Towards Resilient Cyber-Physical Control Systems

Gabriel Salles-Loustau, Saman Zonouz
Electrical and Computer Engineering Department
Rutgers University
{*gs643, saman.zonouz*}*@rutgers.edu*

***Abstract*—Cyber-Physical Systems (CPS) are yielding novel problems and solutions for security researchers. CPSs connect computerized controllers and human supervisors with physical systems used in the energy, transportation, water, manufacturing, and other sectors. Recent attacks against CPS have prompted unprecedented investigation into new threats and mitigations against CPSs. There are motivating examples of real-world control system attacks such as the Maroochy Shire water system attack, the Lodz Poland train derailment, and the Stuxnet virus. In each of these attacks, the adversary capabilities and objectives, vulnerabilities, attack methods, and final outcomes differ significantly. However, despite the increased interest in CPS security problems, the security community faces significant learning curves in addressing them. Modern CPSs are founded on control theory, real-time systems, and obscure, often ad-hoc programming practices. Furthermore, the traditional definitions of security are often in conflict with the goals and operational constraints of CPSs. A security measure that blocks a system operator from executing a critical action could cause as much or more damage than an actual attack. We discuss the most basic and widely deployed application of CPS, control systems, and the emerging problems in their security.**

I. Introduction

Cyber-physical critical infrastructures integrate networks of computation and physical processes to provide the society with essential functionalities and services. Distributed and embedded computers monitor the physical processes and, at the same time, control them, usually with feedback loops in which physical processes affect computations and vice versa. As a case in point, the power grid infrastructure is a vast and interconnected cyber-physical network for delivering electricity from generation plants to end-point consumers. Protecting the critical infrastructures is a vital necessity because the failure of these systems would have a debilitating impact on economic security and public health and safety.

Due to the insufficiency of the deployed protection solutions, there have been several large-scale outages [1]. For instance, the August 2003 blackout was caused by several unrelated interacting factors such as a transmission line outage as a result of a line-tree contacts followed by computer crashes preventing the control operators from finding out about the line outage, and hence taking corrective actions. This led to a cascading outage and ultimately the blackout, which affected around 50 million people and cost approximately 6 billion dollars [2]. While there was no malicious intent behind the 2003 blackout, it showed several cyber-physical system weak-points and potential vulnerabilities that could be exploited by the attackers to cause the same catastrophic consequence.

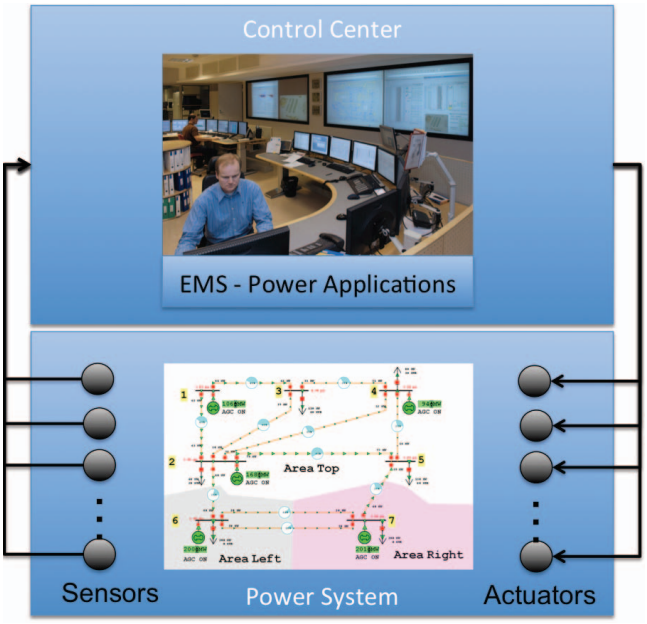

Fig. 1: Cyber-Physical Power Control Systems

Additionally, there have been sophisticated attacks in other industrial settings, giving reason for concern. A recent and well-known example is the Stuxnet computer worm [3], which targeted Siemens industrial software used to control nuclear fuel processing plants. The worm exploited several extremely complicated cyber attack vectors, including four Windows zero-day vulnerabilities [4], to sabotage a suspected uranium processing facility. The scale and complexity of the attack clearly demonstrated the need to fully monitor cyber-physical critical infrastructures in real time for both accidental and malicious failures. Such monitoring would allow the power grid operators to take quick responsive and corrective actions if the power grid is under attack or has experienced failures.

This paper reviews cyber-physical industrial control system networks, and critical power grid infrastructures specifically, cyber-physical vulnerabilities and threats as well as emerging mitigation and intrusion resilience techniques. We will briefly introduce the industrial control networks (Section II), potential cyber-physical system vulnerabilities (Section III), past real-world attacks against those networks as well as possible mitigation techniques against the existing threats (Section IV).

978-1-4799-7591-4/15/$31.00 ©2015 IEEE

II. Control Systems

The subject of modern control systems involves a broad set of topics in control theory, as well as a history of organically developed practices. Given the relative unfamiliarity of computer scientist and security experts with some of these topics, a solid understanding in the foundations and evolution of control systems is crucial for approaching their security problems. To this end, we will focus on two topics: the architecture and basic units of industrial control systems and the methods of embedded controller programming.

Industrial control systems. A control system (Figure 1) is a computerized means of regulating the behavior of a physical process. The control system gives one or more computers the ability to manipulate physical equipment as needed to control various physical quantities, e.g., a computer may be able to control a heating element to regulate the temperature of a chemical reaction. Modern control systems network the controller computers with corporate networks for organization-wide control and data analytics. Early control systems were not software based, but instead were implemented as relay circuits, in which some number of Boolean circuits executed in parallel over a set of sensor values from the physical process. The outputs of these circuits dictate the desired behavior of process machinery. Modern software-based controllers achieve the same ends, while being more easily reconfigurable than hardware relays. This has an important implication: *because modern automation controllers attempt to mimic hardware relays, their program design methodologies are significantly different from traditional general purpose computers.* This concept is covered more in the following section.

Geographically distributed control systems rely heavily on *state estimators*, which provide accurate measurements of physical quantities, even when some sensors may be erroneous. From a data perspective, power systems consist of sensor data acquisition, processing and control command. The information path from the field sensors to end-point power control network assets, e.g., PLCs, enabled power system applications such as state estimation and equipment control. The data integrity within the information path may be low for many reasons, including misconfigurations, sensor or communication failures, or coordinated false data injection attacks. Indeed, noisy data are constantly present in the system, yet the system maintains a high level of reliability due to mechanisms put in place to detect and deal with such data. However, recent research [5], [6] has shown that maliciously coordinated false data injection attacks may be able to bypass traditional state estimation mechanisms put in place to detect noisy data, and that such attacks may impact power system state estimation applications to manipulate the calculated system state estimate [7], [8], [9].

Programmable automation. The basic unit of automation in a control system is the Programmable Logic Controller (PLC). PLCs are directly connected to physical machinery and are responsible for the real-time control of the process. Additionally, PLCs aggregate process statistics for human operators, and execute sub-processes on their behalf. Many times per second, the PLC re-executes its control software in a procedure known as a *scan cycle*. A scan cycle consists of three steps: (*i*.) Measurements are read from plant sensors. (*ii*.) The software control program is executed over the sensor measurements. (*iii*.) The control program's output values are used to govern plant machinery. The software control program executed in step (*ii*.) are typically written in graphical languages, the most popular of which is *Relay Ladder Logic* (RLL). On our research with real PLC systems, we have observed several inconsistencies in RLL program execution between vendors, and the weak, and in some cases, absent type systems used in writing PLC code. This is an important topic as it has implications for the analysis of PLC code.

Despite their critical importance in control systems, insufficient effort has been spent on securing PLCs. New vulnerabilities are increasingly being identified in PLC and their surrounding control system equipment [10], [11], [12], [13]. In addition, PLCs are often exposed to Internet-connected corporate networks [14], and sometimes directly to the Internet [15], [16]. PLCs are often protected only by passwords, and hard coded backdoor accounts are often added by vendors. PLCs have no access control models for manipulating physical devices, and thus any adversary that can upload code to a PLC can have complete control over the plant machinery [3].

III. Systems Vulnerabilities

In our research, we have experimented with several existing hardware and software assets from the major involved vendors in the control system domain. The integration of the cyber and physical components in industrial control systems has resulted in several new cyber-physical system-specific vulnerabilities [17], [18], [19], [20], [21], [22], [23], [24]. Cyber network vulnerabilities, e.g., vulnerable state estimation server process, and physical system weaknesses, e.g., lack of power system $N-1$ reliability compliance [25], can be exploited simultaneously to cause a cyber-physical impact on the control system. Additionally, the *availability* being the most important CIA criterion in most of critical infrastructures can introduce new attack surfaces. As a case in point, to keep control network available all the time and guarantee timely electricity delivery, control system operators face new operational constraints such as easy access to critical functionalities in the case of emergency that hinders deployment of security solutions such as strict global access control policy enforcement.

IV. Attacks and Potential Mitigations

There are several examples of real-world attacks against control systems. The first of these is the Maroochy Shire water breach in which a disgruntled former employee spilled nearly a quarter million gallons of sewage into public water ways. The second attack is the Lodz train attack, where a high schooler used a modified infrared remote control to manipulate train switches, ultimately derailing four train cars and injuring several people. The most well-known attack is the 2009 Stuxnet attack, which leveraged a malicious payload

to cause a PLC to harm physical equipment. We discuss the several mitigation techniques to mitigate the existing threats against cyber-physical systems.

1) Trustworthy Architectures: Following the introduced cyber-physical vulnerabilities, there have many secure architectures proposed for critical infrastructures generally [26], [27], [28]. To that end, several trustworthy control network architectures that have been recommended by several agencies, e.g., NIST [29], and NERC [25] as well as researchers [30], [31]. Additionally, our recent solution [32], [33] on architectural programmable logic controller protection can stop recent real-world intrusions such as Stuxnet worm. In particular, the solution is deployed as an embedded device sitting between the HMI server and PLC device in the control system and investigates every PLC code that is uploaded by the HMI server using static code analyses and formal verification techniques. If the code is detected to be malicious, the code upload request is rejected and the code along with a violating input vector is sent back to the HMI operator for debugging purposes. Otherwise, the code is uploaded on the PLC for execution and control of the physical system.

2) Online Security Assessment: There have been several online security assessment solutions proposed for cyber-physical infrastructures [34], [35], [36], [37]. Security/safety contingency analysis techniques in power systems has been explored by many researchers in the past (see [38] for a comprehensive survey). A contingency is defined as an accidental or malicious failure/incident on the power network, e.g., an unexpected loss of a power transmission line as a result of an attack or a thunderstorm. The initial efforts were based on first-order performance index sensitivities, i.e., a measure of how critical each incident is given the network topology, to rank contingencies [39]. There have been several follow-up attempts to improve the ranking quality by considering higher order sensitivities [40], [41]. Furthermore, there has been an increasing interest in the analysis of multiple contingencies [42], [43] after the introduction of new NERC standards [44], e.g., a linear sensitivity-based approximate measure of how close the power system is brought to islanding by a particular outage contingency [45]. Recently, there have been security-oriented cyber-physical contingency analysis solutions proposed [46], [47] that take into account both cyber and power network topologies to analyze the potential impact of possible cyber attacks on the physical system and consequently come up with the ranked list of contingencies, i.e., cyber vulnerability exploitations and power system contingencies.

3) Cyber-Physical Attack Detection: To terminate malicious compromises, several attack detection solutions using cyber and physical sensors have been proposed [48], [49], [50], [51], [52], [53]. There have been few specific intrusion detection frameworks that concentrate on cyber as well as physical aspects of the control networks. Almost every detection framework includes a solution to the problem of hybrid cyber-physical security modeling of the power-grid [54]. Pasqualetti [55] model a power system under cyber-physical attack as a linear time-invariant descriptor system with unknown inputs, and design a dynamic detection and identification scheme using geometric control theoretic tools. Sridhar et al. [56] review how traditional intrusion detection techniques could be applied in cyber-physical settings, and introduce a layered approach to evaluate risk based on the current state of the power-grid. Recently, cyber-physical detection solutions against false data injection attacks have been proposed that fuse uncertain information from different types of distributed sensors, such as power system meters and cyber-side intrusion detectors, to detect the malicious activities within the cyber-physical system [49]. Specifically, such security-oriented cyber-physical state estimation engines, at each time instant, identify the compromised set of hosts in the cyber network and the maliciously modified set of measurements obtained from power system sensors.

4) Proactive Cyber-Physical Intrusion Tolerance: Preserving the availability and integrity of networked computing systems in the face of those fast-spreading intrusions requires advances not only in detection algorithms, but also in intrusion tolerance and automated response techniques. Additionally, the complexity and connectivity of control networks, and their recently increasing integrations with physical systems signify the quest for systems that detect their own compromises and failures and automatically repair themselves. In particular, the ultimate goal of the intrusion tolerant system design is to adaptively react against malicious attacks in real-time, given offline knowledge about the network's topology, and online alerts and measurements from system-level sensors. Cyber-physical intrusion tolerance solutions are relatively less investigated as they require sufficiently accurate attack detection tools that are currently nonexistent; however, there have been several research attempts in the area [57], [58], [59] using extended attack trees called attack-response tree formalism that not only formulate possible attack vectors but also represents possible system and network-level response and recovery actions that can be taken if the network is partially compromised/down.

V. Cost-Sensitive Security Sensor Deployment

To perform a cost-optimal deployment of security sensors to monitor potential upcoming threats, we extend our existing solution [53] to cyber-physical control systems. The proposed solution makes use of a mapping between system vulnerabilities and available security sensors to select and deploy cost-optimal sensor subset. In order to detect attacks' damage to the system, an initial set of intrusion detection systems (IDSes), i.e., called "attack consequence detectors," would be deployed. Attack consequence detectors are expected to be lightweight detectors that can operate continuously or periodically and detect the eventual symptoms of an intrusion. We assume that consequence detectors cannot be turned off during the attack. Examples include in-network DDoS, BotNet, and worm detection mechanisms, file-integrity checkers run independently of the target machine, or statistical system call/network anomaly detectors. The output of an attack consequence detector is a process, port, or file that exhibits the symptoms of an attack. As a case in point, the Samhain file integrity checker could

TABLE I: Detection Algorithm Categorization

Detection Policy	**Symbol**: **Mechanism**	**Cost**	**Detector**
Information flow analysis	Tnt: Taint tracking	Very High	TEMU
Input investigation	FW: Feature-based packet monitoring	Very Low	Firewalls
	Snrt: Content-based packet monitoring (stateless)	Medium	`Snort`
	App: Application-based IDS (stateful)	Medium	`Secerno`
Execution monitoring	ClSt: Control Violation: call stack monitoring	High	callstack monitoring
	CtFl: Control Violation: control flow integrity monitoring	High	Control-Flow Integrity
	DtFl: Data Violation: data flow monitoring	Very High	`MemCheck`
Consequence detection	AV: Malicious code: executable integrity checking	Low	`ClamAV`
	Hst: Host-based detection systems	Low	`Samhain`
	Stat: Statistical anomaly-based	Low	`Zabbix`

be used as an attack consequence detector because of its low overhead and capability in detecting file-system-related consequence.

Briefly, the core idea of the proposed model is to dynamically (based on ongoing attacks) reconfigure and deploy the required subset (and not all) of the available IDSes, with the lowest possible detection cost in the system. Table I shows different types of IDSes categorized by the mechanisms they use to detect misbehaviors. The table also shows the deployment cost for each IDS, i.e., its performance overhead on the system. For each detection mechanism, a real-world software tool is also provided that could be used in our model. Next, the question is "what is the construct that will be needed to balance detection coverage vs. cost in the system, given the available IDSes and their individual costs?" We first need to define the detection coverage for each IDS; in other words, what vulnerability exploitations can each IDS detect? This is answered, in our model, by the detector-capability matrix, which indicates the ability of a given IDS to detect various vulnerability exploitation types. The matrix is defined over the Cartesian product of the vulnerability type set and the set of IDSes, and shows how likely it is that each IDS could detect an exploitation of a specific vulnerability type.

Table II illustrates a sample detector capability matrix for the different IDSes and vulnerability types. In particular, each row in the table represents a specific intrusion detector type, and each column in the table addresses a specific vulnerability type. The notations used for vulnerability types are as follows. Buff is Buffer overflows; DngPtr is Dangling pointers; FmtStr is Format string bugs; ShlMC is Shell metachar bugs; SQLIn is SQL injection; CodIn is Code injection; DirTrv is Directory traversal; CSS is Cross-site scripting; HttpHdr is HTTP header injection; HttpRsp is HTTP response splitting; TcTu is Time-of-check-time-of-use; SymRc is Symlink races; CSFor is Cross-site request forgery; ClkJk is Clickjacking; FTPBnc is FTP bounce attack; WrnFtg is Warning fatigue; BlmVic is Blaming the Victim; Race is Race Conditions; PwdDic is Password Dictionary; and Encypt is Encryption Bruteforce.

Each element in Table II encodes the detection capability of a particular detector type in identifying individual vulnerability type exploitations. The notations used in the table are as follows: N means that the detection technique cannot detect the exploit; L means that it can only detect a small percentage

TABLE II: The Detector-Capability Matrix

	Buff DngPtr	FmtStr ShlMC SQLIn CodIn DirTrv CSS HttpHdr HttpRsp	TcTu SymRc	CSFor ClkJk FTPBnc	WrnFtg BlmVic Race	PwdDic Encrypt
Tnt	HM	HMC L HCMM	L L	HHH	N N N	N N
FW	L N	L N N L N N L L	N N	L L L	N N N	M M
Snrt	M N	M M M M M N M M	N N	N N M	N N N	H H
App	H L	H H H H H L C C	N N	N N H	N N N	H H
ClSt	C M	H N N N N N N N	N N	N N N	N N N	N N
CtFl	C H	H N N N N N N N	N N	N N N	N N N	N N
DtFl	L L	L M C L H C M M	L L	H H H	N N N	N N
AV	N N	N N N M N N N N	H H	N N N	L L L	N N
Hst	L L	L N N H N N N N	H H	N N H	M M L	N N
Stat	M M	L N N L N N N N	N N	N N H	N N N	H H

of these exploits; M means that the detection capability is medium; H means that the exploit is detected with high probability; and C means that the exploit is definitely detected by the detection technique. Some of the IDSes, e.g., `OSSEC`, monitor system-wide events, whereas others only observe one or a set of processes in the system, e.g., `Memcheck`. Entries in Table II report detection capabilities assuming that the vulnerability exploitation context is being observed by the corresponding IDS. The detection capability matrix is later employed in the model to decide on the minimum-cost set of IDSes with maximum exploit detection capability. Table II is used by the engine to deploy the cheapest detectors continuously.

VI. Conclusions

In this paper, we reviewed potential and real-world cyber-originated threats against cyber-physical critical control infrastructures. We discussed the fact that not every traditional IT security solution fits the cyber-physical security problem, and hence new effective security solutions are required for particular critical infrastructure protection problems. Additionally, we reviewed possible mitigation techniques that could be deployed to protect critical infrastructures against threats.

Acknowledgements

We would like to thank our research sponsor, National Science Foundation (NSF); Award Number 1446471.

REFERENCES

[1] NERC, 2009 NERC disturbance index, 2010.

[2] U. C. P. S. O. T. Force, final report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, 2003.

[3] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet dossier," Symantic Security Response, Tech. Rep., 2010.

[4] R. Naraine, stuxnet attackers used 4 Windows zero-day exploits, 2010.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, pp. 13:1–13:33, 2011.

[6] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, "Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1790–1799, 2012.

[7] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.

[8] L. Jia, R. J. Thomas, and L. Tong, "Impacts of malicious data on real-time price of electricity market operations," in *HICSS*, 2012, pp. 1907–1914.

[9] A. Teixeira, henrik Sandberg, G. Dan, and K.-H. Johansson, "Optimal power flow: Closing the loop over corrupted data," in *Proc. of American Control Conference*, 2012.

[10] D. Beresford, "Exploiting Siemens Simatic S7 PLCs," in *Black Hat USA*, 2011.

[11] D. G. Peterson, "Project Basecamp at S4," January 2012.

[12] Computer Emergency Response Team, "ADVANTECH/BROADWIN WEBACCESS RPC VULNERABILITY," ICS-CERT Advisory 11-094-02, April 2011.

[13] L. Constantin, "Researchers Expose Flaws in Popular Industrial Control Systems," http://www.pcworld.com, January 2012.

[14] T. Yardley, "SCADA: Issues, Vulnerabilities, and Future Directions," *;login*, vol. 34, no. 6, pp. 14–20, December 2008.

[15] J. C. Matherly, "Shodan the computer search engine," 2009.

[16] Éireann P. Levertt, "Quantitatively Assessing and Visualising Industrial System Attack Surfaces," Master's thesis, University of Cambridge, 2011.

[17] S. McLaughlin and P. McDaniel, "Sabot: specification-based payload generation for programmable logic controllers," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 439–449.

[18] S. McLaughlin, "On dynamic malware payloads aimed at programmable logic controllers," in *Proceedings of the 6th USENIX conference on Hot topics in security. HotSec*, vol. 11, 2011, pp. 10–10.

[19] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," in *Critical Information Infrastructures Security*. Springer, 2010, pp. 176–187.

[20] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel, "Multi-vendor penetration testing in the advanced metering infrastructure," in *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM, 2010, pp. 107–116.

[21] M. Brundle and M. Naedele, "Security for process control systems: An overview," *IEEE Security Privacy*, vol. 6, pp. 24–29, 2008.

[22] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *Security & Privacy, IEEE*, vol. 7, no. 3, pp. 75–77, 2009.

[23] S. McLaughlin, D. Podkuiko, A. Delozier, S. Miadzvezhanka, and P. McDaniel, "Embedded firmware diversity for smart electric meters," in *Proceedings of the 5th USENIX Workshop on Hot Topics in Security (HotSec 2010), Washington DC*, 2010.

[24] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems." in *HotSec*, 2008.

[25] "North American Electric Reliability Corporation, CIP-002-5 Cyber Security," 2012.

[26] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 415–427.

[27] S. Zonouz and W. H. Sanders, "A kalman-based coordination for hierarchical state estimation: Agorithm and analysis," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. IEEE, 2008, pp. 187–187.

[28] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 87–98.

[29] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ics) security," *NIST Special Publication*, vol. 800, no. 82, pp. 16–16, 2008.

[30] R. L. Krutz, *Securing SCADA systems*. John Wiley & Sons, 2005.

[31] R. Langner, *Robust control system networks*. Momentum Press, 2011.

[32] S. McLaughlin, S. Zonouz, D. Pohly, and P. McDaniel, "A trusted safety verifier for process controller code," *NDSS 2014*, 2014.

[33] S. Zonouz, J. Rrushi, and S. McLaughlin, "Detecting industrial control malware using automated plc code analytics," *Security & Privacy, IEEE*, vol. 12, no. 6, pp. 40–47, 2014.

[34] S. A. Zonouz, R. Berthier, and P. Haghani, "A fuzzy markov model for scalable reliability analysis of advanced metering infrastructure," in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*. IEEE, 2012, pp. 1–5.

[35] S. Zonouz and S. G. Miremadi, "A fuzzy-monte carlo simulation approach for fault tree analysis," in *Reliability and Maintainability Symposium, 2006. RAMS'06. Annual*. IEEE, 2006, pp. 428–433.

[36] S. A. Zonouz, W. H. Sanders, T. Yardley, R. Berthier, and H. Khurana, "Seclius: An information flow-based, consequence-centric security metric," *IEEE Transactions on Parallel and Distributed Systems*, p. 1, 2013.

[37] L. Garcia and S. Zonouz, "Tmq: Threat model quantification in smart grid critical infrastructures," in *Smart Grid Communications (SmartGridComm), 2014 IEEE International Conference on*. IEEE, 2014, pp. 584–589.

[38] B. Stott, O. Alsac, and A. F.L., "Analytical and computational improvements in performance index ranking algorithms for networks," *International Journal of Electrical Power and Energy Systems*, vol. 7, no. 3, pp. 154–160, 1985.

[39] G. C. Ejebe and B. F. Wollenberg, "Automatic contingency selection," *IEEE Transactions on Power Apparatus and Systems*, vol. 65, no. 1, pp. 859–109, 1979.

[40] T. Mikolinnas and B. Wollenberg, "An advanced contingency selection algorithm," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-100, no. 2, pp. 608–617, feb. 1981.

[41] G. Irisarri and A. Sasson, "An automatic contingency selection method for on-line security analysis," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-100, no. 4, pp. 1838–1844, 1981.

[42] T. Guler and G. Gross, "Detection of island formation and identification of causal factors under multiple line outages," *IEEE Transactions on Power Systems*, vol. 22, no. 2, pp. 505–513, 2007.

[43] T. Halpin, R. Fischl, and R. Fink, "Analysis of automatic contingency selection algorithms," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-103, no. 5, pp. 938–945, may 1984.

[44] NERC. (2005) System performance following loss of two or more bulk electric system elements (category c).

[45] C. Davis and T. Overbye, "Multiple element contingency screening," *IEEE Transactions on Power Systems*, vol. 26, no. 3, pp. 1294–1301, 2011.

[46] S. Zonouz, M. Davis, K. Davis, R. Berthier, R. B. Bobba, and W. Sanders, "Socca: A security-oriented cyber-physical contingency analysis in power infrastructures," *submitted to IEEE Transactions on Smart Grid (minor revision)*, 2013.

[47] R. Berthier, R. Bobba, M. Davis, K. Rogers, and S. Zonouz, "State estimation and contingency analysis of the power grid in a cyber-adversarial environment," *NIST Workshop on Cybersecurity for Cyber-Physical Systems*, 2012.

[48] C. Zimmer, B. Bhat, F. Mueller, and S. Mohan, "Time-based intrusion detection in cyber-physical systems," in *Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems*. ACM, 2010, pp. 109–118.

[49] S. Zonouz, K. Rogers, R. Berthier, R. Bobba, W. Sanders, and T. Overbye, "Scpse: Security-oriented cyber-physical state estimation for power grid critical infrastructures," vol. 3, no. 4, pp. 1790–1799, 2012.

[50] S. McLaughlin, B. Holbert, S. Zonouz, and R. Berthier, "Amids: A multi-sensor energy theft detection framework for advanced metering infrastructures," in *Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on*. IEEE, 2012, pp. 354–359.

[51] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, vol. 31, no. 7, p. 1319, 2013.

[52] S. Zonouz, K. R. Joshi, and W. H. Sanders, "Cost-aware systemwide intrusion defense via online forensics and on-demand detector deployment," in *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*. ACM, 2010, pp. 71–74.

[53] S. A. Zonouz, K. R. Joshi, and W. H. Sanders, "Floguard: cost-aware systemwide intrusion defense via online forensics and on-demand ids deployment," in *Computer Safety, Reliability, and Security*. Springer, 2011, pp. 338–354.

[54] Y. Mo, T. H.-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*, vol. 100, no. 1, pp. 195–209, jan. 2012.

[55] F. Pasqualetti, F. Dörfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," *CoRR*, vol. abs/1103.2795, 2011.

[56] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid." *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[57] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "Rre: A game-theoretic intrusion response and recovery engine," in *Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on*. IEEE, 2009, pp. 439–448.

[58] W. H. Sanders, R. H. Campbell, T. F. Abdelzaher, H. Khurana, and K. R. Joshi, "Game-theoretic intrusion response and recovery," 2012.

[59] S. Zonouz, A. Houmansadr, and P. Haghani, "Elimet: Security metric elicitation in power grid critical infrastructures by observing system administrators' responsive behavior," in *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*. IEEE, 2012, pp. 1–12.