**eNergetics 2024**
DOI: https://doi.org/10.

*Original Scientific Article*

# Attack Evaluation of Cyber Security Analysis in Cyber-Physical Power Systems: A Review Concept

Erdem Koca[1], Musa Terkes[2], Alpaslan Demirci[3]

[1]Electrical Engineering Deparment of Yıldız Technical University, Istanbul, Türkiye
[2]Electrical Engineering Deparment of Yıldız Technical University, Istanbul, Türkiye, https://orcid.org/0000-0002-4411-411X

[3]Electrical Engineering Deparment of Yıldız Technical University, Istanbul, Türkiye, https://orcid.org/0000-0002-1038-7224

[1]kocaa.erdem@gmail.com, [2]musa.terkes@yildiz.edu.tr, [3]ademirci@yildiz.edu.tr

*Abstract*—**After the technological advances, the volume of the digital data pool has fallen into a hazardous game due to cyber and physical attacks, expanding the scope of attacks and raising security concerns. In addition, cyber attackers are using new techniques to manipulate security systems and automate attacks, making cyber security more valuable than ever. It is essential to meticulously address hardware, software, communication, and physical-layer vulnerabilities, identify the main causes of attacks, and detail the operational evolution of attack types. Especially in complex and functionally active cyber-physical power systems (CPPS), safe and reliable operation must be guaranteed with timely detection and defense actions depending on the extent of the attack. This review explains the key terms of cyber security analysis in CPPSs and provides an in-depth overview of the process and aftermath of threats based on attack types. It discusses traditional and next-generation cyber and physical attacks and vividly illustrates the importance of security through real events resulting in cyber vulnerabilities, making the topic more relatable. The study meticulously evaluates the individual and social damages of various cyber-attack practices. It concludes that reinforcing the cyber security of digitalized energy systems is essential for national security and economic stability.**

**Keywords** - Cyber security; Cyber-attack; Physical attack; Cyber-physical power systems; Malware.

## I. INTRODUCTION

Cyber-physical power systems (CPPS) are unique technological infrastructures that manage and control energy generation, transmission, and distribution, integrating traditional energy systems with digital control systems designed to increase efficiency, improve autonomic energy management, and maximize system reliability. They transform the energy landscape of the modern world by combining advanced information processing technology and automation. It manages physical energy infrastructure such as power plants, transmission lines, and distribution networks through information processing, data analytics, and automation processes in cyberspace. It performs many functions to guarantee efficiency, reliability, and sustainability in the physical infrastructure. For instance, it can optimize energy flow by analyzing data collected in real time or proactively detect and manage potential outages and energy system maintenance. Thanks to its proactive behavior, the situation is controlled via early changes instead of waiting for adverse action. It can also offer solutions to carbon concerns by serving to develop renewable

ISBN: xxx-xx-xxxxx-xx-x


Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-Non Commercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission.

energy potential via data-driven management strategies. However, for this to happen, more is needed to use a single system or component in CPPS with the desired accuracy, efficiency, and ergonomics. Simultaneous synchronization and communication of multiple components is required. These include sensors continuously monitoring physical parameters and actuators performing physical actions based on the received data. Broadband communication networks, including wired or wireless technologies that guarantee reliable and sustainable data flow and enable remote monitoring and control, form the communication framework of CPPS. In this direction, a schematic diagram of CPPS is shown in Fig.1 [1].

One of the control, remote monitoring, and data acquisition technologies often used in system infrastructure is supervisory control and data acquisition (SCADA). The human-machine interface (HMI) enables operators to control and monitor equipment in the field, while the graphical user interface provides information on the real-time status of the facility. Alarm and notification systems alert operators in case of abnormal or malfunctioning situations, guaranteeing a fast and effective intervention. This functional process occurs as programmable logic controllers (PLC) and remote terminal units (RTU) process and evaluate data collected from sensors in the field to SCADA. PLCs, which can be expanded with different input/output modules, send commands to actuators based on the data being processed. Often used in geographically distributed systems, RTUs are designed to operate in extreme environmental conditions (e.g., water and wastewater management) and are used to collect data. Ethernet and fiber optics are used for communication infrastructure in wired options, while radio frequency and satellite communication are often preferred in wireless alternatives. Especially in the energy sector, SCADA systems focus on increasing efficiency, reducing costs, and securing energy systems. The general structure of SCADA is shown in Fig. 2 [2]. Integrating SCADA systems with CPPS is one of the most critical aspects of the digital transformation in the energy sector. CPPS can use machine learning and artificial intelligence to optimize production processes, guaranteeing higher efficiency and adaptability. In this context, SCADA provides real-time data flow to control and manage processes. The integrated system enables faster fault condition detection and automatic response mechanisms in power generation and distribution operations.

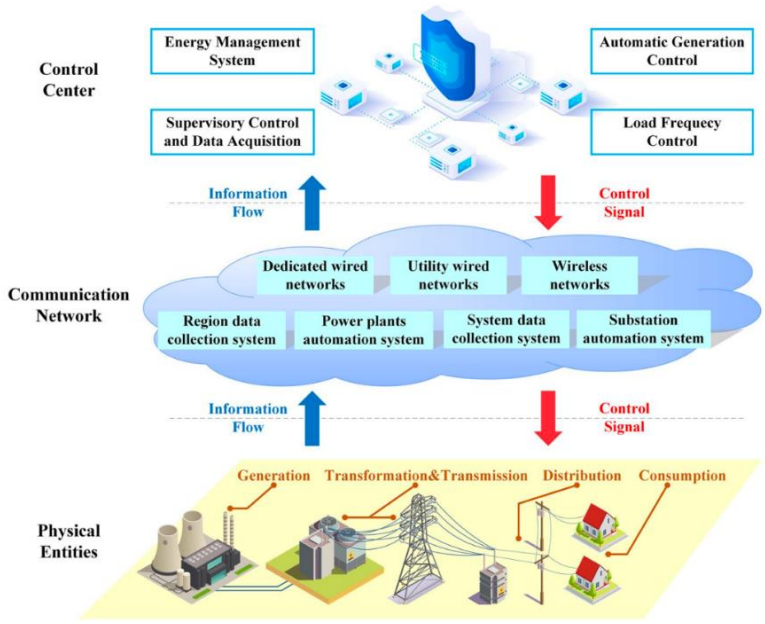



Figure 1. CPPS schematic diagram

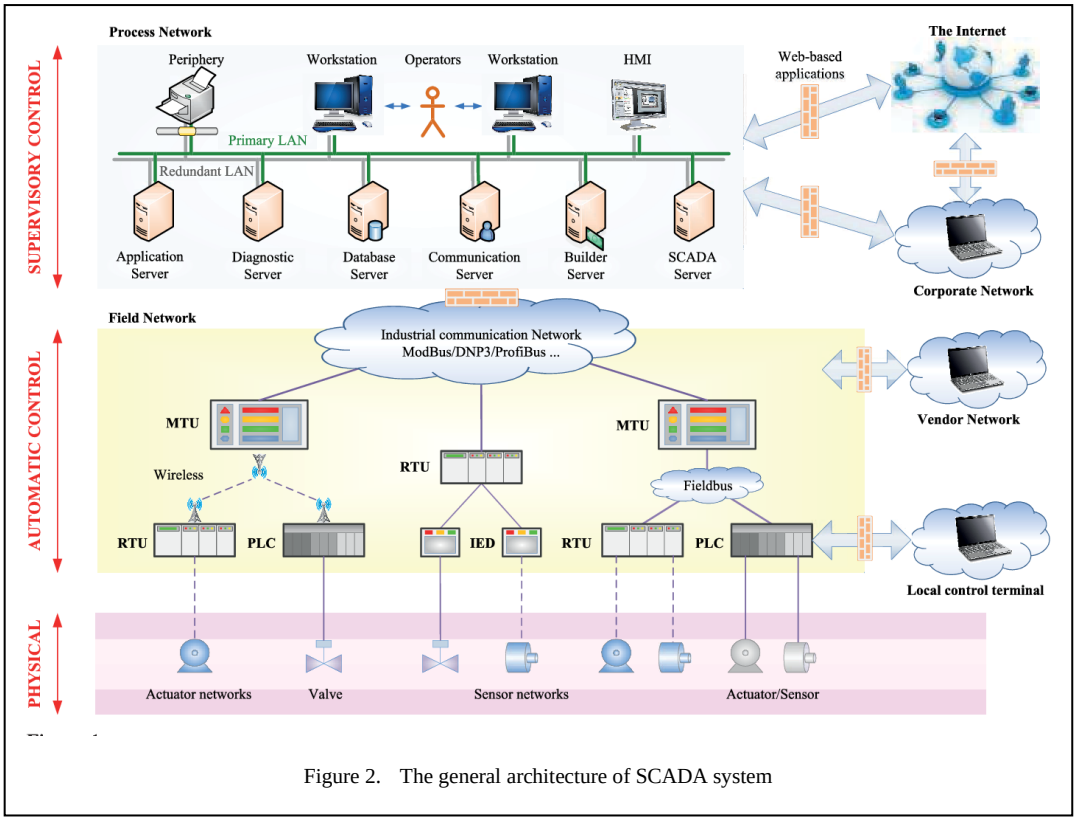



Figure 2. The general architecture of SCADA system

A comprehensive review of the vulnerability of CPPSs to cyber-attacks across cyber-attack types is more valuable than ever due to its complexity and critical functionality. Minor vulnerabilities, especially between layers, can profoundly impact the entire system infrastructure and cause irreversible failures and unsustainable services. To develop cyber-attack defense mechanisms and detection methods, it is essential to conduct attack analysis and know the types of attacks well. This review starts from the basic cyber security terminology for the reliable, sustainable, and social welfare of society. It discusses the types of attacks that threaten security and are at the center of the attention of attackers and their functioning process. In addition, real-life examples of cyber-attacks emphasize the importance of the potential effects of attack types. However, this review focuses only on the attack side, as the attack defense mechanism and detection methods need to be broadly addressed. Section I details the development of CPPS and its potential functional uses today, while Section II discusses the types of cyber and physical attacks, starting with cybersecurity-related terminology. Section III highlights the inspiration for the review and draws inferences for cyber and physical attacks.

## II. Cyber Security Analysis In Cyber-Physical Power Systems

### *A. Fundamental Terms in Cyber Security*

Understanding cybersecurity terminology is essential to determining the severity and scale of a cyber-attack and evaluating the threats affecting data. The first thing that comes to mind is the CIA triangle (see Fig. 3), an idea derived from the terms Confidentiality, Integrity, and Availability, which provides a common framework for cybersecurity analysis [3]. Confidentiality, which means that information is accessible only by authorized persons, aims to minimize the risks of unauthorized persons illegally obtaining, stealing, disclosing, or using the information. Integrity means that information is accurate, complete, and unaltered. Availability is represented by making information available to authorized persons when and where it is needed. As a result, the CIA triad describes the basic principles of information security and aims to protect the organization's information assets.

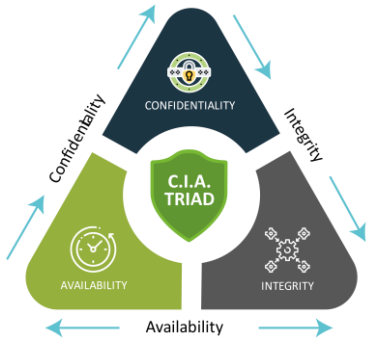



Figure 3. The CIA triad and fundamental principles

Violating any of the three principles results in data loss and eliminates the functionality of the policy chain. Fig. 3 illustrates the relationship between the CIA triad and its principles [4].

A threat is a phenomenon that can damage a system or compromise data. Threats can be software, such as computer viruses, spyware, malicious bots, human error, and environmental factors, such as physical damage or natural disasters. Another concept is vulnerabilities. Vulnerabilities are gaps where an attacker can damage a system, and software errors, outdated infrastructure, weak encryption, or misconfigured networks are indicators of vulnerability. Risk is the combination of the likelihood that a threat will exploit a vulnerability and the possible consequences of that exploitation. Especially in cybersecurity, risk assessment can effectively determine which security measures to prioritize. If the necessary precautions are not taken for risks, attack threats that exploit vulnerabilities will inevitably damage the system. Various threats include distributed denial of service (DDoS) attacks, phishing, and ransomware. Analysis of attacks provides information on how to reinforce defense mechanisms and develop event response plans. Accordingly, defense mechanisms have security controls that can counter threats and address vulnerabilities. Firewalls, antivirus software, encryption, and access control systems are some of such security procedures.

### B. *Next Generation Cyber Attacks Against Traditional Threats*

Traditional threats and next-generation cyber-attacks differ significantly in terms of both impact and prevention methods. While traditional threats are more straightforward and focused on a single vector, next-generation attacks are characterized by complexity and multiple attack vectors. Traditional threats rely on manual interventions, making them easier to detect and prevent, while next-generation attacks use artificial intelligence and automation technologies to create widespread impacts.

While traditional threats target individual devices and small-scale systems, next-generation attacks can target critical infrastructure and large-scale organizations. There is also a big difference in the impact period. While traditional threats cause short-term problems, next-generation attacks can have long-term and permanent effects. Therefore, advanced security systems, zero-trust approaches, and solutions based on continuous threat intelligence are required against next-generation threats.

This distinction and analysis help organizations develop an effective security strategy against both traditional threats and next-generation attacks. Especially given the complexity of next-generation attacks, proactive and automated approaches are critical to ensure the sustainability of security.

### C. *Types of Attacks on Cyber-Pyhsical Power Systems*

Attackers acting for data theft or manipulation may sometimes be unsuccessful in a similar scenario. The attacker, who tries alternative methods until he succeeds, can use many techniques in the attack organization. Here, many types of attacks, from cyber to physical, are discussed.

#### 1) *Cyber attacks*

##### a) *Time synchronization attacks (TSA)*

Operational control of the power system in widely distributed systems is achieved by synchronizing the operation control time in different regions. Timescale signals from GPS satellites are used for the respective purpose and to decide the power flow in transmission and distribution systems. In CPPSs, especially in power management units (PMU), the time synchronization device communicates in plain code without a password authentication mechanism, which introduces many flaws. Using these flaws in their cyber terminals, false synchronization time is received, and fake satellite navigation messages are transmitted via time synchronization attacks in decoding. It also causes time drift in calibration data, corruption of wide-area measurement systems, and incorrect control decisions in the power regulation and

control system. With the loss of control of the system, the attack and destruction achieve their goal [5]. The spoofing of satellite signals was analyzed in [6] using security code prediction and replay attacks. Another approach in [7] tested low-cost controller-based GPS analog positioning software that broadcasts spoofed GPS signals via multiple function calls. A unified replay strategy for suppressing and spoofing GPS signals that cause significant time jumps in time synchronization is investigated in [8]. To illustrate the situations that societies face: a time data jump caused by a malfunction in a time synchronization device caused the power control center in Western China to generate power on the wrong date and several turbines in hydroelectric power plants to shut down abnormally [9]. Although the event was not caused by a cyber-attack on the time synchronization base, it proves the potential of the threat.

*b) Fake data injection attacks (FDIA)*

Fake data injection attacks (FDIA) maliciously manipulate measured data at sampling terminals or state estimation results at control terminals in CPPSs. This results in incorrect assessment and management of operational status and control. The damage level is vital due to the complex topology of CPPS and the low redundancy of measurement data. It can attack sampled voltage, injected power, or line power flow data, especially in SCADA systems. It can also degrade the performance of power system state estimation and load frequency control. It can cause unstable system operations in SCADA and automatic generation control systems. The general action process of FDIA is shown in Fig. 4 [1].

The type of attack concerned is broadly divided into two categories: physical and cyber-based. In the physical-based method, which targets monitoring, control, and security devices, the level of access to various equipment is discussed in [10], the most notable being access to the main processor-based mechanism by causing the RTU software to change. While the number of devices vulnerable to such attacks is limited, cyber-based attacks are typical. The cyber-based subcategory involves the attacker violating the control system or associated applications (process layers such as forecasting, economic distribution, and energy trading) [11]. Such attacker attempts targeting system operations and services can be launched via physical communication modules. This differs from inserting malware into a computer software system or database.

*c) Distributed denial of service (DDoS) attacks*

Distributed denial of service (DDoS) attacks are the most common threat to critical infrastructure today and target the communication network of systems. They prevent legitimate users from accessing services by flooding them with excessive fake traffic. Botnet creation has a series of sequential functionalities such as Command and Control (C&C) servers, target identification, traffic generation, attack methods, and sustaining and terminating the attack [12]. DDoS attacks consist of internet-connected devices (bots) infected with malware (malicious software) that cyber attackers can control. The botnet's size determines the attack's effectiveness, while remote management of the devices allows the targeted attack to be launched at any time. The botnets are managed via command-and-control servers, and the attacker determines when and how to intervene on the infected devices. Once the attack is launched, the botnet network continuously sends fake requests to the target while determining the traffic generation method that will consume the most network resources. To consume the network's bandwidth, it may send large amounts of data or requests that force server processors to perform intensive processing. In real-world examples, a cyberattack targeting the electricity supply network in Ukraine in 2015 blocked access to control systems, disabled automated systems, and left around 230,000 people in the dark [13].

*d) Denial of service (DoS) attacks*

Denial of service (DoS) attacks are performed to close the target system, service, or network to user access. Its primary purpose is to overload the target system's resources (CPU, memory, bandwidth, etc.) and render it unserviceable. It causes the target system to collapse, slow down, or become completely unusable. Flooding, amplification, and protocol-based attacks are available [14]. Flooding attacks cause many user datagram protocol (UDP) packets to be sent to the target system, followed by checking the packets for validity, resulting in excessive resource utilization. Similar resource consumption can also occur when an attacker sends Internet Control Message Protocol (ICMP) “ping” packets rapidly at a high rate and size. The SYN flag initiates synchronization (SYN) flood

attack type. After sending incomplete transmission control protocol (TCP) connections to the target, the target system requests SYN-ACK packets to complete these connections. Still, the attacker cannot send them, resulting in a backlog of incomplete connections and depletion of resources.

On the other hand, amplification attacks are at least as notable as flooding. Specifically, in the Domain Name System (DNS) based attack subcategory, the attacker uses fake internet protocol (IP) addresses to send minor requests to DNS servers. In this way, large responses or large amounts of data are sent from the DNS servers to the spoofed IP addresses, consuming the bandwidth of the target system. Similar logic and procedure can be used to attack network time protocol (NTP) servers instead of DNS. Another example of DoS attacks is protocol-based ones. In network broadcasts using a spoofed IP address, especially in the Smurf attack subcategory, the attacker sends ICMP "ping" requests. Resource consumption cannot be avoided as all devices connected to the network will need to respond to the target system. Fraggle threats, a variant of Smurf attacks, use UDP traffic and packets to broadcast the network and have a similar goal. The classification, types, and example command sequences of DoS attacks are described in Table I. A comparative characteristic analysis of DoS and DDoS attacks, which are often confusing, is highlighted in Table II.

*e) Data replay attacks (DRA)*

Data replay attacks (DRA) fools trusted certification systems by intercepting and retransmitting data messages specific to certain functions, often encountered in authentication. Due to its ability to eavesdrop on networks, it represents a significant threat to CPPS as it can be easily implemented in wireless communication applications [15]. When DRAs are launched by an attacker, manipulation of control commands can directly damage the physical system or prevent anomalous condition detection by replaying incorrect measurement data [16]. Behavioral analysis and detection methods of such attacks, which can cause severe accidents by triggering security defenses, are described in detail in [17], [18].

*f) Phishing attacks*

Phishing is a social engineering attack that attempts to steal private information such as identity, financial, and security data via emails, messages, or websites. There are process steps such as targeting, preparing fake communication, connection, and fake websites, data collection, and deepening the attack. Information technology (IT) personnel and administrators with access to the system are the primary targets, and the attack is made more convincing by investigating the contact information of the relevant people in advance. Victims receive emails and messages from official institutions and individuals but are edited by cyber attackers. After the unsettling messages, which may be urgent calls to action, the victim is redirected to a fake web address. In phishing emails, the redirected sites are copies of legitimate sites, and the attacker controls the victim's credentials based on the identification of login credentials on the sites. An attacker can use this information to access the organization's networks, infiltrate accounts, or launch a broader cyber-attack. Specifically in Ukraine, sophisticated phishing emails sent to system operators in 2015 contained a malicious Microsoft Office document that, when opened, infected systems with the Black Energy malware. This malware infiltrated systems controlling the electricity grid, causing more than 230,000 people connected to the power grid to lose power [13].

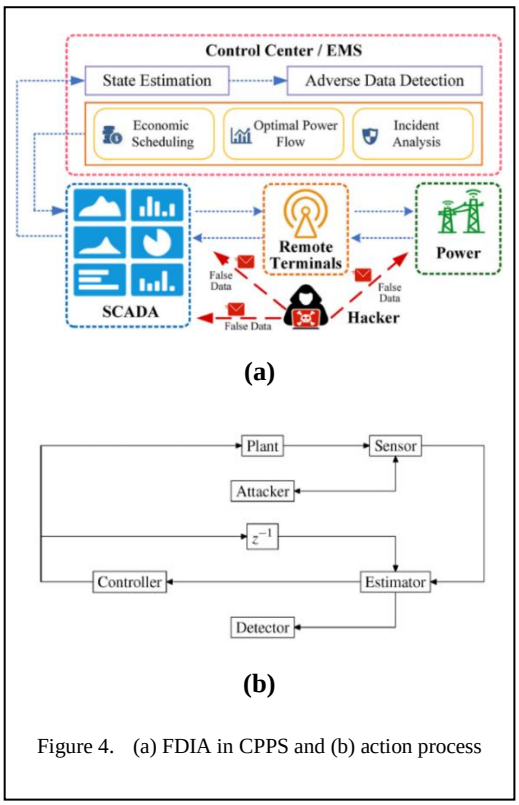



Figure 4. (a) FDIA in CPPS and (b) action process

On the other hand, a similar example happened to Saudi Aramco in 2012. The spread of a computer virus called Shamoon increased after phishing emails containing malicious links were sent to company employees. The malware turned off around 35,000 computers and caused severe problems in the company's business operations [19]. Another example occurred in 2016 against a water utility in the US. Business employees who clicked on fake emails were redirected to a phishing site, making it easier for cyber attackers to infiltrate the system with the information they received. They accessed systems that control water treatment processes and tried to change chemical dosage settings. A severe cyber-attack that would negatively affect human health has survived [20].

*g) Side-channel attacks*

Side-channel is a type of attack that extracts indirect information from the physical operation of the computer or device. It analyzes the by-products (electromagnetic emissions, power consumption, processing times, acoustic signals, etc.) the target system performs while operating, i.e., physical data. The most essential feature is that instead of stealing data directly, it uses information exfiltrated during the normal activities of the target system. Cyber attackers' main methods to obtain information are timing, power, electromagnetic and acoustic analysis. In timing analysis, secret information is obtained by measuring the time spent during the execution of the process. In the field of cryptology, the use of different key/input variations in decryption is subject to various processing times, and by analyzing the time differences, the attacker can detect a specific part or all of the cipher. An example is the Rivest-Shamir-Adleman (RSA) algorithm, widely used in cryptology. The algorithm includes different time intervals depending on the cipher size being exchanged and using modular exponentiation. If the attacker can measure the execution times accurately enough, they can guess some of the private cipher's bits. Power analysis measures the energy consumed by the device during execution. There are two types: simple and differential. Simple power analysis provides critical information by observing the power consumption during a single operation. Differential power analysis performs statistical analysis of many measurements and sophisticated information extraction [21].

Another approach is to study the electromagnetic waves emitted by the device during the operation. Specifications for the process are obtained by focusing on high-frequency processes. Acoustic cryptanalysis is used to analyze the sounds emitted by devices during operation. The sounds produced by various keystrokes and the sounds the processor makes for a task can provide information about the command. High-sensitivity microphones can be used for these tasks, while audio recordings are analyzed to achieve the goal. To prevent side-channel attacks from being effective in CPPS, device physical security measures should be improved, electromagnetic shielding should be used, and processing times should be standardized.

*h) Man-in-the-Middle attacks (MitM)*

MitM is performed by getting between two sides to eavesdrop, redirect, or modify the communication. The attacker controls the entire data flow, but the victims think they are communicating securely. There are processing steps such as eavesdropping, data monitoring and modification, false identity, and spoofing. This cyber-attack usually impersonates the server via Address Resolution Protocol (ARP) and DNS spoofing, Secure Sockets Layer (SSL) stripping, and Wi-Fi eavesdropping. To determine which IP address devices on the network correspond to, devices send an ARP request. To fulfill this request, an ARP response containing the device's Media Access Control (MAC) address is received. In this reliable and seamless process, the ARP protocol has no mechanism to verify the responses sent. The attacker sends spoofed ARP responses to the ARP tables of one or more devices on the network. The spoofed responses associate the attacker's MAC address with IP addresses on the target system. Traffic that would have been routed to IP addresses is falsely routed to the attacker's device, which can then be manipulated (eavesdropping, modifying, or blocking). It is considered part of high-damage attacks, with a high risk of infecting ransomware. The system that converts the IP addresses of devices on the Internet into human-understandable domain names is known as DNS, and a similar cyber-attack can be carried out via this platform. The computer performs a DNS query on the web addresses visited, and the user's internet service provider will inevitably redirect to its own or another DNS server after the query. The attacker interferes with this process and generates fake DNS responses and the user is redirected to the incorrect IP address.

TABLE I. A CLASSIFICATION OF DOS ATTACKS AND A SAMPLE CODE SEQUENCE.

| Class | DoS Attack Type | Sample Command |
|---|---|---|
| Flooding Attack | UDP flood | hping3 --udp -p 80 -i u-100 <target_IP> |
| | ICMP flood | ping -f <target_IP> |
| | SYN flood | hping3 --S -p 80 --flood <target_IP> |
| Amplification Attack | DNS | dig +short ANY example.com @<DNS_server_IP> |
| | NTP | ntpdc -n -c monlist <target_IP> |
| Protocol Based Attack | Smurf | hping3 --icmp -a <target_IP> --spoof <edition_IP> |
| | Fraggle | hping3 --udp -a <target_IP> --spoof <edition_IP> |

TABLE II. COMPARISON OF DOS AND DDOS ATTACKS.

| Attack Type / Specifications | DoS | DDoS |
|---|---|---|
| Number of resources used | Typically, a single resource | Multiple resources |
| Scale | Smaller-scale attacks | A more aggressive attack |
| Detection difficulty | Easier detection | More difficult detection |
| Complexity | Simpler | More complex |

The attack can be performed over the same local area network (LAN) or a different DNS server. SSL stripping weakens the security of a secure HTTPS connection, reducing it to an insecure connection. Wi-Fi eavesdropping involves the unauthorized capture and listening to data transmitted over wireless networks. Due to the high threat potential in weakly encrypted and insecure Wi-Fi networks, it can easily intercept personal information, log cookies, emails, passwords, and other private data. It is considered a passive attack as the data-based network is monitored and listened to, but the traffic is not intercepted. The general process of MitM attacks is shown in Fig. 5 [22].

*2) Pyhsical attacks*

While the most common threatening attacks are cyber-based, the unique physical layer attack on CPPS should be addressed. Here, the aim is to penetrate directly into the power infrastructure and damage the physical system. Electromagnetic attacks can damage electrical devices without touching them using overvoltage or electromagnetic pulses.

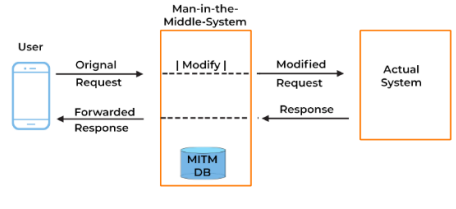



Figure 5. The general procedure of MitM attacks

Resonance attacks (RA) are a typical example and cause abnormal frequency or control variation rates in the power system by changing the power load or contact line signal relative to the resonant source. Since every system has a resonance point, routine detection methods may not easily detect it. This distorts the state signals of weak loads or generators. The RA process is illustrated in Fig. 6 [1]. It continues to be of interest to researchers. For example, the investigation of resonance implementation possibilities via two-domain load frequency control and the irreversible effects of RAs on power system frequency control were studied in [23]. RAs effects on first-order and higher-order linear and nonlinear terms, automatic voltage regulators, and power system stabilizers in similar single- and multi-domain frequency-controlled systems are studied in [24]. It has been experimentally demonstrated that the harmful RA effect may not stay in one region but may spread to other connected areas and cause severe damage.

*3) Coordinated cyber and physical attacks*

Coordinated cyber-physical attacks have recently been presented due to the complex and robust infrastructure of CPPSs. Switching between cyber and physical attack types is easy with two parallel overlapping layers. A general flow of the coordinated attack plan is shown in Fig. 7 [1].

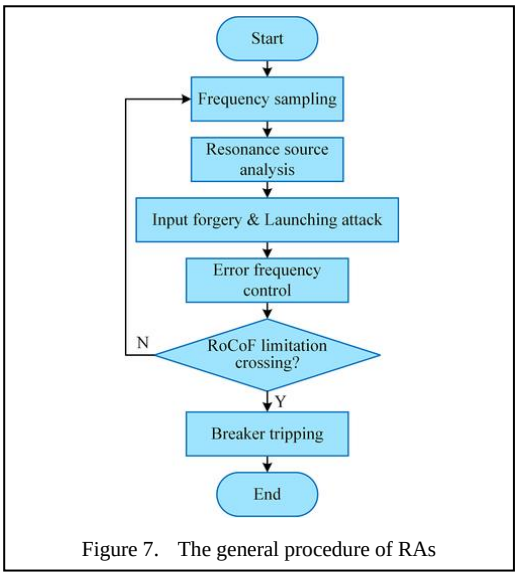



Figure 7. The general procedure of RAs

Venezuela also suffers from a holistic attack plan that facilitates the transition from a singular attack to a large-scale and potent threat. The incident in 2019 exposed the weaknesses of delaying attack detection and exploiting the window of time, proving its great offensive power and defensive challenge [25].

## III. CONCLUSIONS

The changing landscape and growing data usage in power systems and CPPS are potential targets for cyber-attacks. What are the terminologies often used in cybersecurity analysis? What types of cyber threats have organizations and systems faced today, and what vulnerabilities have caused them? What are the types of cyber-attacks to which high-risk victims may be exposed? The key to addressing these questions lies in the continuous evolution of cyber-attack operational processes.

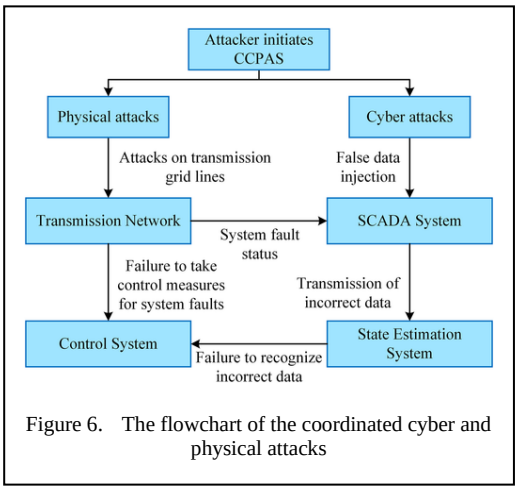



Figure 6. The flowchart of the coordinated cyber and physical attacks

This review aims to provide a comprehensive discussion of the types of cyber-attacks, along with an evaluation of commonly used security standards and terms, their strengths and weaknesses, and the security issues in CPPSs. Defense mechanisms and detection methods in response to cyber-attacks are excluded from the review, focusing on attack analysis and types. With the support of modern communication resources and technology, integrating various physically distributed computing and control mechanisms for CPPS development can solve complex problems with improved capacity performance and promote intelligent resource allocation and energy management. However, the complex structure of power systems can face many types of cyber-attacks due to their distributed and interactive features in time-based operations and their dynamic operation characteristics. For attackers, given the most vulnerable points of the power system, fake data injection attacks are a powerful trump card that can circumvent common detection mechanisms. Due to the high coupling at the cyber and physical layers, an underestimated vulnerability in CPPSs can spread rapidly, creating large-scale power outages and profoundly affecting the sustainable economy. By further exploring attack mechanisms and sequential fault analysis and types in this way, cyber defense architecture can be reinforced, and improving the performance of strategic developments for attack detection can guarantee societal security and welfare. Future work aims to evaluate the societal and economic impact of specific types of cyber-attacks on CPPSs to understand further the critical role of these systems on society and the economy, not just limited to technical security measures.

## REFERENCES

[1] Adepu, S., & Mathur, A. (2021). Distributed Attack Detection in a Water Treatment Plant: Method and Case Study. IEEE Transactions on Dependable and Secure Computing, 18(1), 86–99. https://doi.org/10.1109/TDSC.2018.2875008

[2] Assante, M. (2016). Confirmation of a Coordinated Attack on the Ukrainian Power Grid. 23, 1–5. ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[3] Ayiad, M. M., Leite, H., & Martins, H. (2021). State Estimation for Hybrid VSC Based HVDC/AC: Unified Bad Data Detection Integrated With Gaussian Mixture Model. IEEE Access, 9, 91730–91740. https://doi.org/10.1109/ACCESS.2021.3092308

[4] Content Team. (2021). What is The CIA TRIAD & its Importance for Cybersecurity. Web Security Store. https://websitesecuritystore.com/blog/what-is-the-cia-triad/

[5] Disttrack, S., & Update, M. (2017). Joint Security Awareness Report ( JSAR-12-241-01B ). 3, 16–18.

[6] Do, V. L., Fillatre, L., Nikiforov, I. V, & Willett, P. K. (2017). Feature article: security of SCADA systems against cyber–physical attacks. IEEE Aerospace and Electronic Systems Magazine, 32, 28–45. https://api.semanticscholar.org/CorpusID:20875820

[7] Fruhlinger, J. (2020). The CIA triad: Definition, components and examples. CSO Online.

[8] He, X., Liu, X., & Li, P. (2020). Coordinated False Data Injection Attacks in AGC System and Its Countermeasure. IEEE Access, 8, 194640–194651. https://doi.org/10.1109/ACCESS.2020.3033566

[9] Humphreys, T. E. (2013). Detection Strategy for Cryptographic GNSS Anti-Spoofing. IEEE Transactions on Aerospace and Electronic Systems, 49(2), 1073–1090. https://doi.org/10.1109/TAES.2013.6494400

[10] Ingram, D. M. E., Schaub, P., Campbell, D. A., & Taylor, R. R. (2012). Evaluation of Precision Time synchronisation methods for substation applications. 2012 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication Proceedings, 1–6. https://doi.org/10.1109/ISPCS.2012.6336630

[11] Kim, J., & Tong, L. (2013). On Topology Attack of a Smart Grid: Undetectable Attacks and Countermeasures. IEEE Journal on Selected Areas in Communications, 31(7), 1294–1305. https://doi.org/10.1109/JSAC.2013.130712

[12] Kovacs, E. (2016). Attackers Alter Water Treatment Systems in Utility Hack: Report. https://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report/

[13] Liu, C., Liang, H., & Chen, T. (2021). Network Parameter Coordinated False Data Injection Attacks Against Power System AC State Estimation. IEEE Transactions on Smart Grid, 12(2), 1626–1639. https://doi.org/10.1109/TSG.2020.3033520

[14] Liu, K., Ma, S., Ma, A., Zhang, Q., & Xia, Y. (2021). Secure control for cyber-physical systems based on machine learning. Acta Automatica Sinica, 47(6), 1273–1283.

[15] Liu, S., Hu, Z., Wang, X., & Wu, L. (2019). Stochastic Stability Analysis and Control of Secondary Frequency Regulation for Islanded Microgrids Under Random Denial of Service Attacks. IEEE Transactions on Industrial Informatics, 15(7), 4066–4075. https://doi.org/10.1109/TII.2018.2885170

[16] Liu, X., Li, Z., Liu, X., & Li, Z. (2016). Masking Transmission Line Outages via False Data Injection Attacks. IEEE Transactions on Information Forensics and Security, 11(7), 1592–1602. https://doi.org/10.1109/TIFS.2016.2542061

[17] Mahmoud, M. S., Hamdan, M. M., & Baroudi, U. A. (2019). Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges. Neurocomputing, 338, 101–115. https://doi.org/10.1016/j.neucom.2019.01.099

[18] Mohajerin Esfahani, P., Vrakopoulou, M., Margellos, K., Lygeros, J., & Andersson, G. (2010). Cyber attack in a two-area power system: Impact identification using reachability. Proceedings of the 2010 American Control Conference, 962–967. https://doi.org/10.1109/ACC.2010.5530460

[19] Mohanakrishnan, R. (2022). What Is a Man-in-the-Middle Attack? Definition, Detection, and Prevention Best Practices for 2022. Spiceworks. https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

[20] Qian, B., & others. (2020). Review on time synchronization attack in power system. Power Syst. Technol, 44(10), 4035–4045.

[21] ShangGuan, X.-C., He, Y., Zhang, C.-K., Jin, L., Jiang, L., Wu, M., & Spencer, J. W. (2021). Switching system-based load frequency control for multi-area power system resilient to denial-of-service attacks. Control Engineering Practice, 107, 104678. https://doi.org/10.1016/j.conengprac.2020.104678

[22] Su, L., Ye, D., & Zhao, X. (2020). Static output feedback secure control for cyber‐physical systems based on multisensor scheme against replay attacks. International Journal of Robust and Nonlinear Control, 30(18), 8313‐8326. https://doi.org/10.1002/rnc.5254

[23] Tippenhauer, N. O., Pöpper, C., Rasmussen, K. B., & Capkun, S. (2011). On the requirements for successful GPS spoofing attacks. Proceedings of the 18th ACM Conference on Computer and Communications Security, 75–86. https://doi.org/10.1145/2046707.2046719

[24] UCL Crypto Group. (n.d.). Theoretical Models for Side-Channel Attacks. Retrieved August 1, 2024, from http://www.dice.ucl.ac.be/fstandae/tsca

[25] Wang, Q., Tai, W., Tang, Y., Zhu, H., Zhang, M., & Zhou, D. (2019). Coordinated Defense of Distributed Denial of Service Attacks against the Multi-Area Load Frequency Control Services. Energies, 12(13), 2493. https://doi.org/10.3390/en12132493

[26] Wu, Y., Wei, Z., Weng, J., Li, X., & Deng, R. H. (2018). Resonance Attacks on Load Frequency Control of Smart Grids. IEEE Transactions on Smart Grid, 9(5), 4490–4502. https://doi.org/10.1109/TSG.2017.2661307

[27] Yang, T., Liu, Y., & Li, W. (2022). Attack and defence methods in cyber‐physical power system. IET Energy Systems Integration, 4(2), 159‐170. https://doi.org/10.1049/esi2.12068

[28] Yang, Y. D., Lan, S. L., Tan, Z. J., & others. (2020). Coordinated cyber-physical attacks of cyber-physical power system. Electric Power Automation Equipment, 40(2), 97–102.

[29] Zhang, H., Peng, S., Liu, L., Su, S., & Cao, Y. (2020). Review on GPS spoofing‐based time synchronisation attack on power system. IET Generation, Transmission & Distribution, 14(20), 4301‐4309. https://doi.org/10.1049/iet-gtd.2020.0253

[30] Zhao, Y., & Smidts, C. (2020). A control-theoretic approach to detecting and distinguishing replay attacks from other anomalies in nuclear power plants. Progress in Nuclear Energy, 123, 103315. https://doi.org/10.1016/j.pnucene.2020.103315