Internet of Things Integrated Cyber-Physical Systems: A Survey

1st Austin J Derbique
School of Computing and Augmented Intelligence
Arizona State University
Tempe, USA
Fall 2021 CSE598: Cyber-Physical Systems
aderbiqu@asu.edu

***Abstract*—With hardware and software developments progressing at a staggering rate, internet of things (IoT) devices are becoming more prevalent than ever before. These systems are not just integrated into smart watches or irrigation sensors, they control power plants, autonomous vehicles (AVs), and many mission critical cyber physical systems. This paper explores literature on security implications of these IoT devices across the CPS spectrum. An analysis will be performed to determine what research still needs to be conducted.**

***Index Terms*—CPS, IoT, Security, Decentralization, Peer-to-peer, Smart City**

I. Final Project Report

I have spent time compiling a list of papers that will be included in the project. They are inside bibliography.bib. The references are at the end of this document. There are roughly 8 research papers and three surveys used for formulate the content for this project, with other information being pulled in as needed.

A. Work Performed

I have identified and read the papers I will be using to write this report. I have also created a skeleton that roughly outlines the format I will be using to write my survey. This includes introduction, background, existing work, critical analysis, looking forward, and conclusion. Several figures have been included in this survey to help illustrate concepts of the IOT-CPS research space.

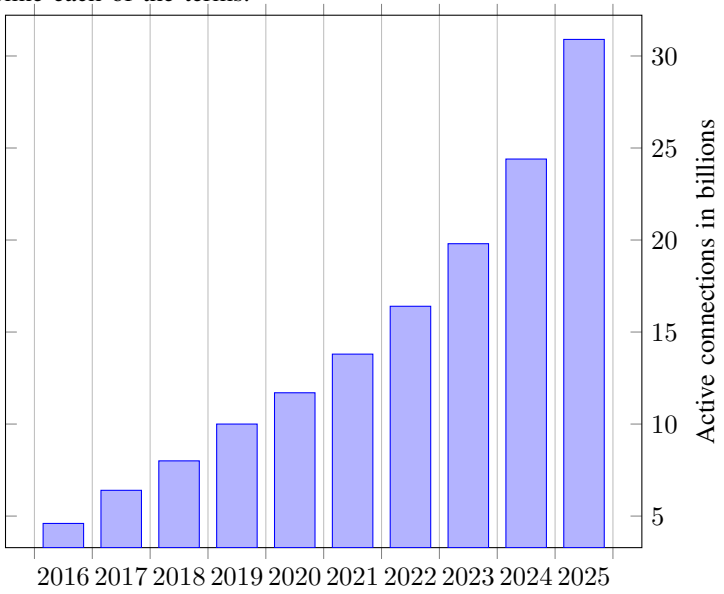
Link to LaTeX document:
https://www.overleaf.com/read/qcxwmjgnycfq

B. Relevance to Course

The relevance to this course is that the survey is on the topic of cyber-physical systems. The material covered in this project builds off of what we have learned in class, and extends to the domains of distributed systems and internet of things.

II. Introduction

While internet of things (IoT) devices and cyber-physical systems (CPS) are nothing new, IoT-CPS systems have been on the drastic in recent years. It is expected that we reach 30 billion interconnected IoT devices by 2025 [2]. In terms of CPS, these devices may come in the form of traffic signals, road sensors, industrial applications, or just about that monitors and produces data. With this increased interoperability and reliance of devices comes an increased attack surface leaving the cyber-physical systems vulnerable to an attack. In order to better understand this topic of IoT and CPS, we will first define each of the terms.



Graph II: Projected IoT Active Device Connections [2]

1) Cyber Physical Systems: A cyber-physical system (CPS) is often defined as a system with three important capabilities [15]:

- **Capability One:** Sensing the physical world. This could be sensing the luminosity of a room or the distance to the car in front of you.
- **Capability Two:** Making decisions. If the room is dark, should the lights be turned on? If the car in front of you brakes, should you brake?
- **Capability Three:** Performing actions in the physical world. Actually turn on the lights. Engaging the brakes on the vehicle to decelerate.

2) Internet of Things: Internet of Things (IoT) devices are devices connected to a network. There are many protocols, but the most common types used are WiFi, Bluetooth, and

Cellular (LTE). This can be either local only or connected to the internet. The range of different types of devices is also extremely diverse. These vary from smart home automation such as smart light bulbs, smart locks, thermostats, smart-outs, to wearable devices such as smart watches, autonomous floor cleaning robots. Another section of IoT devices that we are more focused on in this survey is in regards to the devices that have more real-world consequences. Smart cars and IoT sensors for industrial applications.

3) IoT integrated CPS: IoT integrated CPS are IoT devices that have a real-world impact on the environment surrounding them. Examples of this could be the speedometer in your car or thermometer in the thermostat to measure ambient temperature. In one particular example, an IoT-CPS could be the sensors and mechanisms used in a nuclear plant. To help illustrate the importance and severity of IoT devices with respect to CPS, we examine the classic example of Stuxnet. In 2010, Stuxnet was discovered as a piece of malware used to target a type of CPS [11]. This process of infecting, activating, and launching the attack was responsible for a drop in production output of uranium enrichment by more than 30% [10].

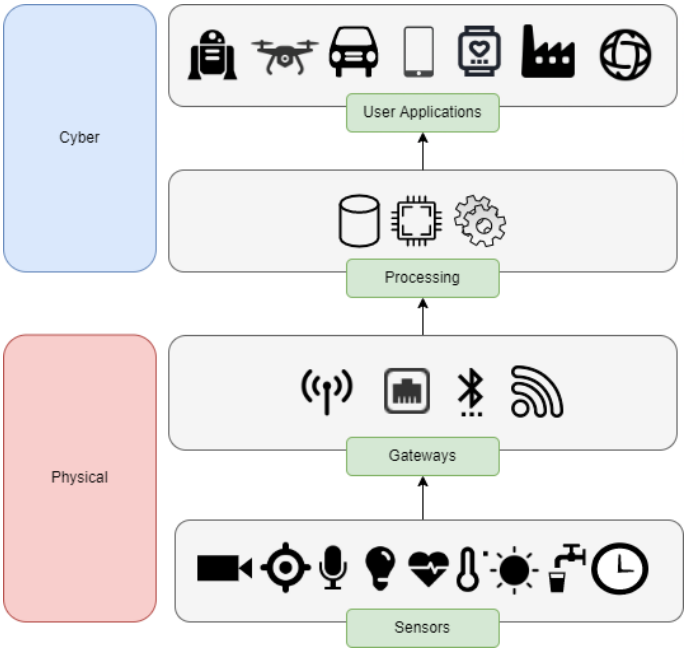


Fig. 1. IoT CPS Illustration

In Figure 1, an IoT integrated CPS is broken down into its cyber-physical components. Note that user applications in this context is the software powering the system. Motors or actuators or things that are physical would fall inside the physical domain at the bottom.

III. Background

Because of the rapid growth of IoT, new cases of CPS are presenting themselves all the time. While diverse, there are some commonalities between all cyber-physical systems. This section intends to cover different types of CPS and go into more detail on the different use cases of internet of things devices and their impact of being a cyber-physical system.

A. Different Types of CPS

Typically, when talking about CPS, several key characteristics come to mind. Availability and Integrity of the system. Both of these are maintained by having a good security mechanism in place. In the survey, "Cyber-Physical Systems Security- A Survey", the authors study existing literature on how to systematize security under a unified framework. Some of these security critical types of CPS were industrial control systems (ICS), smart grids, medical devices, and smart cars [7]. The authors describe each type of CPS and briefly cover security threats and vulnerabilities of each at a high level.

- **Industrial Control Systems:** These are control systems used for controlling, monitoring, and producing products for various industries. These may include oil and gas, manufacturing, nuclear power plants, and sewage systems. Most of these applications make use of sensors and actuators which are connected to a computer or some centralized system.
- **Smart Grid Systems:** Smart grid systems are the future generation of our current grid systems. This intelligent, load balancing system dynamically adapts production rates based on consumption by measuring many different data points. This could also be a decentralized grid where all electric vehicles (EVs) make up a portion of the grid. This type of infrastructure would be a combination of sensors, hardware, and software in a decentralized manner.
- **Medical Devices:** CPS for medical devices would be devices that if compromised could put a patient's life in danger. Such devices could be pacemakers, smart pumps, or other devices intended to improve a patient's life. These could either be worn on the patient or embedded within the patient's body and controlled by a remote control.
- **Smart Cars:** Smart cars are vehicles that are designed to be more environmentally friendly, safe, and have enhanced convenience features. These cars might take an optimized route to reduce trip time or lower the speed to improve fuel economy automatically. Smart cars as we know them today heavily use electronic control units (ECUs) which are responsible for controlling and monitoring various functions of the car.

B. Attacks and Defenses of CPS

In another literature survey, the authors aimed to provide a systematic discussion for the existing work on adversarial attacks and defenses of cyber-physical systems [8]. In this case, adversarial attacks have already been widely studied (as well as potential countermeasures) due to the significance of a successful attack. The authors focus on non-visual attacks and find that two relevant modules are required to carry out an attack: a perturbation and a detector.

- **Perturbation:** In order to carry out an adversarial attack, the attacker must find the common input data. For an Amazon Alexa, this would be voice. Then, in order to modify the data to make it malicious, noise data must be inserted. This is called a perturbation. The resultant of the original data input plus the perturbation will yield the malicious piece of data.
- **Detector:** Because the methods researched in this survey utilize neural networks, a detector must be used to determine whether the desired output selected by the attacker is achieved. A successful attack would make it so that the perturbation goes unnoticed by humans listening to the Amazon Alexa device.

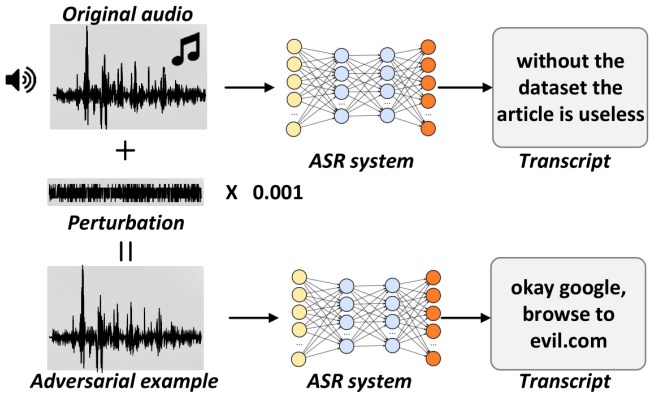


Fig. 2. Adversarial attack using perturbation [8]

In Figure 4, original audio is used in conjunction with a perturbation to create the adversarial example. After being passed through Amazon Alexa's speech identifier, the input is falsified and the adversarial transcript is processed.

1) Smart Cities and Vehicles: Attack surfaces are not only limited to Amazon Alexa devices, however. The greatest threats posed are to human safety and availability to critical infrastructure. In 2003, nearly 50 million Americans and Canadians lost power in a four day blackout due to a software failure [4]. Examples like this is why it is so critical to protect such important infrastructure. In the survey "Cyber-phyical security for on-going smart grid initiatives: a survey", the authors survey literature covering different attack types posed to a smart grid infrastructure [6]. Known as having a cyber-physical interdependency, the smart grid infrastructure relies on a bidirectional connection between the physical and cyber components of the grid. One affects the other and vice-versa. This plays in an important role in maintaining communication and stability of its dynamic control [14]. With this relationship established, the authors found several attack scenarios.

- **Physical attacks**
- **Bad data injection attacks (BDIA)**
- **False data injection attack (FDIA)**
- **Denial of service (DoS) attack**
- **Distributed DoS (DDoS) attack**
- **Replay attack**

Out of the attack scenarios mentioned above, none of them are specific to CPS or smart grids. It is important to realize that attacks on CPS use nothing more than existing known vulnerabilities in a system to gain access and exploit the CPS.

In the paper Automated Driving: The Cyber-Physical Perspective, author Rolf Ernst talks about the complexities surrounding AVs and the challeneges they will face once progressing beyond SAE level two. Currently, ISO26262 safety standards are achieved by returning control to the driver in the event of a hardware or software malfunction. The difficulty arises when humans are no longer always present. This means that the car will have to come to a safe stop by itself. Ernst argues that redundant hardware doesn't satisfy the safety requirement as the failure could be in the software. Instead, the paper proposes implementing diversity by introducing an independent subsystem to take over in case of an error [3].

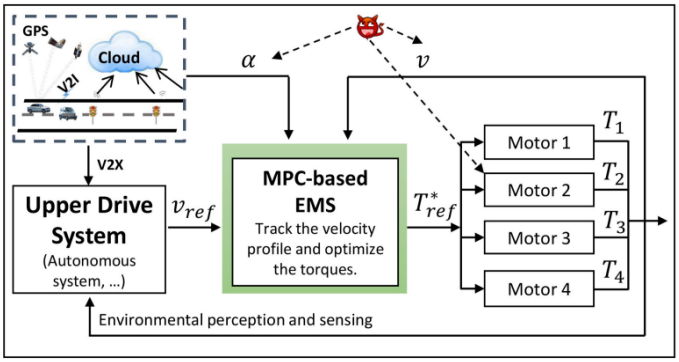


Fig. 3. IoT integrated CAEV EMS [5]

In Figure 4, the devil is depicted to show an adversary intending to attack motor 2 by means of compromising integrity to the energy management system by means of an IoT access point within the car. By gaining access to the car's internals through an IoT access point, an attacker can cause adverse consequences remotely.

2) Attack Surfaces: To help illustrate attack surfaces, a real world scenario was created using an unmanned aerial vehicle (UAV) with communication channels accessible from a computer [15], the authors attempt to model the analysis of cyber-attacks against CPS. In this implementation, there are three different surfaces vulnerable to an attack. The first surface is wireless communication between UAV and the controller. This includes a PPA (Physical - Protocol Analysis) and CCI (Cyber - Command Injection) attacks. The second attack surface is the high level processor on-board the UAV. This is programmable by the user. Possible attacks here include is the physical signal transmission medium. This includes electromagnetic, visual, and audio channels. On another layer of attack surface, there are the processors on-board the UAV which are subject to attack by one of the mediums formerly mentioned.Various attacks described in this paper include CPSWS (Cyber- Physical Component Warning), and CCDI (Cyber - Connected Devices Infection) attacks. A compromised HL could ignore the warnings caused by a component, such as a lithium ion

battery, causing it to fail and potentially catch on fire or explode.

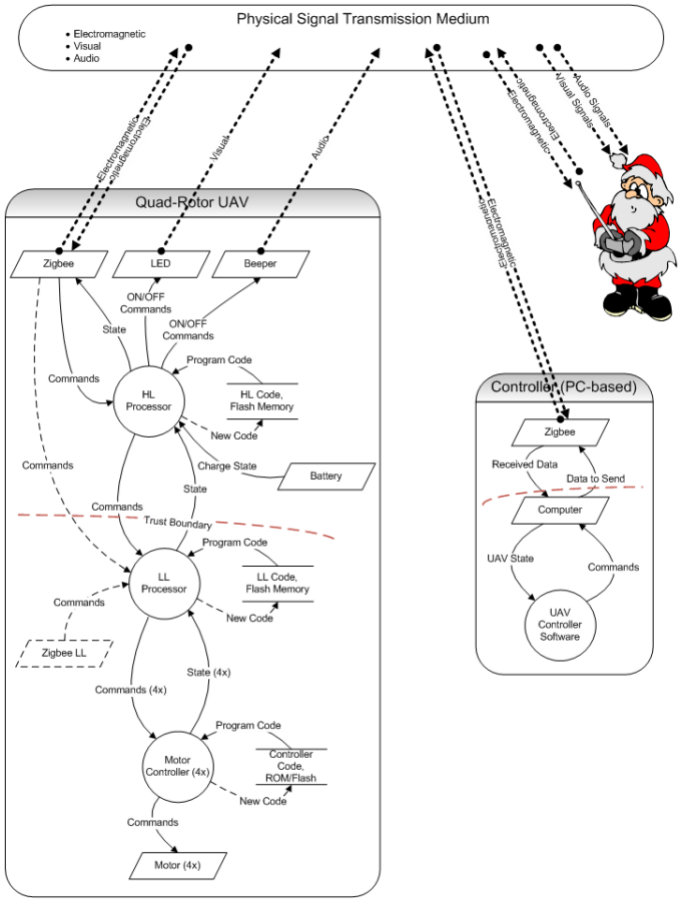


Fig. 4. Quadrocopter Architecture DFD - Extended [15]

In Figure 4, an illustration of the quadrocopter architecture is depicted. This is the DFD with extended attributes to show physical signals. In this case, they are the signals (visual, audio, electromagnetic) between the operator and the UAV.

IV. Existing Research and Findings

In the background, we covered in more detail what IoT CPS systems look like as well as their typical applications. We also covered common attack types and surfaces. While this literature has already been surveyed as referenced in the above section, detecting attacks and the security challanges of protecting IoT CPS have not. In this section, we explore modern literature aimed at giving us a better grasp of how to detect attacks, security challenges associated with attacks, and how the reliability of CPS can be improved using decentralized decision making [16].

A. Security Challenges for IoT CPS

There is nothing special about an IoT CPS. They use regular components subject to the same vulnerabilities as any other system, except with much larger consequences. In a research paper by Kelvin Ly and Yier Jin, the authors look at what those challenges are surrounding security and how to better protect CPS from an attack [9]. In their case study, they found several different types of vulnerabilities.

- **Boot Process Vulnerabilities:** One of the most common components to target in attacks, the boot sequence is the root of trust that forms the starting point for a device's operation. By modifying the boot loader, an attacker can run unsigned code and set custom parameters in the kernel. This effectively grants them full access to the device to do whatever they want.
- **Hardware Exploitation:** At the lowest level is hardware exploitation. This requires physical access to the CPS and is often overlooked by developers and designers. An example of this may be hacking the hardware of a Bird Scooter to obtain free rides by circumventing the IoT logic that necessitates payment. A more common exploit is by using the debugging ports as an entry point into the system.
- **Chip-level Exploitation:** By exploiting particular chips on a device, "secret" information such as private keys stored locally are now not secret. These chips also trust the bootloader, so are subject to exploitation if the bootloader is compromised. This is considered a mid level attack and is less common but still entirely possible.
- **Encryption, Hash Function and Authentication Implementations:** If an IoT CPS uses weak cryptographic cyphers, a bruteforce or some other mechanism could be used to gain access to the device. This is true for old versions of TLS which are known to be vulnerable to an attack.
- **Backdoors in Remote Access Channels:** Remote access channels are channels put in place by the manufacturer commonly used for over the air updates (OTA) or possible means of debugging. If these remote access channels have any kind of bug or insecurity, they can be used by an attacker as a backdoor to gain unauthorized access to the system. Ways to combat this are sanitizing inputs, checking for code injection, changing default user credentials, and keeping a lookout for known vulnerabilities for your particular system.

V. Analysis

A. Table of Research Papers Surveyed

Below are a number of different published papers representing various segments of literature in IOT-CPS systems. This includes the paper title with appropriate citation, motivation for why the paper was written, overall analysis of the paper and how to make sense of the information provided, and finally date published and relevant tags for the paper.

Paper Title	Motivation	Analysis	Published	Tags
The Quest for autonomy. are we there yet? ARE CPS a way to build autonomous systems? [1]	In this conference journal, questions are raised on what the meaning of CPS is and how it has changed over the years. The article also asks the question of if we are any closer to using CPS for autonomous vehicles than we were twenty-five years ago.	This paper was extremely short and only asked the questions. It did not answer them. In such a way, one can infer possible research areas to help answer the questions raised in this paper.	2015	CPS, AVs
Automated driving: The cyber-physical perspective [3]	The author Rolf Ernst covers several key points of CPS in regards to automated driving. The first is the quest for performance. More data and processing onboard means designing a future beyond ADAS and introducing possible software-defined networks (SDN). Second, safety being a challenge for CPS when SAE levels reach beyond two. Finally, the topic of car-to-car and car-to-infrastructure helps in certain ways, but is argued that it will not increase safety due to ISO26262.	Overall, this paper presents CPS in a different way than most papers. Instead of focusing on attack surfaces, etc, the paper envisions the challenges engineers will be faced with as the progression of automated driving improves. While not necessarily technical, the paper provides good insight into what those challenges are and possible techniques that could be employed to solve those challeneges.	2018	SAE, ADAS, SDN, ISO26262
Systematic assessment of Cyber-Physical security of Energy Management System for connected and Automated Electric Vehicles [5]	Unlike internal combustion engine (ICE) vehicles, electric vehicles (EVs) operate in a completely different way. The three main components to an EV are safety system, advanced driving assistant system (ADAS), and energy management system (EMS). This paper explores the security vulnerabilities associated with the EMS and how attacks on EMS sensors can have ripple effects on velocity tracking, torque levels, and overall instability of the system. The authors accomplished this by modeling the attacks using formal approaches. The metrics assessed included velocity tracking, energy consumption, energy efficiency, and comfortability. An attack against the CPS was deemed successful if it could meaningfully alter one of these metrics.	Apart from the research conducted in this paper on developing a way to model and assess CPS attacks against EMS, one interesting paragraph dealt with discerning the difference between an attack of a CPS and a fault. In the event of CAEVs, the authors deemed this metric infeasible. This could be a potential topic for future research.	2021	CAEVs, cybersecurity, impact analysis
Security challenges in CPS and IOT: From end-node to the system [9]	IoT CPS devices typically have a large surface area that can be attacked, meaning that if security is not a primary concern, then the devices are subject to a successful attack. The authors discuss various vulnerabilities and case studies. After recording these vulnerabilities across IoT devices, the authors developed design guidelines to follow to mitigate the possibility of an attack.	While documented in the paper, there is a lack of evidence showing how this was accomplished. Only a mid level overview was given on the different exploits without going into detail how the database was created or used to mitigate attack vulnerabilities. This is certainly an opportunity for future research as exploring how following a set of design guidelines can help reduce the possibility of an attack.	2016	hardware exploits, bootloader, protocols, IoT, CPS

TABLE I
ANALYSIS OF RELATED WORKS

Paper Title	Motivation	Analysis	Published	Tags
Detecting deception attacks on autonomous vehicles via linear time-varying dynamic watermarking [12]	With the rise of autonomous vehicles and the cyber-physical systems they rely upon, it is important to know if an attack has occurred. Historically, linear time-invariant (LTI) methods were used to provide accurate results, however this is insufficient for real time applications. The authors propose a dynamic watermarking system applied to a high-fidelity vehicle model in CarSim to test their proof of concept. Using a replay attack, the authors can quickly and repeatably detect an attack using linear time-varying (LTV) dynamic watermarking.	While a novel achievement, one of the troubling parts with this paper relaxes the requirement for inputs to be visible in a single step. While this is possible and was accomplished in simulation, it would be very difficult getting the implementation to run on a real-world test car. This poses challenges for the applicability of the paper beyond just theoretical means. In another light, this could open up possible research area for how to use LTV Dynamic Watermarking in a generalized fashion for detecting deception attacks on more than just autonomous vehicles. This could be expanded to sensors as a whole with some adaptation. Possible for a future research oppurtunity.	2020	LTI, LTV, CV, attack detection
Integration of human actors in IOT and CPS Landscape [13]	In many IoT CPS landscapes, humans are an essential part of the job and must be able to take over or be involved and any and all steps in the system process. The authors develop a tool called CHARIOT (a Scalable Holistic Middleware Approach foR the Internet Of Things) and use this tool to integrate IoT CPS with human interactions.	The authors of this paper take a creative solution in using augmented reality (AR) to aid in IoT CPS with human integration. In the proposed smart factory environment, workers wear a smart watch that is connected to the IoT CPS application where they can interact with the system on a realtime basis. Currently, this is the only piece of work taking this hybrid approach. It is truly novel and worth more research into how this type of human-IoT interaction can be used in other events. Possibly in vehicles to detect an unconcious driver? This paper expands the current research domain for IoT CPS into the realm of human interactions and AR technology.	2019	hunman-CPS integration, AR, wearables, activity recognition
Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach [15]	Data flow Diagrams (DFDs) are generally a good way to perform systematic analysis of a system. However, this technique is not sufficient for analyzing CPS because it is impossible to distinguish between cyber and physical communications. The authors implement an extension to DFDs which include a physical component, communication medium, data flow, and physical signal. In such a way, the extensions to DFD provide a way to model CPS attacks.	In regards to this survey on IoT, the authors managed to create a realistic attack surface by performing their research using a UAV drone. By having this real-world CPS, both physical and cyber attacks could result in possible damage to physical components on the drone as well as a possible collision with the surrounding environment. Several attack types are described in this paper, however only a few are applicable to this survey. Overall, the paper successfully illustrates the applicability of Data Flow Diagrams for systematic analysis against CPS.	2012	CPS security, taxonomy, CPS Attacks, CPS Defense

TABLE II
ANALYSIS OF RELATED WORKS

B. Critical Review

The new literature surveyed for the purposes of this paper draw several interesting observations. First, the field is extremely broad and continuing to grow. When dealing with cyber-physical systems, each component has its own set of attack surfaces and vulnerabilities, and when combined create a system that is even more susceptible to an attack. Another observation is that there is currently a lot of reserach on attacks, but less so on attack detection, defense, and mitigation strategies. It appears the problem of IoT CPS is now becoming more well defined, but there is still no clear answer on tried and true way of completely securing a given system.

C. Challenges

As detailed in an earlier section, it will always be impossible to ensure an IoT CPS is 100% secured. There will always be threat vectors dealing with hardware exploitation, chip-level exploitation, and insecure cryptographic protocols. Currently, one of the best ways to protect against this is to have sufficient monitoring in place for intrusion detection, software updates, and known vulnerabilities for a given piece of hardware or

software. This challenge is nothing new, and will not be going away any time soon.

VI. Looking Forward

A survey of the papers analyzed shows there is still a lot of research to be accomplished in this field. Potential areas of exploration include

- **Determining whether a failure in a CPS is the result of a fault or attack**
- **How to design a set of guidelines to follow to minimize attack surface for IoT CPS**
- **Researching how to design a safety system for SAE level 3 and above**
- **If decentralized control processes actually improve the security of IoT CPS**

VII. Conclusion

In this paper, we dive into what the use cases are for internet of things devices and cyber physical systems. We look at real world scenarios where they are used in conjunction with each other: industrial control systems, smart grids, medical devices, smart cars. A survey of surveys is accomplished to determine what literature is already well known and researched and identify new domains with less coverage. In the existing research and findings, several papers are analyzed covering topics such as security challenges, attack detection, and systematic assessment of security controls for CAEVs. Overall, the research area is extremely vast, but few papers provide solutions for these issues. Several looking forward topics are proposed with the possibility for future research to be conducted in any of the aforementioned areas. Overall, the usage of IoT CPS will continue to grow and although research is currently being conducted in this area, new challenges are sure to present themselves along the way.

Declaration of Competing Interest

The author declares that there is no competing financial interest or personal relationships that could appear to influence the work reported in this paper.

Acknowledgement

The author thanks Professor Fainekos for his guidance on the research project and underlying knowledge of CPS.

References

[1] Panos Antsaklis. "The Quest for autonomy. are we there yet? ARE CPS a way to build autonomous systems?" In: *2015 American Control Conference (ACC)* (2015). DOI: 10.1109/acc.2015.7172128.

[2] Published by Statista Research Department and Jan 29. *Global number of connected IoT devices 2015-2025*. Jan. 2021. URL: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/.

[3] Rolf Ernst. "Automated driving: The cyber-physical perspective". In: *Computer* 51.9 (2018), pp. 76–79. DOI: 10.1109/mc.2018.3620974.

[4] RG Farmer and EH Allen. "Power system dynamic performance advancement from history of North American blackouts". In: *2006 IEEE PES Power Systems Conference and Exposition*. IEEE. 2006, pp. 293–300.

[5] Lulu Guo et al. "Systematic assessment of Cyber-Physical security of Energy Management System for connected and Automated Electric Vehicles". In: *IEEE Transactions on Industrial Informatics* 17.5 (2021), pp. 3335–3347. DOI: 10.1109/tii.2020.3011821.

[6] Md Musabbir Hossain and Chen Peng. "Cyber–physical security for on-going smart grid initiatives: a survey". In: *IET Cyber-Physical Systems: Theory & Applications* 5.3 (2020), pp. 233–244.

[7] Abdulmalik Humayed et al. "Cyber-physical systems security—A survey". In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1802–1831. DOI: 10.1109/jiot.2017.2703172.

[8] Jiao Li et al. "Adversarial attacks and defenses on Cyber–Physical Systems: A survey". In: *IEEE Internet of Things Journal* 7.6 (2020), pp. 5103–5115. DOI: 10.1109/jiot.2020.2975654.

[9] Kelvin Ly and Yier Jin. "Security challenges in CPS and IOT: From end-node to the system". In: *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)* (2016). DOI: 10.1109/isvlsi.2016.109.

[10] Yossi Melman. *'computer virus in Iran actually targeted larger nuclear facility'*. Sept. 2010. URL: https://www.haaretz.com/1.5118389.

[11] Arash Nourian and Stuart Madnick. "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet". In: *IEEE Transactions on Dependable and Secure Computing* 15.1 (2018), pp. 2–13. DOI: 10.1109/TDSC.2015.2509994.

[12] Matthew Porter et al. "Detecting deception attacks on autonomous vehicles via linear time-varying dynamic watermarking". In: *2020 IEEE Conference on Control Technology and Applications (CCTA)* (2020). DOI: 10.1109/ccta41146.2020.9206278.

[13] Doruk Sahinel et al. "Integration of human actors in IOT and CPS Landscape". In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (2019). DOI: 10.1109/wf-iot.2019.8767276.

[14] Yujae Song et al. "Cellular-assisted D2D communications for advanced metering infrastructure in smart gird". In: *IEEE Systems Journal* 13.2 (2019), pp. 1347–1358.

[15] Mark Yampolskiy et al. "Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach". In: *2012 5th International Symposium on Resilient Control Systems* (2012). DOI: 10.1109/isrcs.2012.6309293.

[16] Peng Zhou et al. "Improving the reliability of CPS with hierarchical-decentralized decision solution". In: *2017 International Conference on Computational Science and Computational Intelligence (CSCI)* (2017). DOI: 10.1109/csci.2017.226.

Austin Derbique received a Bachelor of Science in Computer Science from Utah State University, Logan, Utah, USA in 2017. Upon graduation, he began work as a cloud engineer for a global satellite communications company. As a certified solutions architect on Amazon Web Services, Austin is knowledgeable with compute, storage, and networking. He is currently pursuing a Master of Science in Computer Science at Arizona State University where his research primarily focuses on future blockchain applications.