Cogent Engineering

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/oaen20

A systematic review to aligning research paths: Energy cyber-physical systems

Efe Francis Orumwense & Khaled Abo-Al-Ez |

To cite this article: Efe Francis Orumwense & Khaled Abo-Al-Ez | (2019) A systematic review to aligning research paths: Energy cyber-physical systems, Cogent Engineering, 6:1, 1700738, DOI: 10.1080/23311916.2019.1700738

To link to this article: https://doi.org/10.1080/23311916.2019.1700738

Published online: 13 Dec 2019.

Orumwense & Abo-Al-Ez, *Cogent Engineering* (2019), 6: 1700738
https://doi.org/10.1080/23311916.2019.1700738

cogent engineering

ELECTRICAL & ELECTRONIC ENGINEERING | REVIEW ARTICLE

A systematic review to aligning research paths: Energy cyber-physical systems

Efe Francis Orumwense[1*] and Khaled Abo-Al-Ez[1]

Abstract: Cyber-Physical Systems (CPS) is a new generation of digital technology that is concerned with the integration and inter-dependencies of the cyber and physical world alongside computational elements. As a new and leading technology, its applications are seen in different projects involving energy and this has however generated lots of interest from the industry, researchers in academia and the government. This paper presents an extensive overview and modernistic research on the applications relating to energy CPS and the security issues and challenges revolving around this research path. In order to achieve this, a systematic literature review was carried out which enabled the analysing and classifying of different applications and security issues described in selected publications. Furthermore, the systematic review permitted the discourse stringing these research areas as well as providing future lines of research. Also, results from the review show the paths where there are increasing research focus and expected research trend in the future years to come. These results will not only be useful in serving as a guide to researchers but will also create new research paths to more experienced researchers to actively follow.

Received: 09 August 2019
Accepted: 01 December 2019
First Published: 11 December 2019

*Corresponding author: Efe Francis Orumwense, Centre for Distributer Power and Electronic Systems, Cape Peninsula University of Technology, South Africa
E-mail: efe.orumwense@gmail.com

Reviewing editor:
Qingsong Ai, Wuhan University of Technology, Wuhan, China

Additional information is available at the end of the article

Efe Francis Orumwense

ABOUT THE AUTHOR

Efe Francis Orumwense received his B.Sc (Hons) degree from the School of Engineering, University of Benin, Benin City, Nigeria, his Master's and Doctorate degree from the School of Electrical, Electronic and Computer Engineering, University of KwaZulu-Natal, Durban, South Africa. He rejoined the University of Benin as a Lecturer in 2014. He later worked at Durban University of Technology, Durban, South Africa and rose to the position of Campus Coordinator for Gen. Modules in 2018.
Dr. Efe Orumwense is currently a Post-Doctoral Researcher at the Centre for Distributed Power and Electronic Systems (CDPES) at the Cape Peninsula University of Technology, Cape Town, South Africa. He has authored/co-authored a number of refereed peer-reviewed journal papers, books and conferences both nationally and internationally. He is also supervising post-graduate students in the field of energy and communications. His research interest includes cognitive radio technology, energy efficient systems, network communications, smart grids, internet of things and engineering education.

PUBLIC INTEREST STATEMENT

Cyber-physical systems is a type of heterogeneous system that integrates computational elements with physical properties to ensure a common goal. The interaction between the physical components and the cyber or computational components is done by embedding computers and networks to control and monitor the physical processes. In this paper, an extensive and systematic literature review is carried out on the applications of energy cyber-physical systems and the security issues in the system. The results from this research will assist and enable scholars and researchers to learn new approaches and pave research paths in this research field.

Subjects: Industrial Engineering & Manufacturing; Power & Energy; Electrical & Electronic Engineering

Keywords: cyber-physical systems; applications; security; energy; review

1. Introduction

From years past, researchers in the field of controls and systems have been working on developing efficient and resourceful tools and techniques for evaluating, examining and controlling physical processes, while researchers in the field of computing and electronics have also been trying to achieve a similar feet in cyber systems (Baheti & Gill, 2011). Nevertheless, there still lie a huge disconnect between the physical world where energy and mass transformation takes places and the cyber world where there is transformation and exchange of data and information (Dillon & Chang, 2010). Recently, there have been a massive revolution in the Information Technology (IT), computing and communications sectors where computing gadgets and devices are now more efficient, smaller and faster, communications and communication networks are now less expensive, faster and better. This no doubt have also had a significant impact on energy systems. To further buttress this transformation, objects, structures and entities in the physical environment are now equipped with communication and computing capabilities as well as the components of energy-related systems (Gilroy, 2010). The merger of cyber and physical systems with energy-efficient capabilities that possesses the features of flexibility, security, reliability, sustainability and efficiency poses new challenges to researchers and engineers in this field (Farhangi, 2010; Ilic, Xie, Khan, & Moura, 2010; Lemmon & Venkataramanan, 2009). Hence, a system that possesses cyber abilities integrated into each physical components and all unified to form a large Networked Control Systems (NCS) with efficient control and modelling methodologies can be seen as an alternative tool to resolve these challenges. That means an ideal methodological combination of both systems (physical and cyber) is the main ingredient in forming a Cyber-Physical System (CPS).

CPS can be termed as a new generation of digital systems that combines functional components of the cyber and physical world. It consists of advanced connectivity that guarantees the process of acquiring data from the physical world as well as feedback information from the cyber space with intelligent data computational, analytics and management abilities that constructs the cyber space to ensure a common goal (Baheti & Gill, 2011; Lee, 2008, 2015).

2. Concepts, features and characteristics

CPS has categorically been in existence since the early '70s when the first microprocessors were invented and put into use (Wolf, 2009), but it was not until the year 2006 at the General National Science Foundation meeting, in the USA that Helen Gill coined the name Cyber-Physical System as a term used to describe a system connecting both the physical and cyber world (Gill, 2006). After then, CPS has continued to be an emerging multi-disciplinary area which includes the juxtaposing, overlapping and involvement of various fields in engineering and science. The concept of CPS is so broad and encompassing that it allows an automation and control engineer, a mechanical engineer, chemical engineer, civil engineer and a biologist to collaborate closely with computer scientist and network professional experts to model a workable system. Due to this, the definition of CPS is given by how these different scholars view it in their own disciplines, perspectives and scientific communities.

In the paper by (Kim & Kumar, 2013), CPS is defined as the next generational engineering systems that involves the combination of communication, hi-tech computing and control technologies to accomplish high performance and efficiency, reliability, robustness and stability in physical systems applications involving transportation, medical, defence and energy. Lee (2007) also described CPS as a scalable, controllable and credible network of physical equipment systems that is deeply integrated with control, communications and computational abilities on the foundation of environmental perception. In Ding, Han, Xiang, Ge, and Zhang (2018), CPS is expressed as a heterogeneous, geographically dispersed, life-critical and large-scaled systems

incorporated with devices like actuators and sensors to enable the system monitor, control and sense the physical world. Also in Gunes, Givargis, and Vahid (2014), CPS is defined as "*a complex, physically-aware next generation engineered systems that integrates embedded computer technology (cyber part) into the physical phenomena by using transformative research approaches. This integration mainly includes observation, communication and control aspects of the physical systems for multi-disciplinary perspective*". It however can be very safe to say that several research branches and areas are closely linked or interconnected to CPS. Lee (2015) outlined the differences and similarities between CPS and several research terminologies and fields including Cybernetics, Machine-to-Machine (M2M), Big Data and Internet of Things (IoT).

CPS normally consists of three major components which are the physical system, networking and communication elements and the distributed cyber system. In a typical CPS, the distributed software component plays a key role as it is responsible for processing, filtering and storing information. CPS operates in a three-layer mode which are perception, transmission and application (Ashibani & Mahmoud, 2017). The perception layer which is sometimes regarded as the sensory layer are embedded in devices such as cameras, GPS, readers, actuators, sensors and RFID tags to enable the collection of real-time data from the application layer. The transmission layer which is also referred to as network layer assists in the processing and interchanging of data between the processing layer and application layer. This is achieved with the aid of several communication technologies like Zigbee, Infra-red, Bluetooth, Wi-Fi, LANs or even the Internet. In the application layer, information obtained from the transmission layer is processed and commands are issued to the actuators and sensors for execution which in turn enables a smart environment.

There exist several characteristics of CPS such as mass computing, dynamic reconfiguration, large-scaled diversified networks and highly automated control circuits, but the major characteristics of CPS comprise of reliability, scalability and distributed real-time applications involving real-time control, real-time forecasting and real-time monitoring.

Energy in Cyber-Physical Systems is basically looking at CPS in the energy point of view or the integration of computing, communication and control in the energy domain. This is seen as an important class of CPS as it contributes significantly to the economic, environmental and the social outlook and perspective of CPS. It encompasses the generation (renewables and conventional), distribution and transportations as well as energy storage of a system (Stamatescu, Stamatescu, Arghira, F˘ag˘ar˘asan, & Iliescu, 2014). There exist plenty of research interest on how energy in CPS can be integrated and deployed in various systems. Hence, the main aim of this study is to review cyber-physical systems relating to energy with the objective of providing valuable insight to its applications and security challenges. Our key motivation for this research article is to assist researchers with well-detailed and up-to-date information that would enable them access this field easily and also to enlighten experts in the field on what has been developed and accomplished so far and with a possible avenue to creating future research paths. The remainder of this paper is organised thus—section 3 presents the methodology used for this study while section 4 details the findings from our analysis of different publications. In section 5, discussions arising from the findings in section 4 are presented and section 6 concludes the paper.

3. Methodology

For this review, the Kitchenham's systematic literature review methodology or procedure (Kitchenham et al., 2010) is used. This procedure is often used in software engineering researches and has been very successful in this regard. Due to its success and easy implementation, other fields like education, economics, management and nursing have adopted its usage. In conducting our research, we address our study based on the following actions in this order—

- Research question formulation
- Search processes

- Inclusion criteria
- Exclusion criteria
- Quality assessment
- Data collection
- Data analysis

When conducting research, the very first process is to formulate research questions that entail the basis and focus of the study. These questions are rooted from the analysis of the different issues expressed in different works in the research field. The academic research papers and paper reports examined in this article have been read in order to answer the two formulated research questions deduced for this study.

RQ1. What are the applications of cyber-physical systems as it relates to energy?

RQ2. What are the security issues and concerns in energy cyber-physical systems?

The next process is the search process. The strategy adopted for searching the literature for this research is to systematically search citation databases and relevant digital libraries using keywords and search strings. The keywords combined to create a search string for these research are *cyber physical system, cyber physical energy systems, energy cyber physical system, application of cyber physical systems, security cyber physical systems, issues in cyber physical system, energy CPS, security CPS* and *cyber physical systems issues*.

The inclusion and exclusion criteria for this review article are the criteria for including and excluding research papers from the study in order to refine the search. For our inclusion criteria, papers that are related and relevant to any of the keywords used in the search are included. Papers from January 2010 to July 2019 were considered and included in this study. While for the exclusion criteria, papers that were not written in English were excluded. Also, papers that do not have concrete evidence to back up the research or are not clear enough or have focused entirely on another topic area were excluded. Papers that do not deal explicitly on CPS were also excluded. Table 1 shows the trend and statistics of publications on CPS applications and security.

In the next process, data is collected and analysed from the selected papers. The data collected from these papers are analysed applying a standard template across the board. Afterwards, the work is then classified and categorized using the research questions previously formulated.

Table 1. Article sources and the number of articles found

Article Source	Number of article	Number of article in Conferences	Number of article in Journals
Google Scholar	13	7	6
IEEE Xplore Digital Library	40	30	10
ACM Digital Library	2	1	1
Science Direct	18	1	17
Scopus	4	0	4
Springer Link	5	0	5
Total	82	39	43

4. Results

In this section, we evaluate the findings of the literature review carried out. We start holistically and then begin to narrow down to the concentration of our study by categorizing them into different parts depending on their area of application or security.

4.1. Energy applications in cyber-physical systems

RQ.1 means that this study is to concentrate on the applications of cyber-physical systems in an energy perspective. For this purpose, the literature previously gathered was broken down into different parts to enable us to identify the applications of CPS. It is identified that there are various applications of CPS as it applies to different areas of research. Most of the areas found in the literature that studied the applications of CPS are in agriculture, medicine and health care, process control, intelligent transportation and smart cars, smart grid and smart cities, smart manufacturing, environmental monitoring, energy management and robotics. We will, however, focus on the applications related to energy and group our research findings into different categories.

4.1.1 Smart grid and smart cities

Smart grids are intelligent types of electric network that uses modern technologies to deliver a more reliable and efficient energy supply. Smart grids combine power network infrastructure which we can regard as the physical system with sensors, actuators, and the ICT and communications aspect which we can regard as the cyber system to deliver an intelligent and smarter type of electric network. The publications in this area of research are seen in Table 2.

The paper by Yu and Xue (2016) evaluates the challenges associated with smart grid in the cyber-physical system context. They also identified the possible and likely contributions that CPS can offer to smart grids and showed an architectural design system that incorporates communication, computation and control for the deployment of a CPS. Also, open questions were also raised and these questions will affect the future development of CPS and smart grids. In the paper by Cintuglu, Mohammed, Akkaya, and Uluagac (2017), the authors present a range of testbeds relating cyber-physical systems to smart grid with an aim to providing important features, a wider categorization and design decisions for its development. The paper went on to categorize and classify the cyber-physical smart grid domain into four steps and investigated them individually according to their various criteria. It was also concluded by the authors that improved communication infrastructure in the system is very vital as its data communication, privacy and security will give a better opportunity to combine testbeds with different capabilities.

Table 2. Publications in the smart grid and smart cities research area

Research Area	References	Year of publication
Smart Grids	(Yu & Xue, 2016)	2016
	(Farraj et al., 2018)	2018
	(Allen et al., 2012)	2012
Smart Grid Testbeds	(Cintuglu et al., 2017)	2017
Social smart grids	(Cheng et al., 2016)	2016
	(Zhang et al., 2018)	2018
Software associated smart grids	(Horcas et al., 2019)	2019
	(Xin et al., 2017)	2017
Smart cities	(Cassandras, 2016)	2016
Smart home	(Seiger et al., 2016a)	2016
	(Mazumdar et al., 2016)	2016
	(Seiger et al., 2016b)	2016

The only two models that studied energy in cyber-physical systems in a social view point was found in Cheng, Zhang, and Yang (2016) and Zhang, Xu, and Yu (2018) as also documented in Table 1. A consumer-centred energy system is proposed in Cheng et al. (2016) where a cyber-physical social system combines a physical component which is the power grid and the cyber component which involves computing, communications and consumer interactions (social). The importance of consumer-centred energy system with respect to effective energy utilization was also discussed and an architecture capable of achieving flexible and intelligent energy management for smart grids was also presented. The work in (Zhang et al., 2018) also presents a novel cyber-physical social system with parallel learning for microgrid systems. The work was carried out to solve the human participation and interaction in microgrids. A case study of a microgrid with 11 energy suppliers and 7 energy consumers was used and the technique showed that computer-human collaboration can achieve a higher quality of distributed energy management when compared to other centralized heuristic algorithms.

Farraj, Hammad, and Kundur (2018) presents a cyber-physical control framework for transient stability in smart grids. In this work, a parametric feedback linearization (PFL) controller is utilized to solve the issues associated with the stability of power systems. The PFL controller uses an external vitality capacity framework to absorb and infuse power from the system in order to ensure the stability of the rotor speed. In the paper by Allen, Liu, Lozano, and Yuan (2012), it was confirmed that smart grid is critical in terms of infrastructure and a decentralized, hierarchical framework was proposed to detect and mitigate potential cascade failures. The authors experimented the technique in real life and it was deduced that cascading failures are initiated by interactions developed between contingencies, protective relays and power flow switching among and around the studied zones.

The paper by Horcas, Pinto, and Fuentes (2019) addresses the problem of developing context-aware energy-efficient application for CPS with the aid of a green eco-assistant that utilizes innovative software engineering techniques. This assist software inventors and developers to be increasingly aware of the energy consumption in the associated hardware systems. Also in Xin et al. (2017), an information-energy flow model is developed using a matrix-based computational approach. The energy information flow was calculated in an IEEE 14-node system to help estimate the impacts of various cyber contingencies on a power system.

Smart cities and smart homes are seen in literature to use the CPS applications for innovative facilities like energy distribution, emergency response services, businesses, commerce and so on. Four papers were found that linked energy cyber-physical systems with smart cities and smart homes. The paper (Cassandras, 2016), identifies the main defining characteristics of a smart city as it relates to CPS and considered the smart city as a CPS with a new software platform. In Seiger, Huber, and Schlegel (2016a), an integrated system called PROtEUS is designed for process implementation in CPS. This integrated system unifies components for event processing, human interaction, dynamic service selection and data routing. Two case studies of a smart home domain are used to test its feasibility. Mazumdar and other authors in Mazumdar et al. (2016) introduce a project named AXIOM with an aim to developing a hardware-software platform for CPS to enable easy parallel programming and to easily scale up the performance of the system by adding multiple boards. Smart home living applications and smart video surveillance are used to achieve this design. Lastly, the authors in Seiger, Struwe, Lemme, and Schlegel (2016b), developed a mobile control centre that is user-friendly for cyber-physical systems in the smart home domain with the aim of lessening the hitches in utilising CPS with numerous control options and enabling the system to be more user-friendly to non-expert users.

4.1.2 Intelligent transportation and smart cars

Energy can be conserved and utilized efficiently through the use of smart cars while safety, traffic management, coordination and throughput can be improved through the sharing of real-time information using intelligent transportation systems. In these systems, advanced technologies involving computational software, communication, sensing and control mechanisms are all imbedded in transportation systems like cars, trains and aeroplanes to reduce traffic fatalities. The involvement of CPS in these areas has been found in 14 papers in literature as documented in Table 3.

Table 3. Publications in the intelligent transportation and smart cars research area

Research Area	References	Year of publication
Vehicular CPS	(Bradley & Atkins, 2015)	2015
	(Kumar et al., 2015)	2015
	(Ma et al., 2015)	2015
	(Wan et al., 2014)	2014
Aviation CPS	(Sampigethaya & Poovendran, 2013)	2013
	(Sampigethaya & Poovendran, 2012)	2012
Transportation System	(Zhou et al., 2016)	2016
	(Zhou et al., 2013)	2013
	(Wan, Chen, Xia, Li, & Zhou, 2013)	2013
	(Rawat et al., 2015)	2015
	(Besselink et al., 2016)	2016
	(Möller & Vakilzadian, 2016)	2016
Others	(Kantarci, 2015)	2015
	(Smirnov et al., 2017)	2017

The papers (Bradley & Atkins, 2015; Kumar, Bali, Iqbal, Chilamkurti, & Rho, 2015; Ma, An, Huang, & Cao, 2015; Wan et al., 2014), all examined the concept of vehicular cyber-physical systems. In Bradley and Atkins (2015), cyber-physical vehicle systems is presented where the authors examined various factors like sensor scheduling, task and motion planning, resource sharing, time-varying sampling patterns and feedback scheduling to co-optimize and co-regulate applications in CPS vehicular systems. In Kumar et al. (2015), a stochastic coalition game in a typical vehicular CPS setting is proposed where the vehicles acting as players in the game receive a limited number of resources from the cloud. Also in Ma et al. (2015), Dempster's rule is utilized to improve and resolve the problem of sensor data fusion in vehicular CPS. The results obtained showed that eliminating the issue of conflicting evidence combination yields an improved convergence performance.

The author (Kantarci, 2015), initiates a minimum Steiner tree approach for path selection for paramedics with the aid of cyber-physical systems consisting of human interaction components and vehicular communications. This approach yields an alternative routing selection for paramedics with minimal cost, minimal delay and increased resilience. Traffic measurements in CPS-based transportation are documented in Zhou, Mo, Xiao, Chen, and Yin (2016) and Zhou, Xiao, Mo, Chen, and Yin (2013) where measurements are obtained from various vehicles commuting from one geographical location to the other with the aid of an intelligent cyber-physical road system that is capable of collecting traffic data. In Wan, Chen, et al.(2013), it was proved that CPS is an evolution of Machine2Machine with additional interactive operations and intelligent software. In doing this, two CPS platforms are reviewed including a vehicle with WSNs navigation and cyber transportation system. In Rawat, Bajracharya, and Yan (2015), a study of how different parameters affect communication in smart transportation CPS was carried out.

Not much work have been carried out in terms of intelligent transportation relating to the aviation industry. Nonetheless, a novel CPS scheme that focuses on the cyber component and the cyber-physical interaction in aviation is proposed in Sampigethaya and Poovendran (2013) and Sampigethaya and Poovendran (2012). The work in Sampigethaya and Poovendran (2013) evaluates the integration of CPS in aircraft management including aircraft performance, air traffic, aviation users, flight deck and so on while the work in Sampigethaya and Poovendran (2012) proposes a new CPS

framework for air traffic management and airspace system design to improve interactions in aircraft and airspace.

A Vehicular CPS architecture with the integrated mobile cloud computing system is analysed in Wan et al. (2014) where sensors deployed in the system capture data from a vehicle on a daily basis and store it in a vehicle storage space. A large transportation system based on CPS is studied in Besselink et al. (2016) where an approach sub-divided into layers is used to control platooning vehicles and coordinate transport planning. A CPS for connected car-based e-tourism is presented in Smirnov, Shilov, and Gusikhin (2017) using the cloud to deliver tourist context services, car context services or recommendation services. The system can be integrated into the car information system for planning and scheduling customized visual information and guides based on location. Transportation in CPS including travel time prediction, applications in smart traffic light system and small transportation are all documented in Möller and Vakilzadian (2016).

4.1.3 Industries and smart manufacturing

In the research area of industries and smart manufacturing, researchers evaluate and design architectural platforms to apply CPS in production and manufacturing in order to alleviate problems associated with flexibility, large work force and high energy demand. There are a total of 13 papers found in this area that concentrates on the use of hardware and embedded software technologies to optimize productivity in the manufacturing sector as tabulated in Table 4. The work by Basile, F, Chiacchio, Coppola, and Gerbasio (2015) presents elementary results from designing a suitable distributed control architecture for automated warehouse systems with the aid of functional blocks and cyber-physical systems. The work in Wiesner, Marilungo, and Thoben (2017) introduces a product service-oriented CPS tagged as "cyber-physical product-service systems" and its application in the industry is evaluated. In Monostori et al. (2016), a production design architecture consisting of different levels is analysed. The authors used a cyber-physical module as a case study to research on various production and work applications such as adaptive scheduling, maintenance strategy and automated generation. A self-controlling manufacturing system that sees humans as a component is discussed in Graessler and Poehler (2018) where intelligent controls for manufacturing systems and digital twins approach are proposed for industrial level usage.

Lu and Ju (2017) introduces a service-oriented architecture for industry and smart manufacturing using the CPS concept. The proposed architecture is used to enhance communication between service

Table 4. Publications in the industries and smart manufacturing area of research

Research Area	References	Year of publication
Industry 4.0	(Agbor et al., 2018)	2018
	(Novak et al., 2017)	2017
	(O'Donovan et al., 2018)	2018
	(Hiang, 2018)	2018
Smart Manufacturing	(Lu & Ju, 2017)	2017
	(Kim & Park, 2017)	2017
	(Weyer et al., 2016)	2016
Product Services	(Wiesner et al., 2017)	2017
	(Monostori et al., 2016)	2016
	(Graessler & Poehler, 2018)	2018
	(Herwan et al., 2018)	2018
Industry Controls	(Basile et al., 2015)	2015
	(Lemoine et al., 2018)	2018

request and service consumption and provides appropriate conceptual models for describing and developing manufacturing in CPS and enabling its composition. In Agbor, Cao and Ehmann (2018), a conceptual framework that assists in the selection of correct manufacturing process is conceptualized with the aid of a constraint satisfaction problem. It also provide guidelines for implementers in the manufacturing sector most especially for the industry 4.0 revolution. A human-based and industrial based cyber-physical system is introduced in Lemoine, Berdal, Enjalbert, and Trentesaux (2018) where the authors analysed how possible it will be to involve a human being in the cyber physical-based industry controls. This approach combined industrial CPS and Human-Machine Systems to achieve the goal. In order to deliver an adaptive and autonomous system in machining line in industries, authors in Herwan, Kano, Oleg, Sawada and Kasashima (2018) introduce a CPS production system that will aid tool wear and breakages and also surface roughness monitoring. However, in Novak, Kadera, and Wimmer (2017), the same goal was achieved with the aid of a P'X5 configurator for the Industry 4.0 applications. In O'Donovan, Gallagher, Bruton, and O'Sullivan (2018), the research introduces an industrial CPS based on fog computing paradigm using Predictive Modelling Markup Language (PMML) encoded machine learning models for industry 4.0 applications. Also in Hiang (2018), a smart factory based on CPS that includes a smart factory data center based on the cloud environment and an industrial IoT gateway is looked at for the concept of industry 4.0 application. The paper by Kim and Park (2017) proposes a new optimization strategy for manufacturing systems through the combination of CPS and IoT. Lastly, a paper that proposes a scheme for modelling and simulation of CPS-based factories is seen in Weyer, Weyer, Ohmer, Gorecky, and Zuhlke (2016). This framework was applied in the automotive industry for validation.

4.1.4 Environmental monitoring and energy management

In terms of environmental monitoring and energy management, energy can be conserved and managed since CPS is regarded as a distributed system. In environmental monitoring systems, CPS is distributed relatively over a large geographical location without human involvement for a lengthy period of time with minimal energy consumption. In this sense, Man-made and natural disasters can be averted through CPS by instantly responding to various sensors spread over a geographical area. In this research path, seven papers were found to have targeted this area of research as seen in Table 5. In the paper by Sanislav et al. (2014), the authors introduce an open CPS architecture with a high degree of scalability and reliability that can be applied in environmental monitoring. The architecture is broken into three different layers, the bottom layer permits the acquiring of data and their transfer to other layers while the middle and top layer is responsible for the appropriate and correct function of the CPS based on decision rules and complex data analysis. In the work by Sierla, O'Halloran, Karhela, Papakonstantinou, and Tumer (2013), an architecture for modelling communications between CPS and the environment is presented. The approach has to identify component failures emerging from abnormal environmental conditions and also determine the effects with respect to the degradation or loss of the functionality of the system. A CPS for environmental monitoring that encompasses the ecological states such as

Table 5. Publications in the environmental monitoring and energy management research area

Research Area	References	Year of publication
Environmental Monitoring	(Sanislav et al., 2014)	2014
	(Sierla et al., 2013)	2013
	(Padher & Rohokale, 2018)	2018
Energy Management	(Li et al., 2016)	2016
	(Wan, Yan, Li, Zhou, & Zeng, 2013)	2013
	(Zhao et al., 2010)	2010
	(Aksanli & Rosing, 2017)	2017

temperature, pressure in remote areas is evaluated in Padher and Rohokale (2018). The system analyses the parameters of an environment based on the IEEE 8002.11 infrastructure.

Managing energy in systems was also captured in some academic papers in literature since a lot of devices and components in CPS require energy for operation. In the paper by Li, Wu, and Li (2016), a dynamic-distributed technique designed for different classes of power systems associated with data attack are presented. In this technique, a dynamic state estimator using a nine-bus power system is used to attain an ideal control of large scale distributed systems. Authors in Wan, Yan et al. (2013) propose a novel CPS energy management application framework that has the ability to collect real-time data of power consumed as well as demand from autonomous electric vehicle and charging centres in a smart grid. The energy-efficient-designed application also incorporates path planning of autonomous electric vehicle in real-time and event-based control using wireless sensor networks. Another conceptual framework of CPS for managing energy in building structures is explored in Zhao, Simoes, and Suryanarayanan (2010). The framework analyses a cyber-enabled efficient building energy management system with a goal of attaining a high level of energy self-sufficiency. The paper by Aksanli and Rosing (2017) conceptualizes the human behavioural awareness for energy management in residential CPS. They showed how human behaviour-based decisions and actions affect residential energy consumption and their results showed high energy savings using the approach.

4.2 Security in energy cyber-physical systems

RQ.2 raises the issue of security in CPS as it relates to energy. In as much as CPS is able to utilize the information obtained in the physical domain to generate low cost and energy-efficient functionalities, it can also be prone and vulnerable to threats and attacks. These attacks which can also be in the form of cyber are constantly on the increase since it is a system that promotes connectivity and smart technologies. Security no doubt has earned a lot of attention in the field of CPS due to its important nature and this is evident from the number of papers found in this category as detailed in Table 6.

Issues relating to privacy and information security and trade-off between security and performance in CPS are highlighted in AlDosari (2017). The author presents a common attack known as Side Channel Attacks (SCA) on cryptographic algorithms and the countermeasures against these attacks. In Alguliyev, Imamverdiyev, and Sukhostat (2018), the main types of attacks on CPS are examined where issues relating to CPS components authentication methods, data security and trust levels are analysed and countermeasures were developed. To enable a feasible and extended life time system architecture of a software-defined CPS, the authors in Wu, Luo, Wang, and Wang (2018) proposes a systematic virtual networking architecture and a novel life time extension scheme that performs a global virtualization control and monitoring of a CPS. A theoretic topology decision system was used and the results show that the proposed architecture improves the energy efficiency and life time of the system. In Wu, Kang, and Li (2015) a quantitative hierarchal assessment model that includes attack success probability, attack severity and attack consequence is proposed. The model has the ability to access the risk caused by an attacker on the host and system stratum of CPS. Also in Vegh and Miclea (2016), another hierarchical system of accessing data which is sent through a digital signature algorithm is proposed. This system is designed to equip CPS with an efficient attack detection signature so as to prevent attacks in CPS.

Historical vulnerability data from databases is used to create a framework that characterizes a set of attributes for each given subsystems in CPS in Bakirtzis, Carter, Elks, and Fleming (2018). This framework is used to capture necessary specificity and match possible attack vectors with the model's attributes. The authors in Khalid et al. (2018) propose a security framework that allows the application of humans in collaboration with robots in the industry 4.0 context of CPS. The paper provided mitigation strategies analysed the cyber vulnerabilities in the system and examined the cyber-attack impacts. In Hong, Wang, Ji, and Beyah (2018), the authors propose an attacker location assessment scheme which is based on fake source scheduling (FSSE) for source location

Table 6. Key characteristics and research areas identified in security in CPS

Research Area	Key issues or characteristics	References	Year of publication
Attack	Side Channel Attacks on Cryptographic Algorithms and countermeasures	(AlDosari, 2017)	2017
	A solution to tree of attacks on CPS is presented	(Alguliyev et al., 2018)	2018
	Attack detection using hierarchical model	(Vegh & Miclea, 2016)	2016
	Eliminating attacks using historical data from database	(Bakirtzis et al., 2018)	2018
	Eliminating cyber-attacks using human-robot collaboration.	(Bakirtzis et al., 2018)	2018
	Attacker location evaluation using fake source scheduling	(Hong et al., 2018)	2018
	A method for modeling and quantitative examination of attacks in CPS is presented	(Orojloo & Azgomi, 2014)	2014
	A new method of quantitative evaluation of adversarial attacks on CPS is proposed	(Orojloo & Azgomi, 2015)	2015
	Mitigation of cyber-attacks on CPS processors with TAIGA	(Lyn et al., 2015)	2015
	Cyber-attack description language is developed for structured description of attacks on CPS	(Yampolskiy et al., 2015)	2015
	Game theoretic method application for attacker and defender interactions.	(Sanjab & Saad, 2016)	2016
	Study of numerous attacks in electrical CPS	(Wang et al., 2016)	2016
	Attack detection scheme using advanced machine learning techniques	(Yan et al., 2019)	2019
	Attack detection scheme based on random set theory to combat cyber-attacks in CPS	(Yang et al., 2019)	2019
	Estimating the impact of a successful physics-based attacks on CPS	(Lanotte et al., 2019)	2019

(*Continued*)

cogent engineering

Table 6. (*Continued*)

Research Area	Key issues or characteristics	References	Year of publication
	Learning based attacks are examined	(Khojasteh et al., 2019)	2018
	A semi supervised novel malware detection is used to provide advanced protection in CPS	(Huda et al., 2017)	2017
	Attack tolerant model is achieved in the CPS using residual observers bank	(Rebaï et al., 2018)	2018
	Attack tolerant control is achieved in the CPS using event based implementation	(Rebai et al., 2018)	2018
Threat	Threats are identified in different layers of CPS	(Gao et al., 2014)	2013
	Security threats are examined in CPS	(Rekik et al., 2018)	2018
	Evaluation of threat detectors	(Bou-Harb, 2016)	2016
	Misuse patterns is used to characterize CPS threats and build a secure system unifying CPS threats	(Fernandez, 2016)	2016
	Threats in CPS and possible recommendations	(Zhang et al., 2013)	2013
Risk	Assessing risk of attack using quantitative hierarchal model	(Wu et al., 2015)	2016
	Risk is assessed in CPS and areas for more scrutiny is identified	(Axelrod, 2013)	2013
Trustworthiness	Providing solutions to ensuring trust in modern CPS	(Konstantinou et al., 2015)	2015
	Trustworthiness is examined CPS	(Boyes, 2013)	2013
	Implication of attack on trust and Stuxnet is examined	(Howser & McMillin, 2014)	2014

(*Continued*)

cogent engineering

Table 6. (*Continued*)

Research Area	Key issues or characteristics	References	Year of publication
Others	Differences between CPS security and cyber security	[97]	2013
	Network function virtualization and software defined networking and are used to extend the lifetime of CPS	(Wu et al., 2018)	2018
	Security in cloud based CPS and smart mobility devices	(Puttonen et al., 2015)	2014
	Data security and confidentiality in solutions in CPS	(Vegh & Miclea, 2016),	2014
	Exploring cyber physical testbed developed using engineering models in CPS	(Nguyen et al., 2017)	2017

privacy in CPS. This scheme assists in maintaining the system performance and enhancing the privacy level, energy consumption and transmission delay. The author in Axelrod (2013) proposes a technique that assists in determining the factors responsible for the high levels of combined risk in a CPS and recommended appropriate methods to conveniently mitigate such risk. Risk across a broad range of CPS both in the private and public sectors is accessed. The work in Zhang, Wang, and Tian (2013) investigates security threats common to CPS while security measures and recommendations to these threats are identified. Authors in Gao et al. (2014), Rekik, Gransart, and Berbineau (2018) also examine the security threats associated with CPS. In Gao et al. (2014), the threats were examined in the application, physical and network layers with their vulnerabilities listed in a management and policy, platform and network point of view while in (Rekik et al., 2018), the threats were examined in new generation of CPS trains and vulnerabilities listed in terms of train control and monitoring systems.

Trustworthiness in CPS is examined in Boyes (2013) and techniques to evaluate the risks and resilience in complex CPS are identified. Attacks that disrupt information flow such as Stuxnet is investigated in Howser and McMillin (2014). In this work, the authors explain the attack's implication on trust and how the attack can be dealt with since it hides behind the multiple security domain non-deducibility. In Orojloo and Azgomi (2014, 2015), the authors propose new approaches for qualitative evaluation and modeling security attacks in CPS and also model the classes of adversarial attacks on systems. The authors in Lyn, Lerner, McCarty, and Patterson (2015) identify the potential outcomes of cyber-attacks launched on CPS embedded processor and creates a trustworthy autonomic interface guardian architecture that ensures communication between the physical processes and the embedded controller of a CPS. The paper by Yampolskiy, Horvath, Koutsoukos, Xue, and Sztipanovits (2015) introduces a type of description language fuelled cyber-physical attacks which serves as a basis for a structured characterization of attacks on cyber-physical systems while the paper by Puttonen, Afolaranmi, Moctezuma, Lobov, and Lastra (2015) surveys security-related issues in cloud-based CPS and also evaluates the problem of security and threats in smart mobility services. Security approaches in CPS and various threat detectors in a CPS environment are evaluated in Bou-Harb (2016) while authors in Fernandez (2016) describe how threats in CPS can be modeled and how it can be unified to build a secure system.

(Sanjab & Saad, 2016), proposes a game-theoretic method to study the interactions of an attacker and a defender in a typical CPS and develop a novel optimal strategy to solve the game putting energy markets and wide-area protection into consideration. Vegh and Miclea (2014), provide solutions for ensuring data security and confidentiality in CPS by combining methods involving steganography and cryptography while Wang et al. (2016) studies the fragility of an electrical CPS under numerous forms of attacks like the false data injection attacks and the denial of service attacks. In the paper Yan, Mestha, and Abbaszadeh (2019), an attack detection scheme was proposed at the physical layer of a CPS by using advanced machine learning techniques or obtaining salient signatures and features from a physical component. To deal with the problem of attackers simultaneously launching multiple cyber-attacks on a CPS, an efficient attack detection scheme base on a random set theory is proposed in Yang, Shi, Zhang, Wu, and Shi (2019). In Lanotte, Merro, Muteanou, and Vigano (2019), a comprehensive model for physics-based attacks, a means of accessing attack tolerance, estimating the impact of a successful attack and its chances and a tool for carrying out static security analysis on a CPS when exposed to attacks is documented. Learning-based attacks in CPS are scrutinized in Khojasteh, Khina, Franceschetti, and Javidi (2019) where an attacker uses an arbitrary learning algorithm to estimate the dynamics of the system.

In the paper by Huda et al. (2017), a novel semi-supervised malware detection system for CPS is proposed. The method is seen to fight against new malware variants without any manual effort or signature generation strategies and also offer advanced protection to CPS. Novel security strategies in CPS are proposed in Rebaï, Voos, and Darouach (2018) and Rebai, Voos, and Alamdari (2018) with the aid of an event-based implementation. Simulation results show that there is an attack-

tolerant control in the system despite the infusion of data deception attacks. Authors in Konstantinou et al. (2015) focus on a research on privacy and security challenges at different layers of the composition of a CPS and also provide solutions to guaranteeing trust in a modern CPS. A systematic mapping study is conducted in Nguyen, Ali, and Yue (2017) to identify 48 primary security engineering models in CPS for data extraction and analysis. The results show that more investigation is needed into security solutions for CPS. It is quite interesting to note that cyber security is different from cyber-physical systems (CPS) security. Cyber-physical systems security is more important than cyber security and the latter is often considered as a sub-unit of security in CPS since cyber security is involved in the cyber side of the system and not the physical component part of the system (Northcutt, 2013).

5. Discussion and future line of research

CPS is constantly gaining more research grounds amongst researchers and this innovative line of research has the potential and ability to revolutionize our relation, communication and interactions with various complex systems which the physical world is largely dependent upon (Kim & Kumar, 2013). Virtually all applications of CPS provide pioneering technologies that are tangible enough to make a great impact in the world. The application categories chosen in this study are highly dependent on energy efficiency, resource reduction or consumption and increasing reliability or performance.

From this study, it is seen that although research on the applications of CPS has made tremendous progress over the years, it is still very new and in a developmental stage. From Figure 1, it can be noticed that lots of researchers have preferably been focusing on the application of CPS in the area of intelligent transportation and smart cars as to when compared to other applications. This is evident from the improved sensing and intelligent transport system and self-driving cars that easily interact with the physical environment. Environmental monitoring and energy management attract less research interest and only a few publications are seen in this field. Studies in various applications of CPS started gaining substantial grounds in 2016 when more researchers from different multi-disciplinary fields became involved in this cutting-edge line of research. It is however expected that this trend will continue and more ground-breaking research will emerge from these applications.

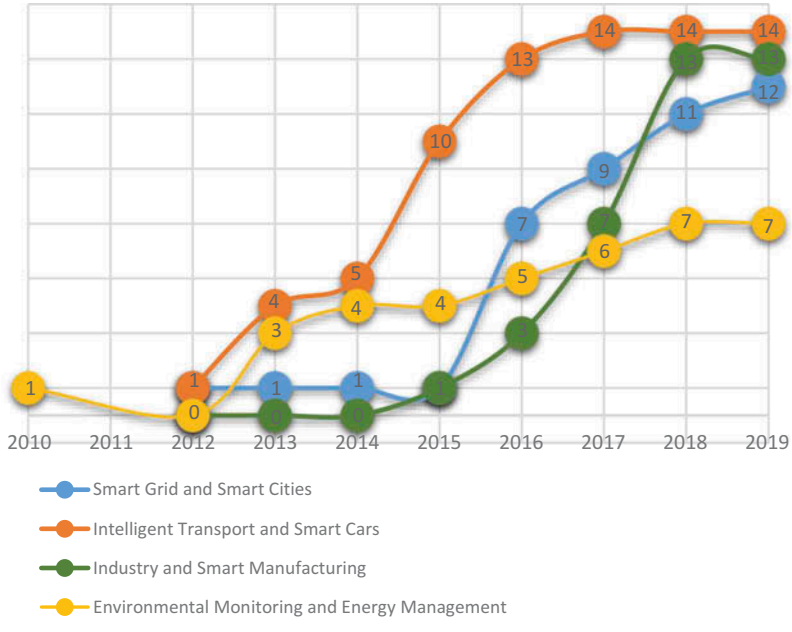

Figure 1. Cumulative number of articles published in the category of applications in energy CPS.

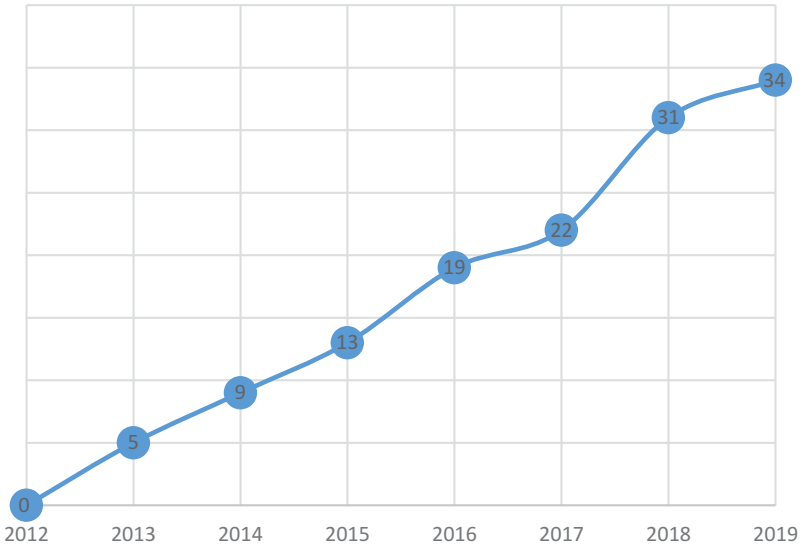

Figure 2. Cumulative number of articles published in the category of security issues in Energy CPS.

CPS applications no doubt face numerous challenges especially in the area of efficiency, security and privacy. Due to the characteristic and intrinsic properties, CPS possesses amongst which are dynamicity, complexity and scalability, it is subjected to various attacks both on the cyber and the physical part of the system. Factors that normally contribute to the vulnerability of CPS making them susceptible to threats and attacks are the use of digital connectivity like the internet, unsecured communication protocols, the use of commercial off-the-shelf technologies and dependency on legacy systems (Gunes et al., 2014). Figure 2 shows the cumulative number of publications on the issue of security as it relates to energy CPS research. It is seen that there is a continual increase in the amount of research in combatting security in this field. From the year 2017, there have been a sharp increase in research activity as issues relating to security in large-scaled systems are being treated.

It is worth mentioning that from Table 1, it is observed that there are a lot of conference papers published in this field of research and this implies that most of the ideas are still in the conceptual stage and a lot of them are novel. Based on the publication search process undertaken in this study, it was observed that CPS is currently gaining more grounds with other interrelated technologies like Machine-2-Machine, Internet of Things, big data, storage and cloud and so on. The combination and merger of these research areas could lead to more technological advancement and breakthrough in the future which is also worth looking at by researchers venturing into this research field. But it will be important if researchers also focus on how these technologies will affect CPS applications and the underlining issues of interoperability, reliability and safety. Also, for future applications, CPS will play a very vital and prominent role in Germany's "Industry 4.0" and China's "Made in China 2025" projects and other CPS related projects in other countries.

6. Conclusion

Cyber-physical system (CPS) is a new technology that integrates cyber and physical components alongside computational elements to achieve high efficiency and performance. The main objective of this paper is to present an up-to-date information and overview on applications relating to energy CPS and also security concerns in the system in order to furnish researchers and scholars with a comprehensive overview on the topic. This study was performed using a Systematic Literature Review methodology that enabled us to search, locate, assess, analyse, and categorize existing selected papers in literature and also identify the connection and relation between papers so as to draw a valid conclusion about its contents. An extensive review of papers was carried out from 2010 to mid-2019 from various databases to assist scholars to learn new approaches in this

research area. From our results, it was seen that this research area is exponentially growing in terms of publications especially in recent years and this confirms the fact that researchers are now more interested in exploring recent theories and technologies from this subject area.

The main limitation of this work is that only publications relating to energy in CPS was selected for this study so as to keep the volume and number of pages of this paper to a required size. Quite a few other CPS research fields were not treated in this paper such as agriculture, robotics, medicine, process control, aerospace systems and education as this will be looked at in future works.

Funding
The authors received no direct funding for this research.

Author details
Efe Francis Orumwense[1]
E-mail: efe.orumwense@gmail.com
ORCID ID: http://orcid.org/0000-0002-3821-910X
Khaled Abo-Al-Ez[1]
E-mail: ABOALEZK@cput.ac.za
[1] Centre for Distributed Power and Electronic Systems, Cape Peninsula University of Technology, Belleville 7535, South Africa.

Citation information
Cite this article as: A systematic review to aligning research paths: Energy cyber-physical systems, Efe Francis Orumwense & Khaled Abo-Al-Ez, *Cogent Engineering* (2019), 6: 1700738.

References

Agbor, E. N., Cao, J., & Ehmann, K. (2018). Towards smart manufacturing process selection in cyber-physical systems,". *Manufacturing Letters*, *17*(1), 1–5. doi:10.1016/j.mfglet.2018.03.002

Aksanli, B., & Rosing, T. S. (2017). Human behavior aware energy management in residential cyber-physical systems. *IEEE Transactions on Emerging Topics in Computing*, 1. doi:doi:10.1109/tetc.2017.2680322

AlDosari, F. (2017). Security and privacy challenges in cyber-physical systems. *Journal of Information Security*, *8*(4), 285–295. doi:10.4236/jis.2017.84019

Alguliyev, R., Imamverdiyev, Y., & Sukhostat, L. (2018). Cyber-physical systems and their security issues. *Computers in Industry*, *100*(1), 212–223. doi:10.1016/j.compind.2018.04.017

Allen, J. D., Liu, X., Lozano, I., & Yuan, X. (2012). A cyber-physical approach to a wide-area actionable system for the power grid, *MILCOM 2012-2012 IEEE Military Communications Conference* (pp. 1–6), Orlando, FL. doi:10.1109/MILCOM.2012.6415666

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computer & Security*, *68*(3), 81–97. doi:10.1016/j.cose.2017.04.005

Axelrod, C. W. (2013). Managing the Risks of Cyber-Physical Systems. In 2013 Systems, Applications and Technology Conf. (LISAT) (pp. 1–6). IEEE: Long Island, New York, USA. doi: 10.1109/LISAT.2013.6578215

Baheti, K., & Gill, H. (2011). Cyber-physical systems, *The Impact of Control Technology,(eds.), IEEE Control Systems Society* (pp. 161–166). Retrieved from www.ieeecss.org

Bakirtzis, G., Carter, B. T., Elks, C. R., & Fleming, C. H. (2018). A model-based approach to security analysis for cyber-physical systems *Presented at 2018 Annual IEEE International Systems Conference (SysCon)*, Vancouver, 2018 (pp. 1–8). doi:10.1109/SYSCON.2018.8369518

Basile, F, Chiacchio, P., Coppola, J., & Gerbasio, D. (2015). Automated warehouse systems: A cyber-physical system perspective. In 2015 IEEE 20th Conf. Emerging Technologies & Factory Automation (ETFA) (pp. 1–4). doi: 10.1109/ETFA.2015.7301597

Besselink, B., Turri, V., Van de Hoef, S. H., Liang, K.-H., Alam, A., Martensson, J., & Johansson, K. (2016). Cyber–Physical control of road freight transport. *Proceedings of the IEEE*, *104*(5), 1128–1141. doi:10.1109/JPROC.2015.2511446

Bou-Harb, E. (2016). A brief survey of security approaches for cyber-physical systems. In 2016 8th IFIP Int. IEEE Conf. New Technologies, Mobility and Security (NTMS) (pp. 1–5). doi: 10.1109/NTMS.2016.7792424.

Boyes, H. A. (2013). Trustworthy cyber-physical systems — A review. IET Conference Proceedings, 3.1-3.1. Retrieved from http://digital-library.theiet.org/content/conferences/10.1049/cp.2013.1707

Bradley, J. M., & Atkins, E. M. (2015). Optimization and control of cyber-physical vehicle systems. *Sensors (Switzerland)*, *15*(9), 23020–23049. doi:10.3390/sl50923020

Cassandras, C. G. (2016). Smart cities as cyber-physical social systems. *Engineering*, *2*(2), 218–219. doi:10.1016/J.ENG.2016.02.012

Cheng, X., Zhang, R., & Yang, L. (2016). Consumer-centered energy system for electric vehicles and the smart grid. *IEEE Intelligent Systems*, *31*(3), 97–101. doi:10.1109/MIS.2016.52

Cintuglu, M. H., Mohammed, O. A., Akkaya, K., & Uluagac, A. S. (2017). A survey on smart grid cyber physical system testbeds. *IEEE Communications Surveys & Tutorials*, *19*(1), 446–464. doi:10.1109/COMST.2016.2627399

Dillon, T., & Chang, E. (2010). Cyber-physical systems as an embodiment of digital ecosystems extended abstract, in *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference on* (p. 701), Dubai: UAE.

Ding, D., Han, Q. L., Xiang, Y., Ge, X., & Zhang, X. M. (2018). A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, *275*(1), 1674–1683. doi:10.1016/j.neucom.2017.10.009

Farhangi, H. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*, *8*(1), 18–28. doi:10.1109/MPE.2009.934876

Farraj, A., Hammad, E., & Kundur, D. (2018). A cyber-physical control framework for transient stability in smart grids. *IEEE Transactions on Smart Grid*, *9*(2), 1205–1215. doi:10.1109/TSG.2016.2581588

Fernandez, E. B. (2016). Threat modeling in cyber-physical systems. In Dependable, Autonomic and Secure Computing, 14th Int. IEEE Conf. Pervasive Intelligence and Computing, 2nd Int. Conf. Big Data

Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech) (pp. 448–453). doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.89

Gao, Y., Peng, Y., Xie, W., Zhao, F., Wang, D., Han, X., & Li, Z. (2014). Analysis of security threats and vulnerability for cyber-physical systems. In 2013 3rd Int. IEEE Conf. Computer Science and Network Technology (ICCSNT) (pp. 50–55). Woburn, USA. doi: 10.1109/THS.2018.8574154.

Gill, H. (2006). *NSF perspective and status on cyber-physical systems. National Workshop on Cyber-physical Systems Austin, TX October 16 –17,2006*. The National Science Foundation, Arlington, USA.

Gilroy, W. G. (2010). Nsf funds cyber-physical systems project. Retrieved from http://newsinfo.nd.edu/news/17248-nsf-funds-cyber-phys/

Graessler, I., & Poehler, A. (2018). Intelligent control of an assembly station by integration of a digital twin for employees into the decentralized control system. *Procedia Manufacturing*, *24*(1), 185–189. doi:10.1016/j.promfg.2018.06.041

Gunes, V. S., Givargis, P. T., & Vahid, F. (2014). A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet and Information Systems*, *8*(12), 4242–4268. doi:10.3837/tiis.2014.12.001

Herwan, J., Kano, S., Oleg, R., Sawada, H., & Kasashima, N. (2018). Cyber-physical system architecture for machining production line. *IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg*, 387–391. doi:10.1109/ICPHYS.2018.8387689

Hiang, J. (2018). An improved cyber-physical system architecture for industry 4.0 smart factories. *Advances in Mechanical Engineering*, *10*(6), 1–15. doi:10.1177/1687814018784192

Hong, Z., Wang, R., Ji, S., & Beyah, R. (2018). Attacker location evaluation-based fake source scheduling for source location privacy in cyber-physical systems. *IEEE Transactions on Information Forensics and Security*, *14*(5), 1337–1350. doi:10.1109/TIFS.2018.2876839

Horcas, J. M., Pinto, M., & Fuentes, L. (2019). Context-aware energy-efficient applications for cyber-physical systems. *Ad Hoc Networks*, *82*, 15–30. ISSN 1570-8705. doi:10.1016/j.adhoc.2018.08.004

Howser, G., & McMillin, B. (2014). A modal model of stuxnet attacks on cyber-physical systems: A matter of trust. In 2014 8th Int.IEEE Conf. Software Security and Reliability (pp. 225–234). doi: 10.1109/SERE.2014.36.

Huda, S., Miah, S., Hassan, M. M., Islam, R., Yearwood, J., Alrubaian, M., & Almogren, A. (2017). Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data. *Inform Sciences*, *379*, 211–228. doi:10.1016/j.ins.2016.09.041

Ilic, M., Xie, L., Khan, U., & Moura, J. (2010). Modeling of future cyber physical energy systems for distributed sensing and control. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, *40*(4), 825–838. doi:10.1109/TSMCA.2010.2048026

Kantarci, B. (2015). Cyber-physical alternate route recommendation system for paramedics in an urban area. In 2015 IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, USA. (pp. 2155–2160). IEEE.

Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K., & Pannek, J. (2018). Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*, *97*(1), 132–145. doi:10.1016/j.compind.2018.02.009

Khojasteh, M. J., Khina, A., Franceschetti, M., & Javidi, T. (2019). Learning based attacks in cyber physical systems. Retrieved from http://acsweb.ucsd.edu/~mkhojast/Papers/Authentication-learning-based.pdf

Kim, K. D., & Kumar, P. R. (2013). An overview and some challenges in cyber-physical systems. *Journal of the Indian Institute of Science*, *93*(3), 341–352.

Kim, S., & Park, S. (2017). CPS (Cyber Physical System) based manufacturing system optimization. *Procedia Computer Science*, *22*(1), 518–524. doi:10.1016/j.procs.2017.11.401

Kitchenham, B., Pretorius, L., Budgen, D., Brereton, O. P., Turner, M., Niazi, M., & Linkman, S. (2010). Systematic literature reviews in software engineering-a tertiary study. *Information Software Technology*, *52*(8), 792–805. doi:doi.10.1016/j.infsof.2010.03.006

Konstantinou, C., Maniatakos, M., Saqib, F., Hu, S., Plusquellic, J., & Jin, Y. (2015). Cyber-physical systems: A security perspective. In 2015 *20th IEEE European Test Symposium (ETS)* (pp. 1–8). doi: 10.1109/ETS.2015.7138763

Kumar, N., Bali, R. S., Iqbal, R., Chilamkurti, N., & Rho, S. (2015). Optimized clustering for data dissemination using stochastic coalition game in vehicular cyber-physical systems. *Journal of Supercomputing*, *71*(9), 3258–3287. doi:10.1007/s11227-015-1436-6

Lanotte, R., Merro, M., Muteanou, A., & Vigano, L. (2019, February). A formal approach to physics-based attacks in cyber-physical systems. *Formal Methodologies for Cyber-Physical Systems*(Exended Version). CoRR abs/1902.04572 (2019).

Lee, E. A. (2007). *Computing foundations and practice for cyber-physical systems: a preliminary report*. Tech. Rep. UCB/EECS-2007-72. Berkeley: University of California. doi:10.1094/PDIS-91-4-0467B

Lee, E. A. (2008). Cyber physical systems: Design challenges. Tech. Rep. UCB/EECS-2008-8. Berkeley: EECS Department, University of California.

Lee, E. A. (2015). The past, present and future of cyber-physical systems: A focus on models. *Sensors (Switzerland)*, *15*(3), 4837–4869. doi:10.3390/s150304837

Lemmon, P. C., & Venkataramanan, G. (2009). Position paper – Using microgrids as a path towards smart grids. In *New research directions for future cyber-physical energy systems.17th* Iranian Conference on Electrical Engineering, (ICEE), Tehran, Iran, 2009, pp. 19-23.

Lemoine, M. P., Berdal, Q., Enjalbert, S., & Trentesaux, D. (2018). Towards human-based industrial cyber-physical systems. *IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg*, 615–620. doi:10.1109/ICPHYS.2018.8390776

Li, Y., Wu, J., & Li, S. (2016). State estimation for distributed cyber-physical power systems under data attacks. *International Journal of Modelling, Identification and Control*, *26*(4), 317–323. doi:10.1504/IJMIC.2016.081137

Lu, Y., & Ju, F. (2017). Smart manufacturing systems based on cyber-physical manufacturing services (CPMS). *Presented on IFAC-PapersOnLine*, 50, 15883–15889. doi:10.1016/j.ifacol.2017.08.2349.

Lyn, K. G., Lerner, L. W., McCarty, C. J., & Patterson, C. D. (2015). The trustworthy autonomic interface guardian architecture for cyber-physical systems. In 2015 IEEE Int. Conf. Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and

Computing (CIT/IUCC/DASC/PICOM) (pp. 1803–1810). doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.263

Ma, M., An, J., Huang, Z., & Cao, Z. (2015). Sensor data fusion based on an improved dempastershafer evidence theory in vehicular cyber-physical systems. In 2015 IEEE Int. Symp. Intelligent Control (ISIC), Sydney, Australia (pp. 683–687).

Mazumdar, S., Ayguade, E., Bettin, N., Bueno, J., Ermini, S., Filgueras, A., & Giorgi, R. (2016). AXIOM: A hardware-software platform for cyber physical systems. In 2016 Euromicro Conf. Digital System Design (DSD), Limassol, Cyprus (pp. 539–546). IEEE.

Möller, D. P. F., & Vakilzadian, H. (2016). Cyber-physical systems in smart transportation, *IEEE International Conference on Electro Information Technology (EIT)*, Grand Forks, ND (pp. 0776–0781). doi: 10.1109/EIT.2016.7535338

Monostori, L., Kadar, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., … Ueda, K. (2016). Cyber-physical systems in manufacturing. *CIRP Annals*, *65 (20*, 621–641. doi:10.1016/j.cirp.2016.06.005

Nguyen, P. H., Ali, S., & Yue, T. (2017). Model-based security engineering for cyber-physical systems: A systematic mapping study. *Information and Software Technology*, *83*(1), 116–135. doi:10.1016/j.infsof.2016.11.004

Northcutt, C. G. (2013). Security of cyber-physical systems: A generalized algorithm for intrusion detection and determining security robustness of cyber physical systems using logical truth tables. *Vanderbilt Undergraduate Research Journal*, 9, 1-9. doi:10.15695/vurj.v9i0.3765

Novak, P., Kadera, P., & Wimmer, M. (2017). Model-based engineering and virtual commissioning of cyber-physical manufacturing systems - Transportation system case study. *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1–4), Limassol. doi: 10.1109/ETFA.2017.8247743

O'Donovan, P., Gallagher, C., Bruton, K., & O'Sullivan, T. J. (2018). A fog computing industrial cyber-physical system for embedded low-latency machine learning Industry 4.0 applications. *Manufacturing Letters*, *15* (1), 139–142. doi:10.1016/j.mfglet.2018.01.005

Orojloo, H., & Azgomi, M. A. (2014). A method for modeling and evaluation of the security of cyber-physical systems. In 2014 11th Int. IEEE ISC Conf. Information Security and Cryptology (ISCISC) (pp. 131–136). doi: 10.1109/ISCISC.2014.6994036

Orojloo, H., & Azgomi, M. A. (2015). Evaluating the complexity and impacts of attacks on cyber-physical systems. In 2015 IEEE CSI Symp. Real-Time and Embedded Systems and Technologies (RTEST) (pp. 1–8). doi: 10.1109/RTEST.2015.7369840

Padher, P., & Rohokale, D. V. (2018). A cyber-physical system for environmental monitoring. *International Journal of Sensor Networks and Data Communications*, *08*(01). doi:10.4172/2090-4886.1000154

Puttonen, J., Afolaranmi, S. O., Moctezuma, L. G., Lobov, A., & Lastra, J. M. L. (2015). Security in cloud-based cyber-physical systems. In 2015 10th Int. IEEE Conf. P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC) (pp. 671–676). doi: 10.1109/3PGCIC.2015.30

Rawat, D. B., Bajracharya, C., & Yan, G. (2015). Towards intelligent transportation cyber-physical systems: Real-time computing and communications perspectives. *SoutheastCon*. doi:10.1109/secon.2015.7132923

Rebaï, B., Voos, S., & Darouach, H. M. (2018). Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems. *European Journal of Control*, *47*(1), 30–36. doi:10.1016/j.ejcon.2018.09.005

Rebai, S. B., Voos, H., & Alamdari, S. A. (2018). A contribution to cyber physical systems security: An event based attack tolerant control approach. *IFAC Paper*, *51*(24), 957–962. Retrieved from https://reader.elsevier.com/reader/sd/pii/S240589631832408X?token=FA1E786EABD15E21079570C8C81D47BBA204B838642B34E1AB5E6C85C92F790247730353261DF1ABC0B6ED38AF3A2F1D

Rekik, M., Gransart, C., & Berbineau, M. (2018, June). Cyber-physical threats and vulnerabilities analysis for train control and monitoring systems. IEEE ISNCC 2018, International Symposium on Networks, Computers and Communications (pp 1–6), Rome, Italy, doi: 10.1109/ISNCC.2018.8531005

Sampigethaya, K., & Poovendran, R. (2012). Cyber-physical system framework for future aircraft and air traffic control. *Presented at 2012 IEEE Aerospace Conference* (pp. 1–9), Big Sky, MT. doi: 10.1109/AERO.2012.6187151

Sampigethaya, K., & Poovendran, R. (2013). Aviation cyber–Physical systems: Foundations for future aircraft and air transport. *Proceedings of the IEEE*, *101* (8), 1834–1855. doi:10.1109/JPROC.2012.2235131

Sanislav, T., Mois, G., Folea, S., Miclea, L., Gambardella, G., & Prinetto, P. (2014). A cloud-based cyber-physical system for environmental monitoring. In 2014 3rd Mediterranean Conf. Embedded Computing (MECO) (pp. 6–9). IEEE. doi: 10.1109/MECO.2014.6862654

Sanjab, A., & Saad, W. (2016). On bounded rationality in cyber-physical systems security: Game-theoretic analysis with application to smart grid protection. In IEEE Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG) (pp. 1–6). doi:10.1109/CPSRSG.2016.7684101

Seiger, R., Huber, S., & Schlegel, T. (2016a). Toward an execution system for self-healing workflows in cyber-physical systems. *Software and Systems Modeling*, *17*(2), 1–22. doi:10.1007/s10270-016-0551-z

Seiger, R., Struwe, S., Lemme, D., & Schlegel, T. (2016b). An interactive mobile control center for cyber-physical systems. In Proc. 2016 ACM Int. Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, Heidelberg, Germany (pp. 193–196). ACM.

Sierla, S., O'Halloran, B. M., Karhela, T., Papakonstantinou, N., & Tumer, I. Y. (2013). Common cause failure analysis of cyber-physical systems situated in constructed environments. *Research in Engineering Design*, *24*(4), 375–394. doi:10.1007/s00163-013-0156-2

Smirnov, A., Shilov, N., & Gusikhin, O. (2017). Cyber physical human system for connected car-based e-tourism: Approach and case study scenario. *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)* (pp. 1–7), Savannah, GA. doi: 10.1109/COGSIMA.2017.7929591

Stamatescu, G., Stamatescu, I., Arghira, N., F˘ag˘ar˘asan, I., & Iliescu, S. S. (2014, May). Embedded networked monitoring and control for renewable energy storage systems. Development and Application Systems (DAS), 2014 International Conference, Suceava, Romania (pp. 1–6).

Vegh, L., & Miclea, L. (2014). Enhancing security in cyber-physical systems through cryptographic and steganographic techniques. In 2014 IEEE Int. Conf.

Automation, Quality and Testing, Robotics (pp. 1–6). doi: 10.1109/AQTR.2014.6857845

Vegh, L., & Miclea, L. (2016). Complex event processing for attack detection in a cyber-physical system *Presented at 2016 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)* (pp. 1–6), Cluj-Napoca. doi:10.1109/AQTR.2016.7501296

Wan, J., Chen, M., Xia, F., Li, D., & Zhou, K. (2013). From machine-to-machine communications towards cyber-physical systems. *Computer Science and Information Systems*, *10*(3), 1105–1128. doi:10.2298/CSIS120326018W

Wan, J., Yan, H., Li, D., Zhou, K., & Zeng, L. (2013). Cyber-physical systems for optimal energy management scheme of autonomous electric vehicle. *Computer Journal*, *56*(8), 947–956. doi:10.1093/comjnl/bxt043

Wan, J., Zhang, D., Sun, Y., Lin, K., Zou, C., & Cai, H. (2014). VCMIA: A novel architecture for integrating vehicular cyber-physical systems and mobile cloud computing. *Mobile Network Applications*, *19*(2), 153–160. doi:10.1007/s11036-014-0499-6

Wang, Y. N., Lin, Z., Liang, X., Xu, W. Y., Yang, Q., & Yan, G. F. (2016). On modeling of electrical cyber-physical systems considering cyber security. *Frontiers of Information Technology and Electronic Engineering*, *17*(5), 465–478. doi:10.1631/FITEE.1500446

Weyer, S., Weyer, T., Ohmer, M., Gorecky, D., & Zuhlke, D. (2016). Future modeling and simulation of CPS-based factories: An example from the automotive industry. *International Federation of Automation Control*, *49* (31), 97–102. doi:10.1016/j.ifacol.2016.12.168

Wiesner, S., Marilungo, E., & Thoben, K. D. (2017). Cyber-physical product-service systems — Challenges for requirements engineering. *International Journal of Automation Technology*, *11*(1), 17–28. doi:10.20965/ijat.2017.p0017

Wolf, W. (2009). Cyber-physical systems. *Computer*, *42*(3), 88–89. doi:10.1109/MC.2009.81

Wu, J., Luo, S., Wang, S., & Wang, H. (2018). NLES: A novel lifetime extension scheme for safety-critical cyber physical systems using SDN and NFV. *IEEE Internet of Things Journal*, *6*(2), 2463–2475. doi:10.1109/JIOT.2018.2870294

Wu, W., Kang, R., & Li, Z. (2015). Risk assessment method for cyber security of cyber physical systems. *Presented at 2015 First International Conference on Reliability Systems Engineering (ICRSE)* (pp. 1–5), Beijing. doi: 10.1109/ICRSE.2015.7366430

Xin, S., Guo, Q., Sun, H., Chen, C., Wang, J., & Zhang, B. (2017). Information-energy flow computation and cyber-physical sensitivity analysis for power systems. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, *7*(2), 329–341. doi:10.1109/JETCAS.2017.2700618

Yampolskiy, M., Horvath, P., Koutsoukos, X. D., Xue, Y., & Sztipanovits, J. (2015). A language for describing attacks on cyber-physical systems. *International Journal of Critical Infrastructure Protection*, *8*, 40–52. doi:10.1016/j.ijcip.2014.09.003

Yan, W., Mestha, L. K., & Abbaszadeh, M. (2019). Attack detection for securing cyber physical systems. *IEEE Internet of Things Journal*, 1. doi:10.1109/jiot.2019.2919635

Yang, C., Shi, Z., Zhang, H., Wu, J., & Shi, X. (2019). Multiple attacks detection in cyber-physical systems using random finite set theory. *IEEE Transactions on Cybernetics*, 1–10. doi:10.1109/tcyb.2019.2912939

Yu, X., & Xue, Y. (2016). Smart grids: A cyber–Physical systems perspective. *Proceedings of the IEEE*, *104*(5), 1058–1070. doi:10.1109/JPROC.2015.2503119

Zhang, L., Wang, Q., & Tian, B. (2013). Security threats and measures for the cyber-physical systems. *Journal of China Universities of Posts and Telecommunications*, *20*(1), 25–29. doi:10.1016/S1005-8885(13)60254-X

Zhang, X., Xu, Z., & Yu, T. (2018), A cyber-physical-social system with parallel learning for distributed energy management of a microgrid. *2018 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)* (pp. 1294–1298), Singapore. doi: 10.1109/ISGT-Asia.2018.8467970

Zhao, P., Simoes, M. G., & Suryanarayanan, S. (2010). A conceptual scheme for cyber-physical systems based energy management in building structures. *2010 9th IEEE/IAS International Conference on Industry Applications - INDUSCON 2010*. doi:10.1109/induscon.2010.5739891

Zhou, Y., Mo, Z., Xiao, Q., Chen, S., & Yin, Y. (2016). Privacy-preserving transportation tra±c measurement in intelligent cyber-physical road systems. *IEEE Transactions on Vehicular Technology*, *65*(5), 3749–3759. doi:10.1109/TVT.2015.2436395

Zhou, Y., Xiao, Z., Mo, S., Chen, C., & Yin, Y. (2013). Privacy-preserving point-to-point transportation traffic measurement through bit array masking in intelligent cyber-physical road systems. In Green Computing and Communications (GreenCom), IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference and IEEE Cyber, Physical and Social Computing (pp. 826–833). IEEE. doi: 10.1109/GreenCom-iThings-CPSCom.2013.146

***Cogent Engineering* (ISSN: 2331-1916) is published by Cogent OA, part of Taylor & Francis Group.**