Savunma Bilimleri Dergisi
The Journal of Defense Sciences
Mayıs / May 2022, Sayı/Issue 41

Cyber-Physical Systems and their Security Issues

Amin MAHNAMFAR[*] - Nafiz ÜNLÜ[**]

Abstract

Broadly, cyber physical systems are systems that integrate computing into the physical world. Control systems, the increase in their intersection with information technology networks and the variety of communication methods also cause the threat vectors in cyber physical systems security to change and increase. This shows that traditional information technology security measures, new generation information technology security solutions or security solutions specific to control systems will be insufficient alone, and the need for integrated security solutions that include all components in the cyber physical systems network and include operational scenarios. In this work, it was cover a couple of definitions of cyber physical systems and it was present an overview of cyber physical systems, what they are, where they are found, and how they are used. It also includes some information on the specific reasons cyber physical systems present greater security demands. The stakes are higher, the components are much more difficult to maintain and update, and the systems are more complex. The goal is to understand these systems well enough to design effective security measures to counter potential attacks.

***Keywords**: Attacks, Cyber-Physical Systems, Security.*

Siber Fiziksel Sistemler ve Güvenlik Sorunları

Öz

Genel olarak, siber fiziksel sistemler, bilgi işlemi fiziksel dünyaya entegre eden sistemlerdir. Kontrol sistemleri, bilgi sistem ağları ile kesişimlerinin artması ve

[*] İstanbul Technical University, Information Institute, Cyber Security, mahnamfar19@itu.edu.tr, ORCID: 0000-0003-1978-2498.
[**] PhD, İstanbul Technical University, Information Institute, Cyber Security, nafiz.unlu@gmail.com, ORCID: 0000-0002-2094-8080.

Geliş Tarihi/Received : 27.05.2021
Kabul Tarihi/Accepted : 03.12.2021
Araştırma Makalesi/ Research Article
DOI: 10.17134/khosbd.1100660

iletişim yöntemlerinin çeşitliliği siber fiziksel sistem güvenliğindeki tehdit vektörlerinin değişmesine ve artmasına neden olmaktadır. Bu, geleneksel bilgi sistem güvenlik önlemlerinin, yeni nesil bilgi sistem güvenlik çözümlerinin veya kontrol sistemlerine özgü güvenlik çözümlerinin tek başına yetersiz kalacağını ve siber fiziksel sistem ağındaki tüm bileşenleri içeren ve operasyonel senaryolar içeren entegre güvenlik çözümlerine duyulan ihtiyaç artmaktadır. Bu çalışmada, siber fiziksel sistemlerin birkaç tanımı ele alınmış ve siber fiziksel sistemlere ne olduklarına, nerede bulunduklarına ve nasıl kullanıldıklarına genel bir bakış ortaya konulmuştur. Ayrıca, siber fiziksel sistemlerin daha fazla güvenlik talepleri sunduğunun belirli nedenleriyle ilgili bilgiler sunulmuştur. Risklerin daha yüksek, bileşenlerin bakımı ve güncellenmesi çok daha zor ve sistemlerin daha karmaşık olduğu ortadadır. Amaç, potansiyel saldırılara karşı koymak için etkili güvenlik önlemleri tasarlanması adına bu sistemleri yeterince iyi anlamaktır.

***Anahtar Kelimeler**: Saldırılar, Siber-Fiziksel Sistemler, Güvenlik.*

Introduction

Advances in digital electronics and the desire for more information and control of physical systems has caused a noteworthy increase in the number of systems that extend across both the cyber field and the physical world. These systems are known as Cyber-Physical Systems, or CPS's. Designing these systems with a relation to unique challenges and compound functionality, reliability, performance, and security requirements, needs a significant amount of reasoning (Humayed et al., 2017).

1. Cyber-Physical Systems

If we consider a few examples of traditionally cyber and traditionally physical devices. In the cyber category we have personal computers, mobile phones, and other embedded devices. In the physical category we have motors, pumps, generators, valves, and so on. So CPSs sit at the intersection of these two categories. There are many different definitions for CPS. For example, Lee, in an earlier research paper defines CPSs as the integration of computing and physical processes (Lee, 2008). Another definition by Rajkumar, describes CPSs as, physical and engineer systems which their operations are checked, controlled, and integrated by computing and communicating core (Rajkumar et al., 2010).

Of course, this area has gathered a significant amount of attention from various government and organizations. For example, an organization with special interest has been established in the US which is called the CPS Virtual Organization (CPSVO), in order to encourage collaboration among CPS experts in academic world, industry and government.

There are various definitions of CPSs but most will agree that CPSs are physically aware, multidisciplinary, complicated, next generation engineered systems. These systems mainly contain observations, communication, and control aspects of a physical system.

CPS is a comparatively new concept. However, the system components are already known. As illustrated in the Figure 1, CPS is made of elements from the physical world, networks, sensors, actuators, and a cyber system (Yao et al., 2019). The physical world refers to the physical event that will be checked or controlled. The cyber systems refer to embedded and standard computing devices which process information and connect with their distributed environment (Cárdenas et al., 2011).

It's critical to appreciate that a significant variance of CPSs compared to most cyber systems is the non-reversibility or actuator operations’ preemption. While in most cyber systems, rollback operations and preemption are possible, but physical operations that the actuators execute typically cannot be reversed. If actuation happens based upon inaccurate or false data, most of the time it is really hard to roll back that activity (Jones et al., 2015; Nunes et al., 2015)

CPSs normally must operate in real time, and the physical systems are often modeled mathematically to ensure that the components of the CPS can be designed properly (Gunes et al., 2014).

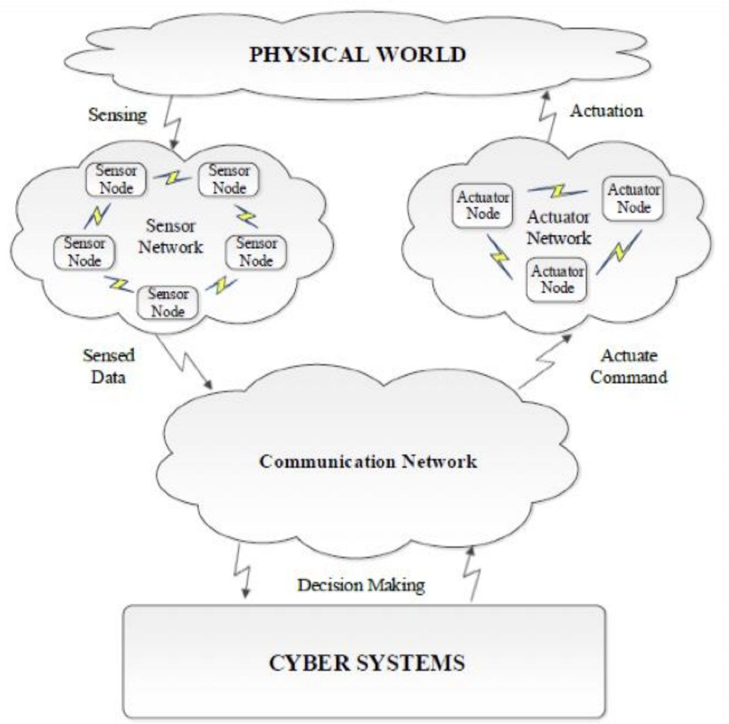

Figure 1. CPS Holistic View (Yao et al., 2019).

There are numerous study areas and expressions that are fairly similar to or are closely aligned with CPSs. For example, wireless sensor networks maybe used as a sensory channel for cyber physical systems. Depending on the cyber physical system, it may likely generate an enormous amount of data. This large amount of data can be processed in the cloud and used to generate various analytics. There's a significant amount of overlap between the Internet of Things, IoT, and CPSs. Many IoT systems are simply CPSs such as an intelligent thermostat and HVAC system. Also, it should be appreciated that many CPSs will generate a large amount of machine-to-machine communication. We can see the list of similar concepts in Figure 2 (Wan et al., 2013; Gunes et al., 2014).

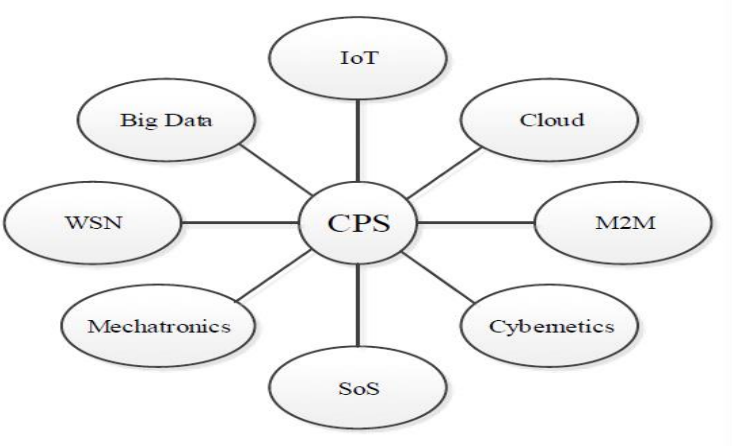

Figure 2. Similar Concepts (Wan et al., 2013; Gunes et al., 2014).

2. Domain and Application

Cyber-physical systems extend across many domains such as smart manufacturing. One definition of smart manufacturing, or the smart factory, is utilizing embedded hardware and software technologies to enhance efficiency in the manufacture of products or service delivery. The advantages comprise productivity, improved safety, more flexible workflow, efficiency, and new forms of partnership (Thoben et al., 2017).

One can think of emergency response as handling threats against public health, safety, and welfare and protecting the goods, nature, and valued infrastructures. So, CPS can deliver quick emergency response with big amount of sensor nodes in the areas in case of some sort of natural or manmade disasters. one can imagine unmanned aerial or ground vehicles deployed to enhance or independently conduct search and rescue efforts.

Air transportation is also another domain. Air transportation refers to military or simple aviation systems and the management of traffic. It is anticipated that smart vehicles, such as drones and unmanned aerial vehicles (UAV), in the close future will be widely available. Particularly for the delivery of consumer goods and military service. CPS are anticipated to make a deep impact on the future air traffic and aviation management through the use of distributed controls throughout the air space (Humayed et al., 2017).

Medicine and health care go back to the issues regarding several sides of patient care. This includes technologies associated with assisted living, smart operating room, home care, smart medical tools like pacemakers and medical ventilators, and smart prescriptions. Further, the expectation is that there will be reliable software to provide new functionalities. Also, the connectivity of medical devices which are equipped with network interfaces, and request for constant patient monitoring will increase. For example, support from in home care and assistant living (Latimer, 2020).

Let's consider transportation. Intelligent transportation refers to leveraging communication, sensing, computation, and control mechanisms in transportation system to ameliorate safety. Services and coordination and traffic management with real-time data share. This next generation transportation system will support both sea and ground conveyance through data sharing over multiple networks including satellite networks. Further, this new system will support communication between vehicles, the infrastructure, and passengers' portable devices. Then, involved it transportation system will also integrate vehicles, pedestrians, roadside infrastructures, sensors, satellites, traffic management centers, and other transportation systems by using variations or even new types of technologies. By integrating the aforementioned data sources with traffic management centers. The intelligence transportation system will be able to provide benefits such as growth of transportation safety and comfort over data exchange. Optimal management of traffic, and of course avoiding collision.

Another example of CPS is a robot, which can be used for various services. Service robots are used to do services for the humans' welfare. They can be operated in an entirely autonomous, semi-autonomous, or remote-controlled manor. The service could be anything from assisting humans with household chores to performing fully autonomous search and rescue missions.

Automation of buildings includes the placement of several actuators, sensors, and distributive control systems. The goal is to deliver optimal automation and control of heating, ventilation, air conditioning (HVAC), fire prevention, lighting, and security systems in buildings. Intelligent or smart buildings are required to achieve the vision of the smart city and smart grid concepts. This is a perfect example to illustrate the overlap and interconnectedness of IoT and CPS (Lawrence and Jokonya, 2020).

The last application and probably the most important one is on is critical infrastructure. Critical infrastructure refers to infrastructure which are essential for the welfare or survival of the country. The power grid is an example of a critical infrastructure that's partly controlled manually and also partly automated using various industrial control systems. The power grid is becoming a smart grid to realize necessary efficiencies and to incorporate renewables and other micro grid technologies.

3. Cyber-Physical Systems' Challenges

When designing and deploying CPSs, several challenges must be addressed, each of which ultimately relate to the security and safety of the system and the public.

As we can see in Figure 3, One challenge is interoperability, which is referring to the systems' ability and the components working together in order to exchange data and to utilize this data to deliver definite services. The absence of standards and interoperability usually decreases effectiveness of a system or ultimately causes a system failure (Lee, 2008).

Another challenge is a need for predictability. Predictability is the anticipation degree of a system state behavior functionality, either quantitatively or qualitatively. A very predictive system should promise the particular result of a system's actions or functionality to a great degree, every time which it is operating while fulfilling all system requirements.

Another challenge is reliability, which basically is the correctness' degree which a system delivers performing its function. And, of course, sustainability, which refers to capability of enduring without any compromise of requirements to the system while replacing the systems resources and effectively using them. A highly maintainable system should be enduring, it should heal itself, and actually dynamic, and able to evolve under various circumstances.

Another challenge is dependability, which is simply the quality of a system to do essential functionalities during its process, without noteworthy degradation in its outcome and performance. reflects A degree of trust put into the entire system is reflected by dependability. So, let's set aside the potential for intrusions. A highly dependable system should provide the services which are requested as stated and not fail performing this operation.

And finally, the most critical challenge for CPSs is providing security. Security has several different attributes, including integrity and confidentiality. I will try to focus on some of the security challenges and discuss about these attributes.

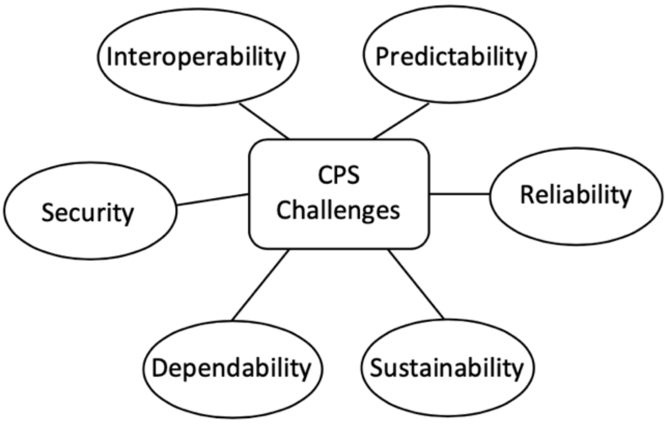

Figure 3. CPS Challenges (Lee, 2008).

4. CPS Security Challenges

As I declared earlier we will take a close look in specific challenges related to securing CPSs.

Many CPSs are getting more vulnerable to computer threats for numerous different reasons. Accordingly, we need to develop strong adversary models. And we must also understand the differences in securing CPS systems versus traditional IT systems. A regular study of the security of any system needs the explanation of the expected threats to face. And creating an adversary model is a way of understanding the extent of the problem and assessment of the risk.

Let's consider some adversary models at a high-level. Who would want to attack a CPS, especially ones that control critical infrastructure and what are the capabilities? The first suspects that come to mind probably are cybercriminals. They compromise computers wherever they exist, even in control systems.

These kinds of attacks may not be targeted. For example, they don't have to have the intention of damaging a control system, but negative effects can be caused by them and of course, displeased employees that currently are the main source of targeted computer attacks against controlled systems.

Then you have various groups like terrorists, activists, hacktivists, or organized criminal groups. While there's no concrete public information so far about activists or terrorists targeting control systems with computer attacks, there's some signs of criminal groups involvement’s possibility.

Lastly nation states, which could absolutely be a threat to the control systems. There was rumored to be the case with Stuxnet and the recent attack on the Ukraine power grid.

The main point here is that different groups had different motivations and different capabilities, thus resulting in different adversary models. This must be taken in consideration to precisely understand one's security posture (Cardenas et al., 2009).

5. IT Security and CPS Security Differences

Priorities and characteristics between corporate IT security and CPS security are different. I will give a brief comparison between them. Control systems are required to make independent decisions in real-time. So, availability is much more important in CPS networks than confidentiality, whereas confidentiality would be a primary goal in IT networks (Haque et al., 2014).

In IT security, attacks are instant and more frequent. Many predefined attacks are detected and blocked beforehand. Attacks on CPS networks, on the other hand, can be more specific and their effects can be destructive and irreversible, as in the case of Stuxnet.

The network topology from any CPS networks, especially industrial control networks, is usually static. For example, servers change rarely and user population is rather static, where IT networks are often dynamic (DHCP). We can conclude that implementing intrusion detection systems might be easier than traditional corporates.

Unfortunately, in CPS networks, patches and updates are administered a lot less frequently then done in IT networks. This is due to damage it can cause if CPS networks are down.

Worse, outdated CPS components can also underpin attacks that cause irreversible damage.

As I mentioned availability of control system is very important and also it can be difficult to arrange a specific time for these upgrades.

6. Maintaining Control Of CPS

Our goal is to maintain control of cyber-physical systems. Ideally, we can deter or prevent attacks. The next level of defense is deploying countermeasures and also detection and recovery techniques. Finally, we hope that the system is designed such that it is resilient in the face of such an attack.

Understanding the attacker's intentions will help us better comprehend the potential consequences of an attack. With this information we can develop various techniques to limit the attacker's capabilities during an attack. By understanding how the physical processes and physical components must act based upon sensor measurements and our control command. It is possible for us to find out if an attacker is tampering with control or sensor data. This idea allows us to design novel attack-detection algorithms. Another approach is designing new attack-resilient architectures and algorithms. For example, if we can detect that an attack is on the way, we might be able to modify the meaning of the control commands in the system to improve the system’s resiliency. This is a form of moving target defense (Olowononi et al., 2014).

a. Prevention

There are currently less efforts in order to follow best practices preventing the compromise of control systems. Programs are currently being developed in several areas such as oil and gas, chemical, and water for securing their infrastructure. Regulation is one approach. Another is the use and enforcement of standards. For example, the North American Electric Reliability Corporation, NERC, has cyber security standards for the power grid. NERC is an authority which can enforce compliance of these standards. A guide to industrial control system security has been also published by the National Institute of Standards and

Technology (NIST). These recommendations might not be enforceable, but they can provide direction for analyzing most utility companies' security for best practices (Humayed et al., 2017).

b. Detection and Recovery

Security engineering has realized the detection and response's importance to attacks as we can never eliminate successful attacks. Control systems can deliver a model change for intrusion detection while old-style intrusion detection systems look at network or computer system traces. Specifically, we might be able to detect attacks that are undetectable from the IT half by monitoring the physical system for anomalies. Providing sufficient information consciousness to operators of control systems is another key part for detecting attacks. Operators might need training in order to detect probable attacks and to have a correctly defined procedure or standard on how to respond and get over these attacks. As attacks become more prevalent, the need for automatic recovery will also increase. Since the CPS issues algorithms which are real-time decision-making and autonomous for controlling the physical world, attacks might introduce new challenges for the analysis and design of systems which are secure. Accordingly, we can leverage notions from control theories like fault detection and isolation, or reconfiguration. These can be utilized in order to design algorithms having autonomous and real time detection and response for applications which safety is critical and require real-time responses (Humayed et al., 2017).

c. Resilience

There exist several security design rules for designing control systems which are capable of surviving attacks. Redundancy is a method for prevention of failure in a single point. Also, separation of privilege can be used to limit the level of privileges that an entity which is corrupted can possess. Analytical and physical redundancy and security principals must be merged to reschedule or adapt its operation during attack. For instance, under false data injection attack on multiple sensors, the system must be able to function using open loop control with adequate time amount. Ultimately, what we'll have to do is design end security at the time these different systems and components of the systems are developed (Humayed et al., 2017).

The physical durability of control systems is no longer the olny requirement for the durability of CPS networks. The longer CPS System can operate without deteriorating, the higher its durability. Therefore, CPS security consideringe how destructive attacks on CPS systems can be, tightening and precautions in security become important. In addition, it is necessary to determine the control flow scenarios in the System and monitör the traffic by the systems that detect out-of-scenario events that may ocur in them.

d. Deterrence

It usually relies on successful legislation, law enforcement, and of course, international cooperation for pursuing committed crimes which are outside of the borders of a country (Humayed et al., 2017).

7. Common Methods of Attack

There are common attack methods that can be used for industrial control systems (ICS). Some examples are man-in- the-middle attacks, Denial-of-Service or DoS attacks and also replay attacks. In some instances, the available information could be utilized as investigation for additional capabilities of a cyber-attack. The main cause for this contains factors such as really small authentication of device-to-device, insecure communications protocols and also embedded devices' good communication stacks. Standard tools could be utilized to deliver target systems' remote access in case of penetration of an industrial network and malware deposition anywhere in the network. At this point the attacker essential owns the ICS device.

Let's consider a man-in-the-middle attack where the attacker seeks to observe and tamper with communication between the two PLC's. If encryption and authentication are not provided in the connection, which is the case for many industrial protocols, it is really straight forward. As an IT networks, a man-in-the-middle attack can also occur if authentication or encryption are used. The attacker simply has to compromise the key exchange process. This of course assumes that there are no safeguards in place to prevent this. Another common attack is a denial-of-service attack. A DoS attack, again is an attack on availability. It is a really comprehensive attacks' category and can comprise everything from communications loss via the device to crashing and/or constraining specific type of services inside the device such the I/O processing, the storage or the continual processing of logic.

DoS attacks do not generally result in noteworthy negative consequences on traditional business systems if determined as soon as possible. A web page access might be decreased or e-mail delivery slowed down till the issue is fixed. To control or monitor a physical process, automation systems are installed. The process would be converting steam into electricity, controlling the unrefined petroleum flow in a pipeline, or control of ignition times in an engine of a car. A controller's incapability like maintaining the state of performing its duty is generally said loss of control or LoC and usually develops in a physical process in place in what is called a safe state until it shuts down. In another words, even basic disruption of controlling functions can rapidly get into physical site troubles that can later cause plant shut downs, environmental issues, mechanical disaster, or other catastrophic events. Denial-of-service is way more than a problem in industrial environments, but can continue to substantial outcomes if not managed appropriately.

Yet another common attack is a replay attack. In this attack, an attacker will eavesdrop on the channel and can replay traffic which may contain data, commands or even log-in information. But introducing precise process commands into an industrial protocol system needs a detailed knowledge of industrial control systems operations. Thus, a naive attacker can potentially sabotage a process by launching a replay attack of the desire process command to the system. It is good thing to recall that most of the traffic is transferred in plain text for industrial control system. Even encrypted traffic can be replayed unless mechanism is in place to protect against this, for example a nonce. The actions of an entire system could be changed like the controller functions in case the device is a process automation controller such as a PLC which can be discovered in more complex gateways of substation. Specific registers can be overridden for injection of incorrect measurements or readings into the system if the target is an IED (Gao and Morris, 2014).

The HMI is one of the most critical components of ICS because it can directly manipulate the process and components. Its compromise could be catastrophic for the ICS. Since it's a GUI, industrial protocols' information is not required and also in ladder logic no particular experience or control system operations is required. Just the power to interpret the GUI, click buttons, and change values with a console which is generally created for ease-of-use. For example, the control of setpoints can be changed with the click of a mouse.

Although directions followed to compromise an Engineering Workstation are not really different from already used ones for the HMI because they both often use standard OSes. The Engineering Workstation is usually a single host that holds the ability to set role-based mechanisms of access control. It also has dedicated tools required to straightly contact with, update, and set the primary control equipment, so PLC's, Sys's, IDS's, etc. Also, it is usual for the engineering work station to have considerable amounts of delicate documentation particular to the design of ICS, plant operation, and configuration. This makes it a target which is very higher valued asset than a normal HMI.

Typically, attacks are not just an exploit for a single vulnerability on one target. The attacks which are more advanced generally use as it is called, a blended threat model. That is, a type of exploit which mixes basics of several malware types and often uses many attack factors in order to boost the amount of damage and the pace of the contamination. Blended threats have evolved to be fairly complex. One can think of Stuxnet, which a single, complicated, and metamorphosing malware framework was deployed that was able tp behaving in numerous ways, depending upon its environment (Knapp and Langill, 2021).

8. Industrial Application Layer Attacks

There are many attacks that could happen at the application layer of network stack, particularly attacks that target industrial applications. They are the protocols and applications which transmit from, to and between supervisory control and process parts of the system. They deliver particular goals inside the ICS which are vulnerable by their essence, since they are control-related design. Whether control of devices or processes directly, or control with supervisory systems indirectly that are used by human operators like a DCS or SCADA to influence and supervise processes or devices. Different from general application layer threats, such as opening a PDF that contains a virus, threats of application layer in industrial systems do not continuously need to exploit a particular vulnerability. The reason is that the design purpose of these applications is for the goal of affecting industrial control environments. They do not require a malware to infect them to get the control needed to do a damage, because they could directly be used as they are designed, but with malevolent purpose.

Take the protocol stack in Figure 4 as an example (Pricop et al., 2017). This is Modbus TCP, and we see at the application layer is the Modbus application layer and Modbus TCP. But the application layer here is essentially Modbus. So, one can actually launch an application layer attack by issuing commands, through Modbus, at the application layer in the TCP/IP protocol stack.

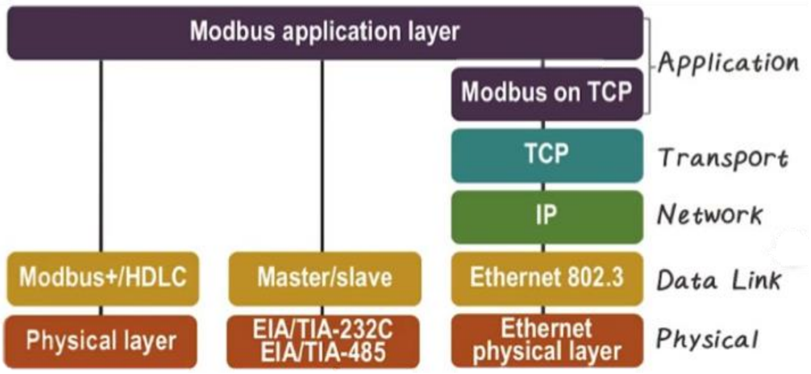

Figure 4. Industrial Layers (Pricop et al., 2017).

That is, by delivering genuine commands among systems that have authority and in complete agreement with the characteristics of protocols, an ICS could be instructed to notify a function that it is out of the intended parameters and goal of the owner. This technique can be thought of as functionality exploitation. And once took into consideration in the ICS security setting, denotes a problem that is not generally addressed over controls of traditional IT security. So legitimate commands can be used to force a system to stop, crash a CPU, dump the device boot code, reset the device, crash the device and even do a flash update.

In general, these attacks result from the protocols' weaknesses which had been designed many years ago and today are confronted with new challenges in security that were unanticipated when they were being developed. As we have experiences with Stuxnet, evolution of malware and utilizing a condition-based logic to manage activity depending on its surrounds till it meets the conditions that are perfect where it will be capable of accomplishing its goals. Those goals include spreading, staying hidden and deploying a weapon. So Stuxnet had a fine goal of discovering a special ICS by replicating broadly over sneaker networks and local networks. When the target environment was found it then only took secondary infection steps. It next looked for special PLC versions and models. Once these models were found, it searched for a particular make and model of BFDs prior to injection of process code inside the PLC. If the infected targets were inappropriate, it would stay inactive until the infection of other hosts. Malware metamorphoses also are by now utilized. Stuxnet, basically, updates itself in the wild over peer-to-peer controls with other infected hosts also and if fresher versions of Stuxnet encounters an earlier version, it upgrades the outdated version, allowing an infection pool to change and update in the wild. Additionally, metamorphosis actions include self-destruction of certain code blocks or self- updates of others. Efficiently the malware gets transformed and made more targeted, as well as much hard to detect. This consist of inspection for the presence of other well-known malware and altering its own profile to use similar ports and services knowing that the new profile will go undetected. It means, malware is becoming very cleverer. At the same time, much more difficult to detect (Knapp and Samani, 2013).

Future cyber-physical systems (CPS) such as smart cities, collaborative robots, autonomous vehicles and intelligent transportation systems are expected to be used. Trends and uncertainties regarding CPS in 2030 identified by Broo et al. (2021).

Conclusion

The research in CPS security is active because of the frequently reported cyber-attacks. Control systems, the increase in their intersection with IT networks and the variety of communication methods also cause the threat vectors in CPS security to change and increase. This shows that traditional IT security measures, new generation IT security solutions or security solutions specific to control systems will be insufficient alone, and the need for integrated security solutions that include all components in the CPS network and include operational scenarios. Although some defense mechanisms have been proposed/deployed, new and systemspecific solutions are still expected in response to the newly identified threats and vulnerabilities. In addition, these anticipated new security solutions should have the feature of preventing the destructive and irreversible damage that may ocur in CPS networks. In this paper, we also highlight challenges and some missing pieces in CPS security research, and hope to stimulate more interests in the research community.

Genişletilmiş Özet

Dijital elektronikteki gelişmeler ve fiziksel sistemlerin daha fazla bilgi ve kontrolüne duyulan istek, hem siber alana hem de fiziksel dünyaya yayılan sistemlerin sayısında kayda değer bir artışa neden olmuştur. Bu sistemler, siber fiziksel sistemler veya CPS'ler olarak bilinir. Bu sistemleri benzersiz zorluklar ve bileşik işlevsellik, güvenilirlik, performans ve güvenlik gereksinimleri ile ilişkili olarak tasarlamak, önemli miktarda akıl yürütme gerektirir (Humayed vd., 2017). Genel olarak, siber fiziksel sistemler, bilgi işlemi fiziksel dünyaya entegre eden sistemlerdir. Kontrol sistemleri, bilgi sistem ağları ile kesişimlerinin artması ve iletişim yöntemlerinin çeşitliliği siber fiziksel sistem güvenliğindeki tehdit vektörlerinin değişmesine ve artmasına neden olmaktadır. Bu, geleneksel bilgi sistem güvenlik önlemlerinin, yeni nesil bilgi sistem güvenlik çözümlerinin veya kontrol sistemlerine özgü güvenlik çözümlerinin tek başına yetersiz kalacağını ve siber fiziksel sistem ağındaki tüm bileşenleri içeren ve operasyonel senaryolar içeren entegre güvenlik çözümlerine duyulan ihtiyaç artmaktadır.

Siber kategoride kişisel bilgisayarlarımız, cep telefonlarımız ve diğer gömülü cihazlarımız bulunmakla birlikte, fiziksel kategoride motorlarımız, pompalarımız, jeneratörlerimiz, valflerimiz vb. vardır. Dolayısıyla CPS'ler bu iki kategorinin kesişme noktasında yer alır. CPS için birçok farklı tanım vardır. Lee (2008) CPS'leri hesaplama ve fiziksel süreçlerin entegrasyonu olarak tanımlamaktadır. Rajkumar vd. (2010) tarafından yapılan başka bir tanımda, CPS'leri, işlemlerinin kontrol edilerek ve entegrasyonun sağlandığı fiziksel sistemler olarak tanımlamaktadır.

CPS, yeni bir kavram olmakla birlikte, sistem bileşenleri bilinmektedir. CPS fiziksel dünya, ağlar, sensörler, aktüatörler ve bir siber sistemden oluşmaktadır (Yao vd., 2019). Fiziksel dünya, kontrol edilecek fiziksel olayları ifade etmektedir. Birbirleri ile internet üzerinden ve atanmış bir internet adresi ile haberleşen nesne ve sistemlerin oluşturduğu ağ; gerçek dünyadaki nesnelerin ve davranışların bilgisayar ortamında simülasyonuyla ortaya çıkan sanal ortamdır.

CPS'ler tasarlanırken ve dağıtılırken, her biri nihayetinde sistemin ve halkın güvenliği ve emniyeti ile ilgili olan çeşitli zorlukların ele alınması gerekir. Karşılaşılan zorluklardan biri, sistemlerin yeteneğine ve veri alışverişine ilişkin birlikte çalışabilirliktir. Standartların ve birlikte çalışabilirliğin olmaması genellikle bir sistemin etkinliğini azaltır veya nihayetinde bir sistem arızasına neden olur (Lee, 2008). Bir başka zorluk da öngörülebilirlik ihtiyacıdır. Tahmin edilebilirlik, niceliksel veya niteliksel olarak bir sistem durumu davranış işlevselliğinin tahmin derecesidir. Çok öngörücü bir sistem, tüm sistem gereksinimlerini karşılarken, her çalıştığında, bir sistemin eylemlerinin veya işlevselliğinin belirli bir sonucunu oluşturur. Diğer bir zorluk, temelde bir sistemin işlevini yerine getirirken sağladığı doğruluk derecesi olan güvenilirliktir. Sistem kaynaklarını değiştirip etkin bir şekilde kullanırken, kendini iyileştirmeli, dinamik olmalı ve çeşitli koşullar altında gelişebilmelidir. CPS'ler için en kritik zorluk güvenli unsurunu sağlamaktır. Güvenlik, bütünlük ve gizlilik dahil olmak üzere birkaç farklı özelliğe sahiptir.

Endüstriyel kontrol sistemleri (ICS) için kullanılabilecek yaygın saldırı yöntemleri vardır. Orrtadaki adam saldırıları, hizmet reddi veya DoS saldırıları ve yeniden yürütme saldırılarını örnek olarak verebiliriz. Bazı durumlarda, mevcut bilgiler bir siber saldırının ek yeteneklerini araştırmak için kullanılabilir. Bunun ana nedeni, cihazdan cihaza gerçekten küçük kimlik doğrulaması, güvenli olmayan iletişim protokolleri ve ayrıca gömülü cihazların iyi iletişim yığınları gibi faktörleri içerir. Endüstriyel bir ağa sızma ve ağın herhangi bir yerinde kötü amaçlı yazılım biriktirme durumunda hedef sistemlerin uzaktan erişimini sağlamak için standart araçlar kullanılabilir.

Saldırganın niyetini anlamak, bir saldırının olası sonuçlarını daha iyi anlamamıza yardımcı olacaktır. Bu bilgilerle, bir saldırı sırasında saldırganın yeteneklerini sınırlamak için çeşitli teknikler geliştirebiliriz. Fiziksel süreçlerin ve fiziksel bileşenlerin sensör ölçümlerine ve kontrol komutumuza göre nasıl davranması gerektiği bilinmelidir. Bir saldırganın kontrol veya sensör verileriyle oynayıp oynamadığını öğrenmemiz mümkündür. Bu yaklaşım, yeni saldırı tespit algoritmaları tasarlamamıza olanak tanıyacaktır. Diğer bir yaklaşım, saldırıya dayanıklı yeni mimariler ve algoritmalar tasarlamaktır. Örneğin, bir saldırının var olduğunu tespit edebilirsek, sistemin dayanıklılığını iyileştirmek için sistemdeki kontrol komutlarının anlamını değiştirebiliriz. Bu, hareketli hedef savunma biçimi belirlenmiş olacaktır (Olowononi vd., 2014).

Genel olarak saldırılar, protokollerin yıllar önce tasarlanmış ve bugün geliştirilirken beklenmeyen yeni güvenlik zorlukları ile karşı karşıya kalan zayıflıklarından kaynaklanmaktadır. Kötü amaçlı yazılım evrimi ve hedeflerine ulaşabileceği mükemmel koşulları karşılayana kadar çevresine bağlı olarak etkinliğini sürdürür. Bu hedefler arasında yayılmak, gizli kalmak ve bir silah olarak ortamda bulunmaktır. Kötü amaçlı yazılımın çok daha akıllı hale gelebilecek ve tespit edilmesi zor olacaktır (Knapp ve Samani, 2013).

CPS güvenliğindeki araştırmalar, sıklıkla bildirilen siber saldırılar ile ilişkilidir. Kontrol sistemlerinin, bilgi teknolojisi ağları ile kesişimlerinin artması ve iletişim yöntemlerinin çeşitliliği de CPS güvenliğindeki tehdit vektörlerinin değişmesine ve artmasına neden olmaktadır. Bu, geleneksel bilgi teknolojisi güvenlik önlemlerinin, yeni nesil güvenlik çözümlerinin tek başına yetersiz kalacağını ve CPS ağındaki tüm bileşenleri içeren ve operasyonel senaryoları içeren entegre güvenlik çözümlerine duyulan ihtiyacı göstermektedir. Bazı savunma mekanizmaları önerilmiş olsa da, yeni tanımlanan tehditlere ve güvenlik açıklarına yanıt olarak sisteme özgü çözümler beklenmektedir. Beklenen bu yeni güvenlik çözümleri, CPS ağlarında oluşabilecek yıkıcı ve geri dönüşü olmayan zararları önleme özelliğine sahip olmalıdır. Bu çalışmada, CPS güvenlik araştırmalarındaki zorluklar ve eksik unsurlar vurgulanmıştır.

References

Books

Knapp, E. D., & Langill, J. T. (2021). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress. (2nd Edition).

Knapp, E. D., & Samani, R. (2013). *Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure*. Newnes.

Articles

Broo, D. G., Boman, U., & Törngren, M. (2021). Cyber-physical systems research and education in 2030: Scenarios and strategies. *Journal of Industrial Information Integration,* 21, 100192.

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, July). Challenges for securing cyber physical systems. *Future directions in cyber-physical systems security.* 5(1), 1-7.

Gao, W., & Morris, T. H. (2014). On cyber attacks and signature based intrusion detection for modbus based industrial control systems. *Journal of Digital Forensics, Security and Law,* 9(1), 3.

Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014). A survey on concepts, applications, and challenges in cyber-physical systems. *KSII Transactions on Internet & Information Systems,* 8(12), 4242-4268.

Haque, S. A., Aziz, S. M., & Rahman, M. (2014). Review of cyber-physical system in healthcare. *International journal of distributed sensor networks*, 10(4), 217415, 1-20.

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. *IEEE Internet of Things Journal*, 4(6), 1802-1831.

Jones, A., Subrahmanian, E., Hamins, A., & Grant, C. (2015). Humans' critical role in smart systems: A smart firefighting example. *IEEE Internet Computing,* 19(3), 28-31.

Latimer, K. (2020). The Art of Care: A Report on the 2019 Vizient Connections Education Summit. *American Journal of Medical Quality,* 35(1_suppl), 5S-111S.

Lee, E. A. (2008, May). Cyber physical systems: Design challenges. *11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)* (pp. 363-369). IEEE.

Nunes, D. S., Zhang, P., & Silva, J. S. (2015). A survey on human-in-the-loop applications towards an internet of all. *IEEE Communications Surveys & Tutorials,* 17(2), 944-965.

Olowononi, F. O., Rawat, D. B., & Liu, C. (2020). Resilient Machine Learning for Networked Cyber Physical Systems: A Survey for Machine Learning Security to Securing Machine Learning for CPS. *IEEE Communications Surveys & Tutorials.* 23(1), 524-552.

Pricop, E., Fattahi, J., Parashiv, N., Zamfir, F., & Ghayoula, E. (2017, April). Method for authentication of sensors connected on Modbus TCP. *4th International Conference on Control, Decision and Information Technologies (CoDIT)* (pp. 0679-0683). IEEE.

Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010, June). Cyber-physical systems: the next computing revolution. *In Design automation conference* (pp. 731-736). IEEE.

Thoben, K. D., Wiesner, S., & Wuest, T. (2017). Industrie 4.0" and smart manufacturing-a review of research issues and application examples. *International journal of automation technology,* 11(1), 4-16.

Wan, J., Chen, M., Xia, F., Di, L., & Zhou, K. (2013). From machine-to-machine communications towards cyber-physical systems. *Computer Science and Information Systems,* 10(3), 1105-1128.

Yao, X., Zhou, J., Lin, Y., Li, Y., Yu, H., & Liu, Y. (2019). Smart manufacturing based on cyber-physical systems and beyond. *Journal of Intelligent Manufacturing*, 30(8), 2805-2817.

Conference Articles

Cárdenas, A. A., Amin, S., Lin, Z. S., Huang, Y. L., Huang, C. Y., & Sastry, S. (2011, March). Attacks against process control systems: risk assessment, detection, and response. *6th ACM symposium on information, computer and communications security* (pp. 355-366).

Lawrence, F. L., & Jokonya, O. (2020, November). Factors Affecting the Adoption of Smart Buildings at Universities. *2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 1-7). IEEE.