A Brief Survey of Security Approaches For Cyber-Physical Systems

Elias Bou-Harb
Cyber Threat Intelligence Laboratory, Florida Atlantic University, USA
ebouharb@fau.edu

***Abstract*—The security of Cyber-Physical Systems (CPS) has been recently receiving significant attention from the research community. To this end, this paper sheds the light on a number of security approaches for CPS from two perspectives, namely, control-theoretic and cyber security. Further, threat detectors in various CPS environments are highlighted and discussed. The aim is to demonstrate the lack of coherent approaches that systematically tackle both security aspects of such systems, in addition to pinpointing several insightful research gaps that endeavor to shape future CPS security solutions.**

***Keywords*—Cyber Security, Control-theoretic, Cyber-Physical Systems, Survey**

I. Introduction

Critical infrastructure systems are indispensable to the broader health, safety, security, and economic well-being of modern society and governments. In recent years, many of these systems have been undergoing large-scale transformations with the infusion of new “smart” cyber-based technologies to improve their efficiency and reliability. These transitions are being driven by continual advances and cost-efficiencies in areas such as integrated networking, information processing, sensing, and actuation. Hence increasingly, physical infrastructure devices and systems are being tasked to co-exist and seamlessly operate in cyber-based environments. Indeed, tightly coupled systems that exhibit this level of integrated intelligence are often referred to as Cyber-Physical Systems (CPS) [1–3].

While CPS endeavor great opportunities, their complexity which arises from the fusion of computational systems with physical processes indeed hinders their utmost embracing [4, 5]. Within the context of security, these integrated systems pose substantial challenges as new vulnerabilities manifest themselves, leading to attack models that are fundamentally new and hard to infer, attribute, and analyze [2, 6, 7]. In turn, these gaps pose immense risks to the physical integrity and operation of critical infrastructures.

While the literature has been addressing the security of CPS by proposing numerous approaches, there still exists a gap that is rendered by the lack of coherent approaches that systemically tackle both aspects of such systems. Additionally, we can pinpoint the inadequacy of CPS threat detectors on various dimensions. Thus, the goal of this paper is to briefly discuss some of the works related to the cyber and control/physical perspectives of CPS, in addition to highlighting various proposals related to threat detectors in the realm of CPS. The latter effort endeavors to clarify such existing gap between those CPS approaches as well as to extract some research limitations that aim at paving the way for future work in the imperative area of CPS security.

The remainder of this paper is organized as follows. In the next section, we survey the literature by discussing several CPS security approaches and threat detectors, in addition to extracting several research gaps/limitations. We present some concluding remarks in Section III.

II. Literature Review and Gap Analysis

In this section, we review the literature by providing two distinct taxonomies in the context of CPS security approaches from both, the physical/control perspective as well as from the cyber security perspective. We further extend this section by providing a third classification in terms of threat detectors in various CPS environments. The aim of this section is to shed the light on the state-of-the-art in those research areas, in addition to pinpointing various research gaps.

A. *CPS Security: Control-theoretic Approaches*

The analysis of CPS security from a control-theoretic perspective has undoubtedly received considerable attention. Table I provides a brief taxonomy highlighting some fundamental and representative works in this area. In a nutshell, such taxonomy captures the modeled systems, whether or not noise has been considered in the approach, the analyzed attack model and its corresponding detection scheme. Such research works consider the system dynamics from a physical point of view to perform their analysis. For instance, in the power grid context, Liu et al. [8] investigated false date injection attacks by inserting arbitrary errors into sensor measurements. The authors analyzed two attack scenarios, where the attacker is either constrained to some specific meters, or limited in the resources required to compromise meters. For each scenario, algebraic conditions are derived to validate the existence of stealthy attack vectors, which do not yield any change to the residue. In the same power grid context, Sandberg et al. [9] characterized various security metrics that model the least effort required by an attacker to inject false data into Supervisory Control and Data Acquisition (SCADA) systems. To design such metrics, the authors exploited the physical topology of the power network, providing situational awareness to the system operator in an attempt to infer data manipulations. In an alternative work, Pasqualetti et al. [10] analyzed attacks on sensors and actuators by considering a generic continuous-time control system. In particular, the authors mathematically characterized certain conditions that provided the probability of detecting such attacks, given a set of known vulnerabilities. The authors further introduced the notion of attack detectability by designing centralized and distributed filters rooted in

978-1-5090-2914-3/16/$31.00 ©2016 IEEE

Type of System	Noise	Attack Models	Defense Mechanisms	Reference
Power Grid	✓	False data injection on sensors	Residue detector	[8]
Power Grid	✓	False data injection on sensors	Residue detector	[9]
Control System	-	Attacks on sensors & actuators	Detection filters	[10]
Control System	-	Attacks on sensors & actuators	Optimization decoders	[6]
Control System	✓	Replay attack	χ^2 detector	[11]
Wireless Network	-	State attacks	Output estimator	[12]
Distributed Network	-	State attacks	Combinatorial estimator	[13]
Sensor Network	✓	Dynamic False data injection	Residue detector	[14]

TABLE I: A brief Taxonomy of CPS Security Approaches from a Control-theoretic Perspective

arithmetic logic of descriptor systems. In the same realm, Fawzi et al. [6] focused on the design, implementation, analysis and characterization of robust estimation and control in CPS when they are affected by corrupted sensors and actuators. A main contribution of the latter work was the introduction and performance evaluation of efficient algorithms inspired by compressive sensing techniques to estimate the system's state under ongoing attacks. In a closely related work, Mo et al. [11] investigated replay attacks against sensors of a control system. In this attack scenario, the adversary replays previous measurements, which are statistically identical to true measurements at normal system state. To combat this threat, which operates similarly to the Stuxnet malware, the authors devised a noisy control authentication signal and a χ^2 detector in an effort to improve detection at the expense of system performance. In the area of distributed control systems security, Pajic et al. [12] analyzed the impact of malicious nodes in the context of a wireless control network. The authors designed and assessed the effectiveness of a detector based on an approach that aims at estimating sensor outputs. In a similar work addressing attacks on system states, Sundaram et al. [13] proposed a combinatorial procedure to compute the initial state of a distributed control system to infer such attacks. Alternatively, Mo et al. [14] considered a data injection attack on a noisy wireless sensor network. The attack was modeled as a constrained optimal control problem in which the Kalman filter was used to perform state estimation, while a failure detector was employed to detect anomalies in the system. In addition to the above, Teixeira et al. [15] have introduced and modeled a combination of different attack scenarios such as false data injections, replay, and zero-dynamics attacks, where adversarial activities attempt to cause damage to the controlled system while remaining stealthy. To this end, active detection methods have been proposed to infer such attacks through analyzing and manipulating the system dynamics. For instance, Mo et al. [16] proposed the method of physical watermarking to authenticate the nominal behavior of a control system. Specifically, in this approach, a known noisy control input is purposely injected to detect replay attacks by analyzing the output of the system. The latter strategy can be, however, ineffective against other types of attacks, including, false data injection attacks. To overcome this limitation, the dynamics of the system to be protected can be conveniently altered and camouflaged in order to actively detect adversarial actions. Indeed, this is the key idea behind [17], where time-varying dynamics, acting as a moving target, are introduced to detect integrity attacks.

Limitations: Indeed, the rationale behind the aforementioned substantial control-theoretic CPS security contributions is that there exist models that precisely describe the underlying physical phenomena, which enables the prediction of future behavior and, more importantly, unforeseen deviations from it. To this end, we can note that such approaches (1) do not provide any concrete evidence that such deviations are in fact originated from *malicious* entities, (2) depict attackers' models in a highly-theoretic manner, which do not necessary reflect the behavior of real CPS attacks and (3) provide experimentation and evaluations that were executed in emulated or simulated CPS environments, without much efforts being dedicated to real-world applications.

B. *CPS Security: Cyber Security Approaches*

Complementary to the above, the cyber security research community has also offered various approaches in an attempt to tackle numerous security aspects of CPS. Such approaches typically put less emphasis on the control system dynamics of CPS by essentially focusing on the cyber (i.e., communication networks, protocols, data, etc.) perspective. We classify a number of such fundamental approaches into four core categories as summarized in Table II and we subsequently discuss only a few of them, for space limitations. In the context of modeling CPS protocols, Goldenberg et al. [22] proposed the use of Deterministic Finite Automata (DFA) to capture the behavior of the Modbus protocol. The employed approach exploits the fact that the generated communication traffic from Modbus is highly periodic. To this end, the authors designed and implemented an algorithm to initially capture the embedded periodicity in network traffic channels and consequently flag any deviations from it. The authors evaluated their anomaly detection approach using different real data sets extracted from an operational facility. In another closely related work, Yoon et al. [23] modeled message sequences derived from CPS communication traffic to capture legitimate plant behavior. To accomplish the latter task, the authors employed a dynamic Bayesion network and a probabilistic suffix tree as the underlying predictive model. Executed evaluations using synthetic data demonstrated that the proposed approach is able to accurately model normal traffic, flag certain deviations, and reduce the false positive rate. From another perspective, several research works investigated secure approaches for CPS software and memory resources. For instance, McLaughlin et al. [24] proposed an approach to verify safety-critical code executed on programmable controllers. The devised approach initially checks such code against a set of physically safe

Analysis Perspective	**Highlights**	**References**
Protocol Vulnerabilities	Modeling CPS protocols to detect anomalies	[18–23]
PLC Software	Verifying PLC code and memory to prevent violations	[24–28]
Process Variables	Predicting CPS process behavior to detect anomalies	[29–32]
Network Measurements	Data-driven approaches to infer CPS cyber attacks	[33–37]

TABLE II: A brief Classification of CPS Security Approaches from a Cyber Security Perspective

measures and subsequently present case studies of abuse in case of any inferred inconsistencies. In this context, the authors introduced the notion of temporal execution graph, which illustrates the consequences of a certain untrusted executed code. The proposed approach was validated in terms of its capability to enforce certain common safety properties by means of experimentation in an emulated environment. In a similar fashion, Malchow et al. [28] proposed the use of an external CPS module to intercept and investigate any traffic targeting programmable controllers. To infer anomalies, code which is intended to be executed is compared to various safe baseline specimens by executing functional code comparisons and assembly matching techniques. Several other research initiatives exploited CPS process variables for anomaly detection. For example, Hadžiosmanović et al. [29] extracted process variables from a CPS plant to build predictability models. By leveraging simple regression models, the authors alerted CPS plant operators of any deviation in the expected parameters as an indicator of an ongoing attack. In an alternative work in the same realm, Caselli at al. [30] presented a sequence-aware detector that aims at inferring CPS semantic attacks on process variables. Such attacks represent specific series of benign operations that together form a malicious attack. Using real empirical measurements from a water treatment facility, the authors assessed and discussed the advantages and drawbacks of their approach. From a data analytics perspective, Almalawi et al. [34] presented a machine learning approach to infer CPS attacks. By employing an unsupervised clustering mechanism based on the k-means algorithm, the proposed approach aims at distinguishing between consistent and inconsistent CPS observations. Simulations were conducted to validate the effectiveness of the devised approach. Within the same category of research works but from an industrial/operational perspective, the security community supporting the open source intrusion detection system Snort [38] has also offered and contributed to various CPS detection rules [36]. The latter aim at inferring unauthorized requests, malformed packets and rarely used and suspicious CPS protocol commands.

Limitations: While the aforementioned research works offer significant contributions, we can still extract (1) the general inadequacy of research attempts to systematically combine or at least diminish the gap between cyber and control capabilities for security CPS, (2) the lack of empirical data related to tangible malicious CPS attacks and strategies that are generated from real unsolicited attackers, which could realistically affect the stability and security of CPS, (3) the deficiency of CPS security approaches in providing, both, attribution evidence and threat severity metrics and (4) the lack of such approaches in proving means for CPS resiliency in the physical realm during or immediately after an attack.

C. Threat Detectors for CPS

For the sake of completeness, in this section, we further pinpoint and discuss a number of diverse literature approaches that have offered CPS detection capabilities in numerous CPS sectors. We classify a few of those fundamental approaches as summarized in Table III based on their detection approach, their investigated attack, their considered CPS environment and their employed dataset. In the aerospace sector, Mitchell et al. [39] proposed a CPS threat detector capable of inferring command injection attacks on sensors and actuators of unmanned air vehicles. Their approach is based on a behavioral model that captures legitimate traffic and flags anomalies by means of constructing and comparing finite-state automata. Through simulations, the authors analyzed their devised model in terms of false positives. A similar approach and evaluation was presented in [40] investigating the automotive industry, where the authors leveraged a Markovian model to study the survivability of such a CPS tolerating a data manipulation attack. In another research work in the medical field, Park et al. [41] exploited spatial and temporal information generated from a human subject to infer anomalies. The authors devised similarity methods to derive a suitable threshold in an attempt to balance false positives and negatives. To evaluate the accuracy of their proposed approach, the authors uniquely employed a real dataset and executed several insightful experiments. In another set of research works, Shin et al. [42] analyzed Denial of Service (DoS) attacks while Verba et al. [44] investigated Man-In-The-Middle (MITM) attacks, in which both research works addressed CPS SCADA systems. To this end, [42] offered an anomaly inference approach based on a clustering mechanism while [44] proposed a signature CPS threat detector, in which benign signatures were derived by observing a functioning SCADA system and recording its protocol communication at normal state. Last but not least, in the power domain, Premaratne et al. [43] explored spoofing and authentication attacks against electric substations. In this context, the authors proposed a signature-based CPS detector by leveraging statistical primitives, which aim at describing benign traffic and subsequently flagging anomalies. Using simulated attacks, the authors analyzed the accuracy of their approach as well as its effectiveness against previously unseen attacks.

Limitations: From such insightful research works, we can extract several research gaps, including, (1) the lack of CPS threat detectors that are tailored towards the manufacturing sector, (2) the absence of theoretical and practical analysis investigating the detection latency as a performance metric, (3) the general inadequacy of CPS threat detectors that leverage network traffic and measurement approaches, (4) the lack of concrete and realistic CPS attack models in addition to the shortage of signature-based detection models and (5) the

Inference Approach	Attack Type	CPS Type	Dataset	Reference
Anomaly-based	Protocol command injection	Aerospace	Simulated	[39]
Anomaly-based	Data manipulation	Automotive	Simulated	[40]
Anomaly-based	Replay attack	Medical	Real	[41]
Anomaly-based	DoS attack	SCADA	Emulated	[42]
Signature-based	Authentication & spoofing attacks	Power utility	Emulated	[43]
Signature-based	MITM attacks	SCADA	Simulated	[44]

TABLE III: A brief Categorization of a few Proposed Threat Detectors for CPS

scarcity of CPS threat detectors which experiment with real data sets.
Indeed, the above three brief taxonomies highlight several research gaps, which we hope could be useful in tackling future research in the area of CPS security. It is worthy to mention that while there exists a few surveys dedicated to CPS [45], we are not aware of any that address the security approaches of such systems from the three highlighted perspectives.

III. Concluding Remarks

Research and development activities which tackle the security of Cyber-Physical Systems (CPS) are undoubtedly of significant importance, given the impact of such systems on our contemporary societies and critical infrastructure. To this end, this paper presented some research works related to various aspects of CPS in a dedicated effort to extract some research gaps that are worthy of undertaking and addressing. While such gaps are of interest to the author, nevertheless, the constructed taxonomies and the reported references aim to allow other researchers to investigate additional impactful and current research issues related to CPS security as deemed appropriate. For future work, we intend to extend this survey by providing more rigorous comparisons among other CPS approaches and dimensions, in addition to undertaking some technical research problems that arose from this work.

Acknowledgment

The author is grateful to Florida Atlantic University for supporting this work.

References

[1] Xu Li, Rongxing Lu, Xiaohui Liang, Xuemin Shen, Jiming Chen, and Xiaodong Lin. Smart community: An internet of things application. *Communications Magazine, IEEE*, 49(11):68–75, 2011.

[2] Ragunathan Raj Rajkumar, Insup Lee, Lui Sha, and John Stankovic. Cyber-physical systems: the next computing revolution. In *Proceedings of the 47th Design Automation Conference*, pages 731–736. ACM, 2010.

[3] Kyoung-Dae Kim and Panganamala R Kumar. Cyber–physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100(Special Centennial Issue):1287–1308, 2012.

[4] Jay Taneja, Randy Katz, and David Culler. Defining cps challenges in a sustainable electricity grid. In *Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems*, pages 119–128. IEEE Computer Society, 2012.

[5] Insup Lee, Oleg Sokolsky, Sanjian Chen, John Hatcliff, Eunkyoung Jee, BaekGyu Kim, Andrew King, Margaret Mullen-Fortino, Soojin Park, Alexander Roederer, et al. Challenges and research directions in medical cyber–physical systems. *Proceedings of the IEEE*, 100(1):75–90, 2012.

[6] Hamza Fawzi, Paulo Tabuada, and Suhas Diggavi. Secure estimation and control for cyber-physical systems under adversarial attacks. *Automatic Control, IEEE Transactions on*, 59(6):1454–1467, 2014.

[7] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli. Cyber–physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 100(1):195–209, 2012.

[8] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13, 2011.

[9] Henrik Sandberg, André Teixeira, and Karl H Johansson. On security indices for state estimators in power networks. In *First Workshop on Secure Control Systems (SCS), Stockholm, 2010*, 2010.

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

[11] Yilin Mo, Rohan Chabukswar, and Bruno Sinopoli. Detecting integrity attacks on scada systems. *Control Systems Technology, IEEE Transactions on*, 22(4):1396–1407, 2014.

[12] Miroslav Pajic, Shreyas Sundaram, George J Pappas, and Rahul Mangharam. The wireless control network: A new approach for control over networks. *Automatic Control, IEEE Transactions on*, 56(10):2305–2318, 2011.

[13] Shreyas Sundaram and Christoforos N Hadjicostis. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *Automatic Control, IEEE Transactions on*, 56(7):1495–1508, 2011.

[14] Yilin Mo, Emanuele Garone, Alessandro Casavola, and Bruno Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *Decision and Control (CDC), 2010 49th IEEE Conference on*, pages 5967–5972. IEEE, 2010.

[15] A. Teixeira, I. Shames, H. Sandberg, and K.H. Johansson. A secure control framework for resource-limited adversaries. *Automatica*, 51:135 – 148, 2015.

[16] Y. Mo, S. Weerakkody, and B. Sinopoli. Physical au-

thentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. *Control Systems, IEEE*, 35(1):93–109, Feb 2015.

[17] S. Weerakkody and B. Sinopoli. Detecting integrity attacks on control systems using a moving target approach. *Decision and Control (CDC), 2015 IEEE 54th Annual Conference on*, pages –, Dec 2015.

[18] Carlo Bellettini and Julian L Rrushi. Vulnerability analysis of scada protocol binaries through detection of memory access taintedness. In *Information Assurance and Security Workshop, 2007. IAW'07. IEEE SMC*, pages 341–348. IEEE, 2007.

[19] Eric J Byres, Dan Hoffman, and Nate Kube. On shaky ground–a study of security vulnerabilities in control protocols. *Proc. 5th American Nuclear Society Int. Mtg. on Nuclear Plant Instrumentation, Controls, and HMI Technology*, 2006.

[20] Albert Treytl, Thilo Sauter, and Christian Schwaiger. Security measures for industrial fieldbus systems-state of the art and solutions for ip-based approaches. In *Factory Communication Systems, 2004. Proceedings. 2004 IEEE International Workshop on*, pages 201–209. IEEE, 2004.

[21] Steven Cheung, Bruno Dutertre, Martin Fong, Ulf Lindqvist, Keith Skinner, and Alfonso Valdes. Using model-based intrusion detection for scada networks. In *Proceedings of the SCADA security scientific symposium*, volume 46, pages 1–12. Citeseer, 2007.

[22] Niv Goldenberg and Avishai Wool. Accurate modeling of modbus/tcp for intrusion detection in scada systems. *International Journal of Critical Infrastructure Protection*, 6(2):63–75, 2013.

[23] Man-Ki Yoon and Gabriela F Ciocarlie. Communication pattern monitoring: Improving the utility of anomaly detection for industrial control systems. In *NDSS Workshop on Security of Emerging Networking Technologies*, 2014.

[24] Stephen E McLaughlin, Saman A Zonouz, Devin J Pohly, and Patrick Drew McDaniel. A trusted safety verifier for process controller code. In *NDSS*, 2014.

[25] Sibin Mohan et al. S3a: secure system simplex architecture for enhanced security of cyber-physical systems. *arXiv preprint arXiv:1202.5722*, 2012.

[26] Helge Janicke, Andrew Nicholson, Stuart Webber, and Antonio Cau. Runtime-monitoring for industrial control systems. *Electronics*, 4(4):995–1017, 2015.

[27] Saman Zonouz, Julian Rrushi, and Steve McLaughlin. Detecting industrial control malware using automated plc code analytics. *Security & Privacy, IEEE*, 12(6):40–47, 2014.

[28] Jan-Ole Malchow, Daniel Marzin, Johannes Klick, Robert Kovacs, and Volker Roth. Plc guard: A practical defense against attacks on cyber-physical systems. In *Communications and Network Security (CNS), 2015 IEEE Conference on*, pages 326–334. IEEE, 2015.

[29] Dina Hadžiosmanović et al. Through the eye of the plc: semantic security monitoring for industrial processes. In *Proceedings of the 30th ACSAC*, pages 126–135. ACM, 2014.

[30] Marco Caselli, Emmanuele Zambon, Jonathan Petit, and Frank Kargl. Modeling message sequences for intrusion detection in industrial control systems. In *Critical Infrastructure Protection IX*, pages 49–71. Springer, 2015.

[31] Stephen E McLaughlin. On dynamic malware payloads aimed at programmable logic controllers. In *HotSec*, 2011.

[32] Stephen McLaughlin and Patrick McDaniel. Sabot: specification-based payload generation for programmable logic controllers. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 439–449. ACM, 2012.

[33] Düssel et al. Cyber-critical infrastructure protection using real-time payload-based anomaly detection. In *Critical Information Infrastructures Security*, pages 85–97. Springer, 2009.

[34] Abdulmohsen Almalawi, Xinghuo Yu, Zahir Tari, Adil Fahad, and Ibrahim Khalil. An unsupervised anomaly-based detection approach for integrity attacks on scada systems. *Computers & Security*, 46:94–110, 2014.

[35] Wei Gao, Thomas Morris, Bradley Reaves, and Drew Richey. On scada control system command and response injection and intrusion detection. In *eCrime Researchers Summit (eCrime), 2010*, pages 1–9. IEEE, 2010.

[36] Quickdraw SCADA IDS. http://www.digitalbond.com/tools/quickdraw/.

[37] Andreas Paul, Franka Schuster, and Hartmut König. Towards the protection of industrial control systems–conclusions of a vulnerability analysis of profinet io. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 160–176. Springer, 2013.

[38] Martin Roesch et al. Snort: Lightweight intrusion detection for networks. In *LISA*, volume 99, pages 229–238, 1999.

[39] Robert Mitchell and Ing-Ray Chen. Specification based intrusion detection for unmanned aircraft systems. In *Proceedings of the first ACM MobiHoc workshop on Airborne Networks and Communications*, pages 31–36. ACM, 2012.

[40] Robert Mitchell and Ray Chen. On survivability of mobile cyber physical systems with intrusion detection. *Wireless personal communications*, 68(4):1377–1391, 2013.

[41] Kyungseo et al. Abnormal human behavioral pattern detection in assisted living environments. In *Proceedings of the 3rd International Conference on PErvasive Technologies Related to Assistive Environments*, page 9. ACM, 2010.

[42] Sooyeon Shin, Taekyoung Kwon, Gil-Yong Jo, Youngman Park, and Haekyu Rhy. An experimental study of hierarchical intrusion detection for wireless industrial sensor networks. *Industrial Informatics, IEEE Transactions on*, 6(4):744–757, 2010.

[43] Upeka Kanchana Premaratne, Jagath Samarabandu, Tarlochan S Sidhu, Robert Beresh, and Jian-Cheng Tan. An intrusion detection system for iec61850 automated substations. *Power Delivery, IEEE Transactions on*, 25(4):2376–2383, 2010.

[44] Jared Verba and Michael Milvich. Idaho national laboratory supervisory control and data acquisition intrusion detection system (scada ids). In *Technologies for Homeland Security, 2008 IEEE Conference on*, pages 469–473. IEEE, 2008.

[45] Jianhua Shi, Jiafu Wan, Hehua Yan, and Hui Suo. A survey of cyber-physical systems. In *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on*, pages 1–6. IEEE, 2011.