Cyber–Physical Systems Forensics

Subjects: Others | Others

Contributor: Jameela Al-Jaroodi

Cyber–Physical Systems (CPS) connect the physical world (systems, environments, and humans) with the cyber world (software, data, etc.) to intelligently enhance the operational environment they serve. CPS are distributed software and hardware components embedded in the physical world and possibly attached to humans. CPS are vulnerable to security risks, which requires incorporating appropriate forensics measures in the design and operations of these systems.

Keywords: cyber-physical systems ; CPS ; digital forensics ; network forensics

1. Introduction

Cyber–physical Systems (CPS) provide useful integration and interactions between the physical and the cyber worlds [1]. CPS offer promising technology that adds many capabilities to different physical-based applications in diverse domains. CPS can be used to enhance automation capabilities in manufacturing processes for better productivity, efficiency, accuracy, safety, and reliability [2][3]. It can be used in healthcare applications to provide useful real-time services for patients and healthcare professionals [4][5]. CPS can be used in large commercial and residential buildings to improve energy efficiency and living/working conditions [6][7]. They can also be used in transportation systems to enhance safety and efficiency [8]. CPS utilize and integrate numerous technologies, features, and ideas from networking, distributed systems, sensors, embedded systems, software systems, and hardware devices such as microcontrollers and actuators. CPS also encompass different disciplines such as mechanical, biomedical, construction, systems, and electrical engineering along with healthcare, transportation, and energy fields to add value to applications in the physical world [9].

While CPS can offer many smart enhancements for improving physical systems and processes, they are, like any other computerized and distributed system, vulnerable to security attacks and criminal activities. Unlike other systems, however, security attacks may cause not only data, software and hardware damages but also major physical damages. These physical damages may include human deaths and injuries, infrastructure damages, loss of resources, and machine breakdowns or malfunctions. An interesting case involving a security attack on a CPS known as the Stuxnet worm is analyzed in [10]. The Stuxnet worm is a highly sophisticated cyber-attack using several security attack techniques with a specific goal of disabling a manufacturing facility. Another attack was discovered a few years later on the US power grid (Calpine Corporation, Houston, TX, USA) with the intentions of causing a major blackout in the country [11].

When a general-purpose software is attacked or breached, forensics (digital criminal investigations) will involve analyzing operational and access logs, tracking network traffic sources, and figuring out how it was done, who did it, and of course why. Forensics efforts will also use this information and additional software operational information to create defense mechanisms for future attacks. As the applications of CPS are rapidly being developed and deployed in different critical domains, various security measures are considered and included to protect them. Along with the security measures, it is extremely important that CPS also include suitable and effective forensics capabilities. These are critical, yet difficult to achieve, when attacks are detected and investigations to find the culprits and mitigate the damages are needed. In CPS, the forensics process becomes a much wider and more complex endeavor. Analysis, tracking, and investigations will have to cover all software and hardware components, digital and physical evidence, and all interactions across the whole system, which usually involves largely distributed and heterogeneous components. In addition, currently available CPS forensics methods rely mainly on traditional techniques that, despite their effectiveness in some fields, may not be effective enough for CPS forensics. As a result, CPS forensics can benefit from another native behavior/feature of CPS, which is access to huge amounts of data. Data collected before, during and after a security attack are available for analysis to arrive at more definitive forensics evidence. The key is to adapt forensics techniques and create new ones that can take advantage of these data.

2. Background

This section covers some related work and background information about CPS, forensics, and the relevant work in these fields.

2.1. Cyber-Physical Systems

CPS are networked embedded systems, categorized by solid and constant interactions between physical and cyber components [9]. CPS are being progressively utilized everywhere to enhance physical domains. A great part of CPS is designed to support smart and context-aware mission-critical applications [1]. Predefined objectives of the related application domain are realized through the monitoring and control processes, as provided by CPS. The control decisions are usually performed by the cyber world using smart algorithms constructed by software.

Unlike regular embedded systems, CPS are networked embedded systems that consist of several heterogeneous distrusted components. These components may be computing nodes, sensors, actuators, smart devices, and software. These components are connected through wired and/or different types of wireless networks, as shown in **Figure 1**. Both sensor and actuator components are tightly attached to their physical environment. Sensors and actuators provide the interface between the cyber world and the physical world. Sensors are used to monitor the physical world, while the actuators are used to manipulate the physical world. One or more computation units are used to execute control software for the environment. These computation units can be computers or microcontrollers.

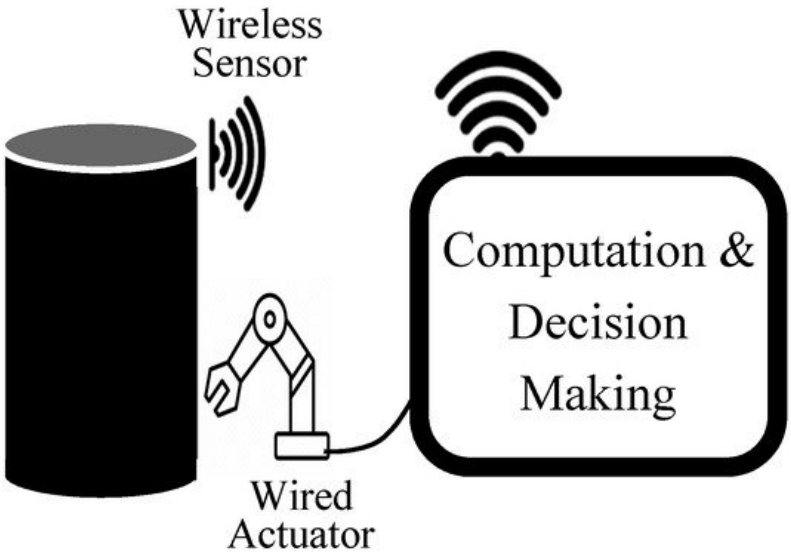

Figure 1. Cyber–physical Systems (CPS) components connected by wired and wireless networks.

The three main functions in CPS of operations are: monitoring using sensors, making decisions using smart software, and applying actions using actuators [12]. These three functions operate within a feedback loop covering the whole CPS as shown in **Figure 2**.

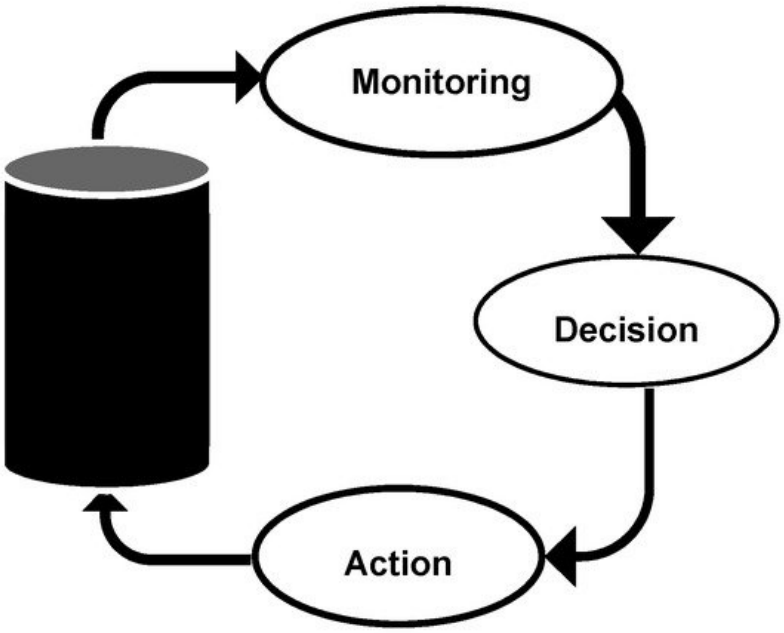

Figure 2. Closed-loop control steps of CPS.

Multiple connected CPS can also work together to complete a task or mission. These CPS form large-scale CPS that consist of multiple resources utilized for completing the assigned task or mission. Each CPS has its own sensors, actuators, and computation resources, but they need to work together. These CPS can be homogenous or heterogeneous in terms of their resources and capabilities. However, these collaborative CPS share their resources for the benefit of the application they are being used for. Such a system is referred to as a Collaborative Cyber-Physical System (CCPS) [13]. One example of CCPS is industrial collaborative robotic CPS that form the main requirement to create smart manufacturing [14].

CPS can also be connected to other systems such as cloud and fog computing to use the advanced services and large-scale resources provided by such systems. Cloud computing can provide scalable and flexible computational and storage services as well as advanced software services to support CPS. In smart manufacturing, for example, CPS collected data can be off-loaded to the cloud for storage and future analysis [15]. Fog computing can provide more localized services such as limited processing services, real-time services, data caching, short-term storage services, and efficient communication services [12]. In the smart manufacturing CPS, fog nodes can be the points of control and decision making based on the data collected locally in the area. Such functions require some storage and processing power but cannot tolerate the delays of using the cloud. When CPS utilize cloud and fog computing for their operations, they are referred to as Cyber-Physical Cloud Systems (CPCS) [16].

2.2. Forensics

Forensic science is an ancient profession associated with any type of criminal activity. Criminal investigations and the use of forensic science advanced a lot over time [17][18][19]. In the past few decades computers and software applications supporting forensics have been created and are in use for various activities such as facial recognition, DNA analysis, examining crime scene devices and content, and crime scene simulations [20]. Quickly, computers and computing devices became the crime scene for criminal activities such as stealing data, disrupting operations, or spying on others. Digital crimes led to the need for new and more sophisticated forensic approaches to computing devices, software, and data to collect evidence [21][22].

The technical and the law enforcement communities had to work together to address digital crimes and digital investigations. In addition, the legal system needed to extend some of its laws and regulations to incorporate these developments. A lot of effort and advances were made in this direction [23][24][25][26]. These rapid advancements in computing and technology increased the complexity of computer systems, and, as a result, forensics also became difficult and complex. A study of the historical development in this area is presented in [27]. A simple example to illustrate this is securing the evidence found. In a physical crime scene, the location can be isolated and access control is implemented. With digital crimes, access points to crime scenes can be unlimited and change can be done quickly and remotely. Investigators have to work methodically and fast to identify and isolate evidence before anyone can remove or modify it through digital means. This will involve severing all physical connections, disabling wireless connectivity, and possibly

finding components (cyber and/or physical) that may change or destroy evidence. With CPS, the issues are combined and magnified, adding more requirements to achieve effective and efficient forensics.

2.3. Related Work

Several researchers investigated and highlighted the importance of securing CPS and the associated issues. General security issues and challenges in CPS are investigated by many researchers such as Humayed et al. [28], Ashibani and Mahmoud [29], Wang et al. [30], Alguliyev et al. [31], Neuman [32], Banerjee et al. [33], Burg et al. [34], and Cardenas et al. [35]. Some research efforts focused mainly on security for specific CPS applications. Sridhar et al. [36] and Sun et al. [37], for example, studied the CPS security of power grids. Huang et al. [38] investigated CPS security for industrial processes. Wells et al. [39] investigated the challenges of securing manufacturing CPS.

Other research efforts offered different techniques and frameworks to evaluate CPS security. Wurm et al. [40] investigated the security vulnerabilities of some implemented CPS from a cross-layer perspective. This investigation includes the CPS and the underlying hardware platforms. DiMase et al. [41] developed a system engineering framework to evaluate the well-being of CPS security. Hahn et al. [42] developed a framework for understanding cyber-attacks and the associated security risks to CPS.

Forensic issues and solutions were investigated in many emerging related areas. Some examples of these areas are in cloud computing [43][44][45][46], fog and edge computing [47][48][49], smartphones [50][51][52][53], and internet of things (IoT) [54][55][56][57]. Cloud computing, fog computing, smartphones, and IoT are usually components of and enabling technologies for CPS. Therefore, all their challenges will be inherited by the CPS using them. Moreover, there are two major differences between the forensics of CPS and those of the other technologies. The first one is that the forensics of the other technologies are mainly of the cyber/digital type. That is the issues investigated are mostly in the software part of the system or sometimes in the directly connected devices in this system. CPS forensics, in addition to the two types above, also involve forensics on the physical environment the CPS is serving. The second difference is that CPS operations rely heavily on the utilization of the feedback and control loops. These loops span all parts of the CPS (physical, cyber/physical, and cyber). This means that the effects of an attack may cause more damage or generate effects in areas not directly connected to the location of the attacks. This unique feature in CPS will also affect the methods by which forensic data are collected and preserved for analysis. These two differences create additional challenges for CPS forensics investigations. Yet, these same unique features in CPS create opportunities to create better proactive CPS security and forensics.

Some researchers also investigated issues and proposed solutions for forensics in specific areas of CPS. One area is concerning SCADA (Supervisory Control and Data Acquisition), which is used for monitoring and controlling industrial facilities such as oil and gas refineries as illustrated in [58][59][60]. Other areas include the electrical power grid [61], smart homes [62], smart cities [63], connected vehicles [64], and additive manufacturing systems [65]. However, these efforts were mainly investigating the cyber/digital and network forensics of the CPS applications in their respective domains.

3. Security Attacks on CPS

Implementing and deploying CPS solutions benefit many applications; however, they have major security risks if they are exposed. These risks may escalate to the levels of resulting in human deaths, infrastructure damages, and negative economic impact. In CPS both the cyber part and the physical part need to be protected from any possible attacks, since these can target the physical parts, the cyber parts, or both. In addition, the effects or damages from the attacks initiated on the cyber parts may propagate to the physical parts and vice versa. One example of such an attack is gaining unauthorized access to a control software function (cyber part) leading to the injection of fake control messages, such as one making one of the actuators in the CPS perform unwanted actions. Another example could be blocking a sensor (physical part) from obtaining the correct measurements for a specific condition which may lead the software to generate incorrect results or decisions leading the whole CPS system to operate in the wrong direction.

In actual incidents, many CPS security attacks targeted parts of the CPS that could lead to physical damages by directly attacking SCADA systems or the ICS (Industrial Control System) and affecting the actual operations of the industry. In some cases, the attack may target the computing infrastructure that runs and operates the control systems. Examples include the cyberattack on the Ukrainian power grid leading to massive power outages in 2015 [66] and the cyberattack on Saudi Aramco, where over 30,000 workstations were infected with a virus resulting in operational disruptions company-wide in 2012 [67]. Several additional examples are discussed in [68][69].

Attacks on CPS can be categorized into passive and active attacks and each has some different characteristics and effects. They also differ in modes such as sources, intentions, and targets. Each of these categories is further divided into several other types as shown in **Figure 3**. Different passive and active attacks can compromise different CPS components and some examples of these attacks are depicted in **Figure 4**. The attacks may target any or all components (cyber and physical) and have effects on both. For example, attacks on ICS affecting how the device/machine will behave; disrupting or modifying messages causing some software modules to trigger the wrong actions; and hacking into a video camera and using the videos to discover trade secrets. This is in addition to the more typical attacks on the software components.

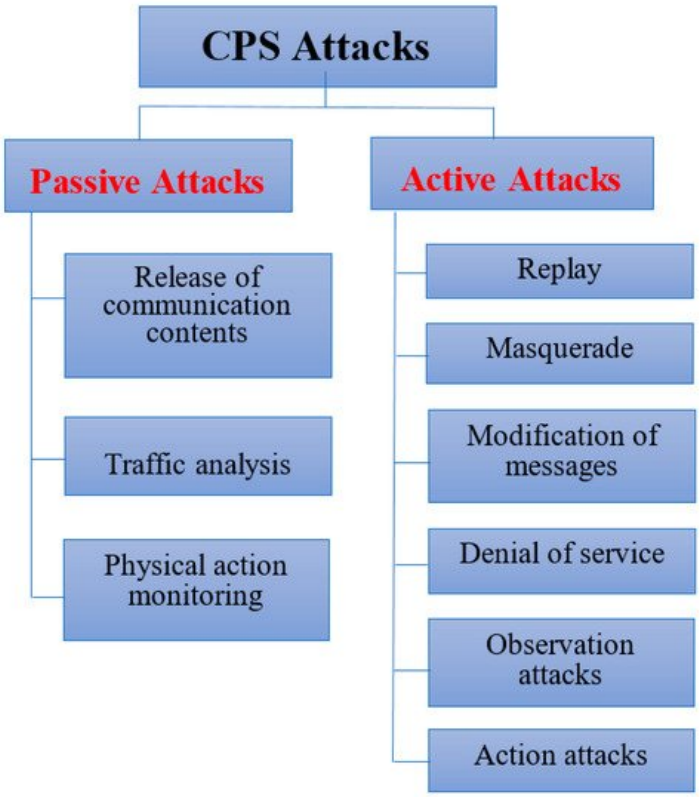

Figure 3. General CPS Attacks.

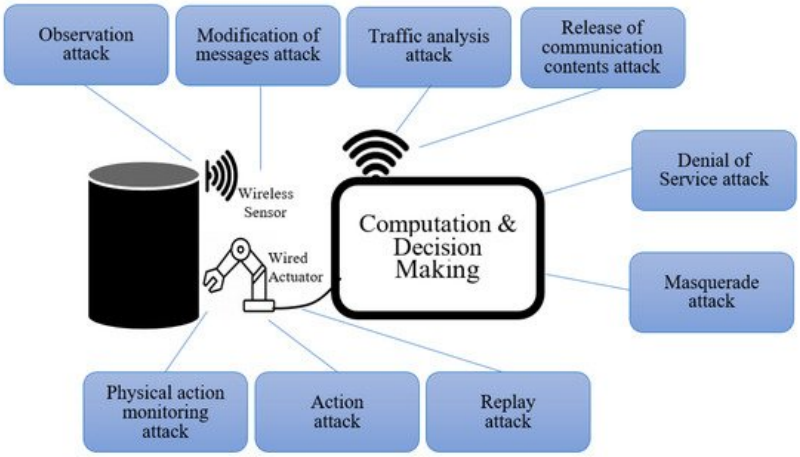

Figure 4. CPS components with possible passive and active security attacks.

3.1. Passive Attacks

Passive security attacks are recognized as attacks that provide access of some form to the CPS but does not directly affect it. Examples include eavesdropping and monitoring information transmissions; reading information stored in the system; or observing actions taken in the CPS. All of these activities will expose the CPS but will not cause any alternations or damages in the transmitted or stored information, or the CPS cyber or physical resources. As this category of attacks will not alter or damage the CPS and their operations, it is difficult to discover them. There are three possible outcomes of passive attacks: the release of communication contents; communication traffic analysis leading to, for example, trade secrets being exposed; and physical action monitoring that may help the attacker learn about operational procedures or trade secrets.

The release of communication contents will expose information that may be sensitive or private such as system information, control information, internal decisions, or other information among CPS components, among collaborative CPS, or between a CPS and other supported systems such as cloud and fog computing. Monitoring communication traffic allows intruders to know the contents of the communications in the CPS if the messages are not encrypted. If encrypted, the monitoring may not disclose the information, but can provide the intruders with the pattern of communication and sensing and control messages among different components of the CPS. Using this information, the intruders could identify the type of sensing or control messages, location of CPS components, and the type and frequency of current CPS operations.

Monitoring physical activities will allow the intruders to learn about the CPS activities and the actual operations taking place in the physical world. All of this can create multiple problems and consequences, such as violating the confidentiality of the system; violating the privacy of consumers, patients, or organizations; and enabling industrial and commercial espionage. Fortunately, many of the passive attacks can be thwarted by employing good physical security measures and using strong encryption/decryption methods for data in transit and at rest to hide exchanged information, control signals, and feedback content.

3.2. Active Attacks

The main characteristic of these attacks is that they will cause some form of alteration or damage to the CPS or some of its components. Intruders could attack by finding ways to access the system and alter communication messages, stored information, or actions to be taken. Unlike passive attacks, active attacks could be noticed relatively quickly through the alterations or damages they cause. There are six general types of active attacks on CPS: replay, masquerade, modification, denial of service, observation, and action attacks.

The first four types are attacks on the cyber parts, while the last two are physical attacks which require physical access to the system. In a replay attack, the intruder passively captures messages or action signals being exchanged and resends them in the CPS to create unauthorized outcomes including erroneous cyber or physical actions. The masquerade attack is when an intruder without any privileges or having limited privileges in the CPS impersonates entities with higher privileges to gain unheroized access and to gain access to restricted data or resources or conduct unauthorized actions. In message modification attacks, the intruders either alter, delay, or reorder some sensing or control messages to produce unauthorized cyber or physical actions. The denial of service attack is when intruders avert the regular use of CPS by flooding it with fake requests and message exchanges. This type of attack is usually performed by overloading some components of the CPS with messages greater than their capacity that will make the component and possibly the whole CPS stop or degrade operational performance. This is usually possible when the components of the CPS are connected through wireless networks or there are possible access points to the CPS components from outside the system (e.g., access through internet connections).

Observation attacks require intruders to have physical access to some sensing components in the CPS. The attack is performed by blocking the sensors or generating wrong observations through these sensors (e.g., deliberately increasing the heat near a temperature sensor to report an incorrect situation). Based on the wrong observations, the CPS may make incorrect decisions and take inappropriate actions (e.g., starting the sprinkler system in the area being monitored due to the faked high temperature readings). This type of attack usually starts as a physical attack but could quickly propagate to the cyber parts leading to software issues as well. The action attacks are also physical attacks targeting the actuators and action controllers in the CPS. Intruders may alter the actuator’s responses to change the outcomes of their operations. One example is changing the type of material in a 3D printer in the CPS so that the printed product will be faulty or will not match the specifications. Physical attacks cannot be performed without actual physical access to some CPS components.

Many methods to protect CPS from active attacks are possible such as ramping up physical security of the physical operational sites, implementing strong access and control policies, adding multiple message validation steps in critical parts of the CPS, and including active monitoring techniques in the CPS operations.

3.3. Attack Modes

CPS security attacks, whether passive or active, may come from different sources, have different targets, and have different objectives. Similar to other systems, CPS security attacks may be internal, external, or both. Internal attacks are the ones initiated by a user who is authorized to access CPS resources and services (an employee for example); nonetheless, they use these access privileges to attack the CPS. They may, for example, alter operations, use resources for alternate goals, or steal/corrupt data or information. On the other hand, external attacks are the ones initiated by

unauthorized attackers without prior access privileges to the CPS, such as criminals, competitors, terrorists, or hostile governments.

CPS security attacks may also target different parts (physical or cyber) of the CPS or all of it. For example, some passive attacks may only target digital data, for example, obtaining personnel data or spying on the message exchanges in the CPS. While others are initiated to observe physical activities to learn about operations or steal trade secrets. One example of an attack targeting physical parts is described in [65], where a thermal video camera was used to record the process of printing an object on a 3D printer and using that to obtain a detailed view of the structure and design on the object. This is also an insider attack since the camera had to be installed at the 3D printing location and passive since it did not alter the original system attacked. Passive digital security attacks will directly target the data or computational components of the CPS to steal or learn secrets.

Active attacks also have many consequences on any and all the components of the CPS. These could vary from major physical damages and loss of resources (including humans) to minor annoyances. Some catastrophic physical effects could be an explosion in a manufacturing facility, altering the operations of some manufacturing machines leading to unnoticed changes in the product, that later could cause major damages where it is used (e.g., altering the design of a medical device that could result in patients death or injuries). On the other side of the spectrum, attacks could also cause digital damages at varying levels. It could be a complete wipe out of software components or data on one end, to minor alterations of some interface layout. However, most damages in one type of resource will eventually lead to damages in the other. For example, losing some control data may lead to incorrect or delayed physical actions that may cause damages or problems. Furthermore, attacking sensors in the CPS by blocking their sensing mechanisms is a physical attack that could lead to incorrect data and incorrect results. Major examples here are the Stuxnet attack [10] and the Calpine Corporation [11]. More analysis of the propagation of attacks' impact on CPS is presented in [70].

CPS that have direct links to humans, medical CPS for example, could suffer heavily from security attacks because the possibility of human harm is very high. In [71] the authors discuss four possible security attacks on implantable medical devices. One example discussed in the article is an attack on an implantable cardioverter defibrillator, where attackers were able to inject malicious messages that could change the devices treatment actions. Energy CPS can also be affected in many severe ways, but most will not likely cause direct human harm, except when power is lost in a critical situation such as a hospital operating room during surgery. However, massive infrastructure and loss of resources is possible. Plumer [72] discusses the possibility of causing a national blackout due to security attacks. With less severe effects, a water pipeline monitoring CPS failure due to a security attack may delay the discovery of leaks, alter pressure levels, or report nonexistent leaks; all of which can be verified and managed without major losses especially to humans. **Table 1** provides a summary of major CPS applications covering their main objectives and potential security risks.

Table 1. CPS Applications Benefits and Potential Security Risks.

CPS Applications	Major Objectives	Potential Security Risks
Medical CPS	- Timely patient monitoring and treatment - Accurate monitoring and treatment	- Loss of lives and injuries - Loss of critical resources
Smart Buildings	- Reduced energy consumption - Enhanced quality of life for occupants	- HVAC (Heating, Ventilating, and Air-Conditioning) systems damages - unnecessary energy consumption - Reduction in the quality of life

CPS Applications	Major Objectives	Potential Security Risks
Smart Grids	- Optimized energy utilization - Reduced overload risks - Reduced energy waste	- Energy infrastructure damages - Energy efficiency reductions - Negative economic impact - Consumers loss of services
Pipelines Monitoring and Control	- Maintained health and operations of pipelines - Reduced impact of failures, accidents, and possible attacks	- Pipeline infrastructure damages - Possible fires due to natural gas and oil pipelines damages - Human deaths or injuries - Environmental pollution - Negative economic impact
Smart Water Networks	- Reduced water loss - Optimized water production and utilization - Enhanced water quality - Better service availability for consumers	- Water network infrastructure damages - Water networks efficiency reduction - Water pollution - Human health consequences - Negative economic impact
Vehicular Safety	- Reduced possibility of accidents - Reduced congestion - Reduced traffic violations	- Vehicular accidents - Human deaths and injuries - Road infrastructure damages - Traffic delays
Smart Manufacturing	- Optimized production and maintenance - Enhanced product quality - Customizable production processes - Enhanced safety	- Production efficiency reduction - Manufacturing equipment damages - Increase in resources consumption - Manufacturing safety reduction - Human deaths and injuries - Negative economic impact

CPS Applications	Major Objectives	Potential Security Risks
Self-Driving Vehicles	- Reduced transportation costs - Optimized traffic flow - Enhanced safety - Efficient ride sharing systems - Reduced congestion	- Vehicular accidents - Human deaths and injuries - Structure damages - Traffic delays
Intelligent Traffic Lights	- Reduced traffic delays - Minimized vehicles travel times - Increased vehicles average velocity	- Vehicular accidents - Human deaths and injuries - Road infrastructure damages - Traffic delays
Renewable Energy Production (Wind Farms, solar and Hydropower Plants)	- Maximized power generation - Improved ability to integrate with other systems such as smart grids - Better capabilities to balance energy production and consumption	- Renewable energy infrastructure damages - Reduction in energy production - Problems with other integrated systems
Energy Efficiency in Data Centers	- Reduced energy consumption - Maintained good health of the equipment - Reduced maintenance and operations costs	- Equipment damages - Reduction in energy consumption efficiency - Loss of data - Openings for unauthorized access
Greenhouse Efficient Controls	- Enhanced plants growth and produce quantity and quality - Optimized resources utilization	- Plants deaths - Reduction in produce quantity and quality - Increased unnecessary recourses consumption

The last factor to consider is one that many have not addressed or do not consider to be a security attack. This is whether the attack was intentional (pre-meditated) or non-intentional (accidental). The general trend is that any attack of any type and consequence is intentional. However, there are some possibilities of damages caused by an unintentional action or erroneous operations. For example, someone unintentionally forgetting to sign out of the system console, could lead to others exploiting the issue. Sometimes users may install or add something to a device that will later have some impact on the other software leading to damages. There is also the possibility of accidently copying or corrupting data or control signals leading to problems or damages. All these examples show that CPS forensics are also necessary to handle this type of issue. The main idea is that many damages assumed to be caused by a pre-meditated security attack could have simply happened by mistake. Therefore, forensics investigations should be carried out with the understanding of the possible discovery of an error or mistakes.

References

1. Lee, E.A. Cyber physical systems: Design challenges. In Proceedings of the 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, 5–7 May 2008.
2. Lee, J.; Bagheri, B.; Kao, H. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manuf. Lett. 2015, 3, 18–23.
3. Mohamed, N.; Al-Jaroodi, J.; Lazarova-Molnar, S. Leveraging the Capabilities of Industry 4.0 for Improving Energy Efficiency in Smart Factories. IEEE Access 2019, 7, 18008–18020.
4. Lee, I.; Sokolsky, O.; Chen, S.; Hatcliff, J.; Jee, E.; Kim, B.; King, A.; Mullen-Fortino, M.; Park, S.; Roederer, A.; et al. Challenges and research directions in medical cyber–physical systems. Proc. IEEE 2011, 100, 75–90.
5. Mohamed, N.; Al-Jaroodi, J. The Impact of Industry 4.0 on Healthcare System Engineering. In Proceedings of the 13th Annual IEEE International Systems Conference (SYSCON), Orlando, FL, USA, 8–11 April 2019; pp. 431–437.
6. Schmidt, M.; Åhlund, C. Smart buildings as Cyber-Physical Systems: Data-driven predictive control strategies for energy efficiency. Renew. Sustain. Energy Rev. 2018, 99, 742–756.
7. Lazarova-Molnar, S.; Shaker, H.R.; Mohamed, N. Reliability of Cyber Physical Systems with Focus on Building Management Systems. In Proceedings of the IEEE Int'l Performance Computing and Communications Conference (IPCCC), Las Vegas, NV, USA, 9–11 December 2016.
8. Deka, L.; Khan, S.M.; Chowdhury, M.; Ayres, N. Transportation cyber-physical system and its importance for future mobility. In Transportation Cyber-Physical Systems; Elsevier: Amsterdam, The Netherlands, 2018; pp. 1–20.
9. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010; pp. 731–736.
10. Karnouskos, S. Stuxnet worm impact on industrial cyber-physical system security. In Proceedings of the IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, Victoria, Australia, 7–10 November 2011; pp. 4490–4494.
11. Viganò, E.; Loi, M.; Yaghmaei, E. Cybersecurity of Critical Infrastructure. In The Ethics of Cybersecurity; Christen, M., Gordijn, B., Loi, M., Eds.; The International Library of Ethics, Law and Technology, Springer: Cham, Switzerland, 2020; Volume 21.
12. Al-Jaroodi, J.; Mohamed, N. PsCPS: A Distributed Platform for Cloud and Fog Integrated Smart Cyber-Physical Systems. IEEE Access 2018, 6, 41432–41449.
13. Nazarenko, A.A.; Camarinha-Matos, L.M. Towards collaborative cyber-physical systems. In Proceedings of the International Young Engineers Forum (YEF-ECE), Costa de Caparica (Lisbon), Portugal, 5 May 2017; pp. 12–17.
14. Khalid, A.; Kirisci, P.; Khan, Z.H.; Ghrairi, Z.; Thoben, K.D.; Pannek, J. Security framework for industrial collaborative robotic cyber-physical systems. Comput. Ind. 2018, 97, 132–145.
15. Al-Jaroodi, J.; Mohamed, N.; Jawhar, I. A service-oriented middleware framework for manufacturing industry 4.0. ACM SIGBED Rev. 2018, 15, 29–36.
16. Simmon, E.; Kim, K.S.; Subrahmanian, E.; Lee, R.; De Vaulx, F.; Murakami, Y.; Zettsu, K.; Sriram, R.D. A Vision of Cyber-Physical Cloud Computing for Smart Networked Systems; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2013.
17. Lyman, M.D. Criminal Investigation: The Art and the Science; Prentice Hall: Upper Saddle River, NJ, USA, 2001.
18. Bell, S. Crime and Circumstance: Investigating the History of Forensic Science; ABC-CLIO: Santa Barbara, CA, USA, 2008.
19. Catts, E.P.; Goff, M.L. Forensic entomology in criminal investigations. Annu. Rev. Entomol. 1992, 37, 253–272.
20. Allen, W.H. Computer forensics. IEEE Secur. Priv. 2005, 3, 59–62.
21. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet; Academic Press: Cambridge, MA, USA, 2011.
22. Handbook of Computer Crime Investigation: Forensic Tools and Technology; Casey, E. (Ed.) Elsevier: Amsterdam, The Netherlands, 2001.
23. Taylor, R.W.; Fritsch, E.J.; Liederbach, J. Digital Crime and Digital Terrorism; Prentice Hall Press: Upper Saddle River, NJ, USA, 2014.
24. Reith, M.; Carr, C.; Gunsch, G. An examination of digital forensic models. Int. J. Digit. Evid. 2002, 1, 1–12.

25. Wang, Y.; Lee, H.C. Research on some relevant problems in computer forensics. In Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 22–23 March 2013; Atlantis Press: Paris, France, 2013.
26. Andersson, V. Standards and Methodologies for Evaluating Digital Forensics Tools: Developing and Testing a New Methodology. Bachelor's Thesis, Halmstad University, Halmstad, Sweden, 2018.
27. Choi, K.-S.; Lee, C.S.; Louderback, E.R. Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime. In The Palgrave Handbook of International Cybercrime and Cyberdeviance; Springer Nature Switzerland AG: Cham, Switzerland, 2020; pp. 27–43.
28. Humayed, A.; Lin, J.; Li, F.; Luo, B. Cyber-physical systems security—A survey. IEEE Internet Things J. 2017, 4, 1802–1831.
29. Ashibani, Y.; Mahmoud, Q.H. Cyber physical systems security: Analysis, challenges and solutions. Comput. Secur. 2017, 68, 81–97.
30. Wang, E.Y.; Ye, Y.; Xu, X.; Yiu, S.M.; Hui, L.C.K.; Chow, K.P. Security issues and challenges for cyber physical system. In Proceedings of the IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing, Hangzhou, China, 18–20 December 2010; pp. 733–738.
31. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. Comput. Ind. 2018, 100, 212–223.
32. Neuman, C. Challenges in security for cyber-physical systems. In DHS Workshop on Future Directions in Cyber-Physical Systems Security; 2009; pp. 22–24. Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.152.973&rep=rep1&type=pdf (accessed on 7 July 2020).
33. Banerjee, A.; Venkatasubramanian, K.K.; Mukherjee, T.; Gupta, S.K.S. Ensuring safety, security, and sustainability of mission-critical cyber–physical systems. Proc. IEEE 2011, 100, 283–299.
34. Burg, A.; Chattopadhyay, A.; Lam, K.Y. Wireless communication and security issues for cyber-physical systems and the Internet-of-Things. Proc. IEEE 2017, 106, 38–60.
35. Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. In Workshop on Future Directions in Cyber-Physical Systems Security; 2009; Available online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.152.5198&rep=rep1&type=pdf (accessed on 7 July 2020).
36. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. Proc. IEEE 2011, 100, 210–224.
37. Sun, C.C.; Liu, C.C.; Xie, J. Cyber-physical system security of a power grid: State-of-the-art. Electronics 2016, 5, 40.
38. Huang, S.; Zhou, C.J.; Yang, S.H.; Qin, Y.Q. Cyber-physical system security for networked industrial processes. Int. J. Autom. Comput. 2015, 12, 567–578.
39. Wells, L.J.; Camelio, J.A.; Williams, C.B.; White, J. Cyber-physical security challenges in manufacturing systems. Manuf. Lett. 2014, 2, 74–77.
40. Wurm, J.; Jin, Y.; Liu, Y.; Hu, S.; Heffner, K.; Rahman, F.; Tehranipoor, M. Introduction to cyber-physical system security: A cross-layer perspective. IEEE Trans. Multi-Scale Comput. Syst. 2016, 3, 215–227.
41. DiMase, D.; Collier, Z.A.; Heffner, K.; Linkov, L. Systems engineering framework for cyber physical security and resilience. Environ. Syst. Decis. 2015, 35, 291–300.
42. Hahn, A.; Thomas, R.K.; Lozano, I.; Cardenas, A. A multi-layered and kill-chain based security analysis framework for cyber-physical systems. Int. J. Crit. Infrastruct. Prot. 2015, 11, 39–50.
43. Ruan, K.; Carthy, J.; Kechadi, T.; Crosbie, M. Cloud forensics. In IFIP International Conference on Digital Forensics; Springer: Heidelberg/Berlin, Germany, 2011; pp. 35–46.
44. Ruan, K.; Carthy, J.; Kechadi, T.; Baggili, I. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. Digit. Investig. 2013, 10, 34–43.
45. Dykstra, J.; Sherman, A.T. Understanding Issues in Cloud Forensics: Two Hypothetical Case Studies; ADFSL Conference on Digital Forensics, Security and Law: Richmond, VA, USA, 2011.
46. Alex, M.E.; Kishore, R. Forensics framework for cloud computing. Comput. Electr. Eng. 2017, 60, 193–205.
47. Huang, C.; Lu, R.; Choo, K.K.R. Vehicular fog computing: Architecture, use case, and security and forensic challenges. IEEE Commun. Mag. 2017, 55, 105–111.
48. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and privacy in fog computing: Challenges. IEEE Access 2017, 5, 19293–19304.

49. Esposito, C.; Castiglione, A.; Pop, F.; Choo, K.K.R. Challenges of connecting edge and cloud computing: A security and forensic perspective. IEEE Cloud Comput. 2017, 4, 13–17.
50. Mylonas, A.; Meletiadis, V.; Tsoumas, B.; Mitrou, L.; Gritzalis, D. Smartphone forensics: A proactive investigation scheme for evidence acquisition. In IFIP International Information Security Conference; Springer: Heidelberg/Berlin, Germany, 2012; pp. 249–260.
51. Mylonas, A.; Meletiadis, V.; Mitrou, L.; Gritzalis, D. Smartphone sensor data as digital evidence. Comput. Secur. 2013, 38, 51–75.
52. Grover, J. Android forensics: Automated data collection and reporting from a mobile device. Digit. Investig. 2013, 10, S12–S20.
53. Mahalik, H.; Tamma, R.; Bommisetty, S. Practical Mobile Forensics; Packt Publishing Ltd.: Birmingham, UK, 2016.
54. MacDermott, A.; Baker, T.; Shi, Q. Iot forensics: Challenges for the ioa era. In Proceedings of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.
55. Meffert, C.; Clark, D.; Baggili, I.; Breitinger, F. Forensic State Acquisition from Internet of Things (FSAIoT) A general framework and practical approach for IoT forensics through IoT device state acquisition. In Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, 29 August–2 September 2017; pp. 1–11.
56. Yaqoob, I.; Hashem, I.A.T.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Gener. Comput. Syst. 2019, 92, 265–275.
57. Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Gener. Comput. Syst. 2018, 78, 544–546.
58. Ahmed, I.; Obermeier, S.; Naedele, M.; Richard, G.G., III. Scada systems: Challenges for forensic investigators. Computer 2012, 45, 44–51.
59. Elhoseny, M.; Hosny, A.; Hassanien, A.E.; Muhammad, K.; Sangaiah, A.K. Secure automated forensic investigation for sustainable critical infrastructures compliant with green computing requirements. IEEE Trans. Sustain. Comput. 2017, 5, 174–191.
60. Hilal, H.; Nangim, A. Network security analysis SCADA system automation on industrial process. In Proceedings of the 2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP), Jakarta, Indonesia, 21–23 November 2017; pp. 1–6.
61. Sohl, E.; Fielding, C.; Hanlon, T.; Rrushi, J.; Farhangi, H.; Howey, C.; Carmichael, K.; Dabell, J. A field study of digital forensics of intrusions in the electrical power grid. In Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, Denver, CO, USA, 12 October 2015; pp. 113–122.
62. Do, Q.; Martini, B.; Choo, K.K.R. Cyber-physical systems information gathering: A smart home case study. Comput. Netw. 2018, 138, 1–12.
63. Baig, Z.A.; Szewczyk, P.; Valli, C.; Rabadia, P.; Hannay, P.; Chernyshev, M.; Johnstone, M.; Kerai, P.; Ibrahim, A.; Sansurooah, K.; et al. Future challenges for smart cities: Cyber-security and digital forensics. Digit. Investig. 2017, 22, 3–13.
64. Cebe, M.; Erdin, E.; Akkaya, K.; Aksu, H.; Uluagac, S. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Commun. Mag. 2018, 56, 50–57.
65. Al Faruque, M.A.; Chhetri, S.R.; Canedo, A.; Wan, J. Forensics of Thermal Side-Channel in Additive Manufacturing Systems; University of California: Irvine, CA, USA, 2016.
66. North America Electric Reliability Corp, Defense Use Case. Analysis of the Cyber Attack on the Ukrainian Power Grid; SANS Ind. Control Syst.: Wachington, DC, USA, 2016; Tech. Rep.
67. Bronk, C.; Tikk-Ringas, E. The Cyber Attack on Saudi Aramco. Survival 2013, 55, 81–96.
68. Lindsay, J.R. Stuxnet and the Limits of Cyber Warfare. Secur. Stud. 2013, 22, 365–404.
69. Al-Mhiqani, M.N.; Ahmad, R.; Yassin, W.; Hassan, A.; Abidin, Z.Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-security incidents: A review cases in cyber-physical systems. Int. J. Adv. Comput. Sci. Appl. 2018, 9, 499–508.
70. Orojloo, H.; Azgomi, M.A. A method for evaluating the consequence propagation of security attacks in cyber–physical systems. Future Gener. Comput. Syst. 2017, 67, 57–71.
71. AlTawy, R.; Youssef, A.M. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. IEEE Access 2016, 4, 959–979.

72. Plumer, B. It’s Way too Easy to Cause a Massive Blackout in the US. in Vox. Available online: https://www.vox.com/2014/4/14/5604992/us-power-grid-vulnerability (accessed on 30 June 2020).