libraries, we utilized Amesim to model the system functions (multi-physics), cybersecurity functions, and scenarios (e.g., environmental conditions). In addition, we used Matlab/Simulink for its mathematical capabilities to model the cybersecurity attacks. Six types of attack models are integrated in our current design automation tool.

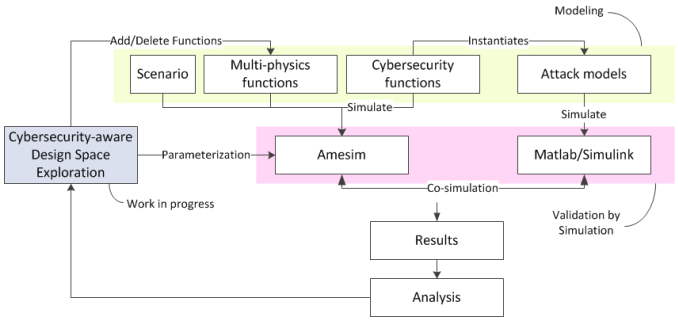

Figure 2: The design automation tool developed by the UCI group [58].

To demonstrate the proposed design automation tool and the attack models during the early design stage, we used the design of an Electric Vehicle (EV) as a case study . We

instantiate an attack model interface using an attack model from the library and insert it between the motor and the motor-controlling ECU. Figure 3, we see that the fuzzy attack successfully destabilizes the motor behavior by adding noise to the control signals.

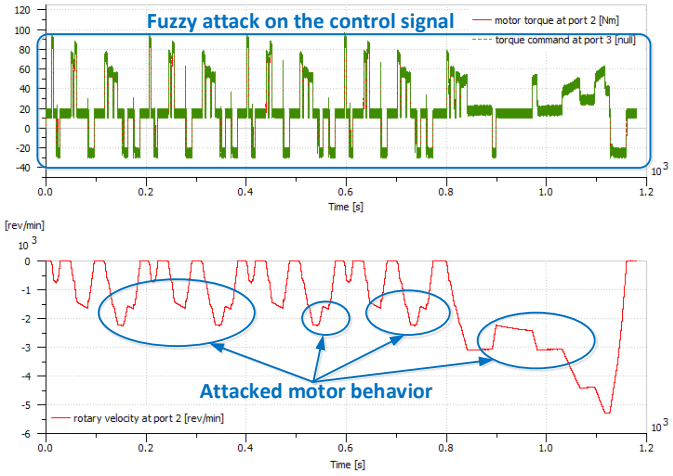

Figure 3: Simulation results with the proposed attack models.

In this work, the UCI group developed a functional model to analyze security challenges during the early design stage. In the future, the UCI group will explore the capability of the functional model to not only help the security analysis, but also to automatically generate/synthesize system-level simulation models in response to the analysis. Moreover, for demonstration purposes, they included six different attack models in their library but in the future, they may develop additional attack models that can capture both cyber and physical domain attacks. Lastly, the group plans on developing security cost metrics to integrate with the proposed security-aware functional models.

3. PLATFORM-AWARE CONTROL DESIGN FOR SECURE CPS

There is a need to change the way we reason about control in CPS, and to start designing attack-resilient control schemes and architectures capable of dealing with cyber-physical attacks on the environment of the controller (e.g., sensors, actuators, and communication media). Recent attacks on control component of CPS have clearly revealed that relying exclusively on cyber-security techniques for securing CPS is insufficient. Consequently, they have spanned research into control-level techniques that address the problem of state estimation and intrusion detection under attacks on the environment of the controller, i.e., attacks on sensors, actuators and communication networks (e.g., [50, 54, 39, 15, 51, 35, 18, 17, 30, 29]).

In this section, we present recent efforts by the Duke research group, to exploit the knowledge of the system dynamics for attack-resilient control of CPS. The goal of our work has been to develop tools and techniques to ensure that CPS maintain a degree of control even when the system is under cyber and/or physical attack.

We propose adding security-awareness to the control system design that allows control systems to recover the information about the state of the controlled process despite the attacks. Our approach to building attack-resilient control systems is to combine secure-detection and attack-identification with added logical redundancy in system design (see Figure 4). Here, we assume that control design for no-attack case has been developed and concentrate on techniques for state estimation and sensor fusion under external attacks. Note that since previously developed methods for attack-resilient state estimation (e.g., [15, 39, 48]) require the unpractical assumption of the exact knowledge of the controlled plant's dynamics, resilience-to-attack guarantees do not hold when these assumptis are violated.

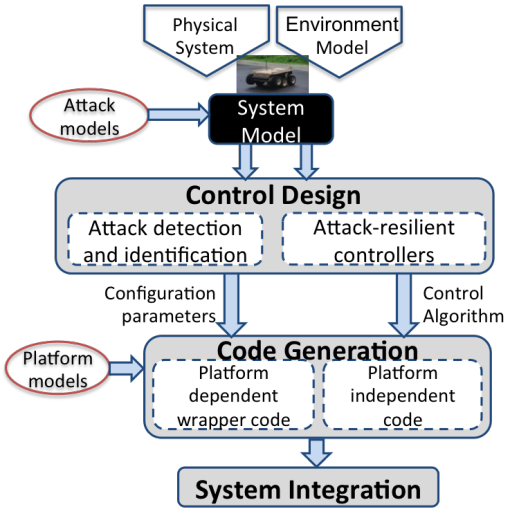

Figure 4: The proposed design framework for secure control of cyber-physical systems.

From the perspective of controlling CPS, the main idea has been to exploit knowledge of the system's dynamics for state estimation and attack detection and identification in the presence of sensor and actuator attacks and attacks on control resources. For instance, in [37], we introduced a method for attack-resilient state estimation for systems with modeling errors and illustrated its use on a real-world case study – design of attack-resilient cruise control on an unmanned ground robot (Figure 5(a)). To obtain the state of a controlled physical process when the attacker compromises system sensors and actuators, we introduced an Integer Programming (IP) based procedure that utilizes a window of previous sensor measurement vectors and (limited) knowledge of the system's dynamics.

Furthermore, we showed how to capture effects of the utilized computation and communication platforms on the accuracy of the dynamical model and described how implementation issues including jitter, latency, and synchronization errors can be captured by the model. This has allowed for the mapping of attack-resilient control objectives into real-time performance requirements from the utilized platform, which facilitates reasoning about attack-resilience across different implementation layers as illustrated in Figure 5(b).

As shown in [24, 12], the lack of understanding between control design assumptions and system implementation can be heavily exploited to compromise system's functionality. For example, by changing scheduling sequence for control and sensing actions/computations, we could dramatically

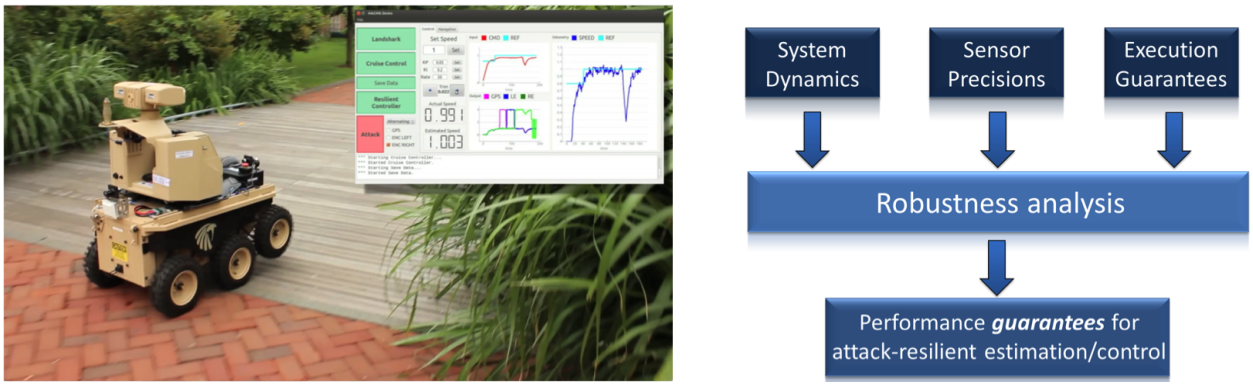

Figure 5: (a) The LandShark ground robot running attack-resilient cruise control, (b) Zoomed on Z3 execution times for verification of TF invariants – note that this approach does not scale well because controllers with size greater than two can not be verified with this type of invariants.

affect the stability and safety of the controlled process [33]. Consequently, to facilitate design of secure control for CPS we have developed *a framework for cross-layer analysis of platform effects on security* properties of employed control algorithms. For illustration, in time-triggered architectures [23] we can rigorously quantify the modeling and performance gap between the model-level semantics of linear dynamic controllers and their implementation-level semantics [33]. Thus, we could analyze the effect and provide performance guarantees when a malicious adversary imposes the worst computing sequence from control's perspective. In [17, 19] we reported preliminary work on this topic, focused on impacts of communication schedule on attack-resilient sensor fusion when the system model is not known. In addition, we proposed methods for attack-detection and identification for more complex system models. For example, motivated by sensor fault models in some CPS applications (e.g., GPS) we considered attack-resilient sensor fusion that exploits knowledge of temporal sensor fault-models without conservatively treating them as compromised [38].

Finally, in the context of CPS, resource constraints might impose an insurmountable obstacle for the use of developed control techniques. Hence, it is necessary to provide non-optimal methods for attack-resilient control with formal resilience guarantees. For example, in [36] we show how to exploit techniques from compressed sensing to investigate conditions that will enable the use of convex estimators for attack-identification while providing formal resiliency guarantees. Note that since extracting accurate-enough dynamical models for some CPS (e.g., patient modeling in Medical CPS) is quite challenging (if at all possible), there are limitations to the use of *model-driven methods for attack-resilient control*. To overcome this weakness, an avenue of our future work is on *data-driven methods for attack-detection and identification* when some of the sensors are potentially corrupted.

4. SECURING CPS FROM THE HARDWARE POINT OF VIEW

The main difference between Cyber-physical and other systems is probably the interaction that CPS have with the physical world. CPS, in fact, integrate sensing, computations and actuation capabilities, and they are used to interact and to control critical infrastructure or critical applications. Applications range from automotive to industrial control systems or medical devices, and for many of them, safety is of utmost importance, as a failure of the system could have catastrophic consequences. Often, CPSs are deployed in an harsh environment, thus requiring reliability and tolerance to faults, and they are characterized by very strict constraints in terms of battery and computation power.

Low power, reliability and safety however are not the only properties which designers have to provide to CPSs. The use of CPSs in critical applications makes them an attractive target for cyber-attacks. The most famous example of attack to cyber-physical system is probably STUXNET [13], but several other works demonstrate the severity of the problem also for automotive industry [47] and smart grids [63]. In this section we discuss Lightweight cryptography [41] is a branch of cryptography aiming at implementing cryptographic algorithms using an extremely limited amount of resources. This goal is achieved following two main approaches [3]. The first approach consists in minimizing the amount of resources needed for implementing standard algorithms (AES for instance can be implemented using approximately 2500 Gate Equivalent [32]). The second approach is to design novel algorithms considering since the beginning that they have to be implemented using a limited amount of resources. The most successful examples of the second approach are PRESENT [8] and CLEFIA [46], which recently become ISO standard for lightweight cryptography. Further suitable algorithms can be identified also among the candidates recently submitted to the CAESAR contest [1] which has the goal of selecting a portfolio of algorithms for providing authenticate encryption. The designer has to select the appropriate hardware block according to the needs of the application, considering also that, in particular for control systems, CPSs might have extremely strict legacy requirements. Furthermore, designers should be aware that in lightweight cryptography usually trade resources with performance. As CPSs, due to their nature of being a controlling systems, often have strict real time requirements, it should be guaranteed that the included security primitives are capable of meeting them.

CPSs, as several other embedded systems can be deployed in an hostile environment, thus they are potentially in the hand of the attacker. For this reason, designer of secure hardware for cyber-physical systems have to implement it in such a way that is robust against physical attacks. When carrying out physical attacks, the adversary, instead of attacking the mathematical structure of a cryptographic primitive, tries to exploit weaknesses of its implementation for accessing secret information. Physical attacks are usually divided in active or passive [27]. During active attacks, the adversary tampers with the device in order to modify its behavior. Example of these attacks are fault attacks [4], in which an adversary induce a fault into a device, for instance by underfeeding the power supply [5], and extract the secret key by exploiting the differences between correct and faulty output. In passive attacks, usually called side channel attacks, the adversary extracts secret information by analyzing a physical observable and exploiting its correlation with the secret which is computed. The most common side channel attack is power analysis [20], which extract the secret key by relating it to the power consumed during encryption. However, also other channels such as timing [22] or electromagnetic emission [45] were successfully used in the past.

Resistance against timing attacks can be achieved by guaranteeing that all the operations depending on secret data are carried out in the same amount of time. This approach is successfully used in servers and in embedded systems, thus can be used also by CPSs designers. Resistance against power analysis attacks can be obtained by breaking the link between the data computed and the actual data (this approach is called masking [28]) or by breaking the correlation between the data being processed and the power consumption (this approach is called hiding [56]). Hardware blocks resistant against power analysis attacks are usually designed and tested by well trained engineers which manually apply a countermeasure or a number of them to a cryptographic block []. However, there have been several attempts to automatically realize hardware resistant against power analysis attacks [56, 43, 44, 40]. Similar approaches, can be used by the cyber-physical systems designers for securing their devices against physical attacks. It is important to underline however that design of secure hardware is still an open problem. These countermeasures are only protecting only the cyber part of the device, not the physical one. A hardware design flow which considers security also for the physical part of the CPS, to date, still does not exist.

The overall security of a CPS depends from the security of its building blocks. CPS as other systems, are subject to hardware Trojans, which, potentially, is one of the most serious threat for hardware security. Hardware Trojans can be defined as a deliberate and malicious modification of a hardware component carried out with the goal of altering its correct behavior. Possible example of alteration can be the leak of secret data or a denial of service. Hardware Trojans received a lot of attention from the community due to the potential devastating effects which they can have on security [6]. Trojans can be inserted at several points of the design flow: by malicious designer or IP provider, by a malicious foundry, or by malicious tool. Several technique to detect hardware Trojans were proposed in the past, ranging from testing, analysis of side channel, or optical inspection [7], nevertheless, none of them is perfect, and several of them require a gold model to be effective. Hardware designer of CPS has to be aware of this threat and apply the appropriate detection techniques to identify hardware Trojans or to adopt the appropriate approach at system level to tolerate the presence of Trojans.

Finally, as mentioned, in addition to security requirements, cyber-physical systems needs to provide safety and reliability, whose needs might be in contrast with the ones of security. For instance, it is important to consider the effects which redundancy, added to provide fault tolerance, might have on security. Designers of secure cyber-physical systems should always keep a global vision of all the requirements and evaluate the effects which each design choice has on the others. This is a difficult and error prone task, which would be dramatically simplified by the eventual coming of dedicated design tools.

5. CONCLUSION

In this paper, we have focused on the design challenges for securing Cyber-Physical Systems. Specifically, we have presented an overview of tools, design methods, and building blocks used to design secure CPS. We have considered three complementary approaches for ensuring security in CPS. First, we have described methods for multi-domain modeling, simulation, and software synthesis for secure CPS. Second, we have presented a control-aware design framework to ensure attack-resiliency in CPS. Third, we have addressed the security challenges related to the design and use of computing hardware in CPS. Finally, potential avenues for future work have been discussed.

6. REFERENCES

[1] http://competitions.cr.yp.to/caesar.html.

[2] Spoofers Use Fake GPS Signals to Knock a Yacht Off Course.

[3] C. Alippi, A. Bogdanov, and F. Regazzoni. Lightweight cryptography for constrained devices. In *Integrated Circuits (ISIC), 2014 14th International Symposium on*, pages 144–147. IEEE, 2014.

[4] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan. The sorcerer's apprentice guide to fault attacks. *Proceedings of the IEEE*, 94(2):370–382, 2006.

[5] A. Barenghi, C. Hocquet, D. Bol, F.-X. Standaert, F. Regazzoni, and I. Koren. Exploring the feasibility of low cost fault injection attacks on sub-threshold devices through an example of a 65nm aes implementation. In *RFID. Security and Privacy*, pages 48–60. Springer, 2012.

[6] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson. Stealthy dopant-level hardware trojans. In *Cryptographic Hardware and Embedded Systems-CHES 2013*, pages 197–214. Springer, 2013.

[7] S. Bhasin and F. Regazzoni. A survey on hardware trojan detection techniques. In *IEEE International Symposium on Circuits and Systems (ISCAS 2015)*, 2015.

[8] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe. *PRESENT: An ultra-lightweight block cipher*. Springer, 2007.

[9] A. Canedo, A. Faruque, M. Abdullah, and J. H. Richter. Multi-disciplinary integrated design

automation tool for automotive cyber-physical systems. In *Proceedings of the conference on Design, Automation & Test in Europe*, page 315. European Design and Automation Association, 2014.

[10] A. Canedo, E. Schwarzenbach, and M. A. Al Faruque. "Context-sensitive synthesis of executable functional models of cyber-physical systems". *ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, pages 99–108, 2013.

[11] A. Canedo, J. Wan, and M. A. A. Faruque. "Functional Modeling Compiler for System-Level Design of Automotive Cyber-Physical Systems". In *Proceedings of the ACM/IEEE International Conference on Computer-Aided Design (ICCAD)*, 2014.

[12] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *SEC'11: Proceedings of the 20th USENIX conference on Security*, pages 1–16. USENIX Association, Aug. 2011.

[13] N. Falliere, L. O. Murchu, and E. Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 2011.

[14] J. P. Farwell and R. Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, 2011.

[15] H. Fawzi, P. Tabuada, and S. Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *arXiv preprint arXiv:1205.5073*, 2012.

[16] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. OŠHanlon, and P. M. Kintner Jr. Assessing the spoofing threat: Development of a portable gps civilian spoofer. In *Proceedings of the ION GNSS international technical meeting of the satellite division*, volume 55, page 56, 2008.

[17] R. Ivanov, M. Pajic, and I. Lee. Attack-resilient sensor fusion. In *DATE'14: Design, Automation and Test in Europe*, 2014.

[18] R. Ivanov, M. Pajic, and I. Lee. Resilient multidimensional sensor fusion using measurement history. In *HiCoNS'14: High Confidence Networked Systems*, 2014.

[19] R. Ivanov, M. Pajic, and I. Lee. Resilient sensor fusion for safety-critical cyber-physical systems. 2014. Submitted.

[20] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Advances in CryptologyâĂŤCRYPTOâĂŹ99*, pages 388–397. Springer, 1999.

[21] P. Kocher, R. Lee, G. McGraw, A. Raghunathan, and S. Moderator-Ravi. Security as a new dimension in embedded system design. In *Proceedings of the 41st annual Design Automation Conference*, pages 753–760. ACM, 2004.

[22] P. C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Advances in CryptologyâĂŤCRYPTOâĂŹ96*, pages 104–113. Springer, 1996.

[23] H. Kopetz and G. Bauer. The time-triggered architecture. *PROCEEDINGS OF THE IEEE*, 91(1):112–126, 2003.

[24] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy (SP)*, pages 447 –462, 2010.

[25] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *Security Privacy, IEEE*, 9(3):49–51, 2011.

[26] C. Li, A. Raghunathan, and N. Jha. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*, pages 150–156, 2011.

[27] S. Mangard, E. Oswald, and T. Popp. *Power analysis attacks: Revealing the secrets of smart cards*, volume 31. Springer Science & Business Media, 2008.

[28] T. S. Messerges. Securing the aes finalists against power analysis attacks. In *Fast Software Encryption*, pages 150–164. Springer, 2001.

[29] F. Miao, M. Pajic, and G. J. Pappas. Stochastic game approach for replay attack detection. In *Decision and Control (CDC), 2013 IEEE 52nd Annual Conference on*, pages 1854–1859, 2013.

[30] Y. Mo, T.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[31] A. P. Moore, R. J. Ellison, and R. C. Linger. Attack modeling for information security and survivability. Technical report, DTIC Document, 2001.

[32] A. Moradi, A. Poschmann, S. Ling, C. Paar, and H. Wang. Pushing the limits: A very compact and a threshold implementation of aes. In *Advances in Cryptology–EUROCRYPT 2011*, pages 69–88. Springer, 2011.

[33] T. Nghiem, G. J. Pappas, R. Alur, and A. Girard. Time-triggered implementations of dynamic controllers. *ACM Transactions on Embedded Computing Systems (TECS)*, 11(S2):58, 2012.

[34] D. M. Nicol, W. H. Sanders, and K. S. Trivedi. Model-based evaluation: from dependability to security. *Dependable and Secure Computing, IEEE Transactions on*, 1(1):48–65, 2004.

[35] M. Pajic, N. Bezzo, J. Weimer, R. Alur, R. Mangharam, N. Michael, G. J. Pappas, O. Sokolsky, P. Tabuada, S. Weirich, et al. Towards synthesis of platform-aware attack-resilient control systems. In *Proceedings of the 2nd ACM international conference on High confidence networked systems*, 2013.

[36] M. Pajic, P. Tabuada, I. Lee, and G. Pappas. Attack-Resilient State Estimation in the Presence of Noise. Technical report, 2015. Under review.

[37] M. Pajic, J. Weimer, N. Bezzo, P. Tabuada, O. Sokolsky, I. Lee, and G. Pappas. Robustness of attack-resilient state estimators. In *Cyber-Physical Systems (ICCPS), 2014 ACM/IEEE International Conference on*, pages 163–174, 2014.

[38] J. Park, R. Ivanov, J. Weimer, M. Pajic, and I. Lee. Sensor attack detection in the presence of transient faults. In *Proceedings of the ACM/IEEE Sixth*

International Conference on Cyber-Physical Systems (ICCPS), pages 1–10, 2015.

[39] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *Automatic Control, IEEE Transactions on*, 58(11):2715–2729, 2013.

[40] T. Popp and S. Mangard. Masked dual-rail pre-charge logic: Dpa-resistance without routing constraints. In *Cryptographic Hardware and Embedded Systems–CHES 2005*, pages 172–186. Springer, 2005.

[41] A. Poschmann. Lightweight cryptography - cryptographic engineering for a pervasive world. Cryptology ePrint Archive, Report 2009/516, 2009.

[42] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady. Security in embedded systems: Design challenges. *ACM Transactions on Embedded Computing Systems (TECS)*, 3(3):461–491, 2004.

[43] F. Regazzoni, S. Badel, T. Eisenbarth, J. Grobschadl, A. Poschmann, Z. Toprak, M. Macchetti, L. Pozzi, C. Paar, Y. Leblebici, et al. A simulation-based methodology for evaluating the dpa-resistance of cryptographic functional units with application to cmos and mcml technologies. In *Embedded Computer Systems: Architectures, Modeling and Simulation, 2007. IC-SAMOS 2007. International Conference on*, pages 209–214. IEEE, 2007.

[44] F. Regazzoni, A. Cevrero, F.-X. Standaert, S. Badel, T. Kluter, P. Brisk, Y. Leblebici, and P. Ienne. A design flow and evaluation framework for dpa-resistant instruction set extensions. In *Cryptographic Hardware and Embedded Systems-CHES 2009*, pages 205–219. Springer, 2009.

[45] P. Rohatgi. Electromagnetic attacks and countermeasures. In *Cryptographic Engineering*, pages 407–430. Springer, 2009.

[46] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata. The 128-bit blockcipher clefia. In *Fast software encryption*, pages 181–195. Springer, 2007.

[47] Y. Shoukry, P. D. Martin, P. Tabuada, and M. B. Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In G. Bertoni and J. Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 55–72. Springer, 2013.

[48] Y. Shoukry and P. Tabuada. Event-triggered state observers for sparse sensor noise/attacks. *arXiv preprint arXiv:1309.3511*, 2013.

[49] J. Slay and M. Miller. Lessons learned from the maroochy water breach. In *Critical Infrast. Protection*, pages 73–82, 2007.

[50] R. Smith. A decoupled feedback structure for covertly appropriating networked control systems. *Proc. IFAC World Congress*, pages 90–95, 2011.

[51] S. Sundaram, M. Pajic, C. Hadjicostis, R. Mangharam, and G. Pappas. The Wireless Control Network: Monitoring for malicious behavior. In *Proceedings of the 49th IEEE Conference on Decision and Control*, pages 5979–5984, 2010.

[52] D. Talbot. Computer viruses are ŞrampantŤ on medical devices in hospitals. *MIT Technology Review, Oct*, 17:19, 2012.

[53] C. R. Taylor, K. Venkatasubramanian, and C. A. Shue. Understanding the security of interoperable medical devices using attack graphs. In *Proceedings of the 3rd International Conference on High Confidence Networked Systems*, HiCoNS '14, pages 31–40, 2014.

[54] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the 1st international conference on High Confidence Networked Systems*, HiCoNS '12, pages 55–64, 2012.

[55] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun. On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 75–86, 2011.

[56] K. Tiri and I. Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proceedings of the conference on Design, automation and test in Europe-Volume 1*, page 10246. IEEE Computer Society, 2004.

[57] J. Wan, A. Canedo, and M. A. A. Faruque. "Functional Model-based Design Methodology for Automotive Cyber-Physical Systems". *IEEE Systems Journal (ISJ)*, 2014.

[58] J. Wan, A. Canedo, and M. A. A. Faruque. "Security-Aware Functional Modeling of Cyber-Physical Systems". *20th IEEE International Conference on Emerging Technology & Factory Automation (ETFA'15)*, 2015.

[59] J. S. Warner and R. G. Johnston. A simple demonstration that the global positioning system (gps) is vulnerable to spoofing. *Journal of Security Administration*, 25(2):19–27, 2002.

[60] A. Wasicek, P. Derler, and E. A. Lee. Aspect-oriented modeling of attacks in automotive cyber-physical systems. In *Design Automation Conference (DAC), 2014 51st ACM/EDAC/IEEE*, pages 1–6. IEEE, 2014.

[61] C. Weaver. Patients put at risk by computer viruses. *The Wall Street Journal*, 2013.

[62] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits. Systematic analysis of cyber-attacks on cps-evaluating applicability of dfd-based approach. In *Resilient Control Systems (ISRCS), 2012 5th International Symposium on*, pages 55–62. IEEE, 2012.

[63] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li. Time synchronization attack in smart grid: Impact and analysis. *IEEE Trans. Smart Grid*, 4(1):87–98, 2013.