VOL. 12, NO. 22, NOVEMBER 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

INVESTIGATION STUDY OF CYBER-PHYSICAL SYSTEMS: CHARACTERISTICS, APPLICATION DOMAINS, AND SECURITY CHALLENGES

Mohammed Nasser Al-Mhiqani[1], Rabiah Ahmad[1], Karrar Hameed Abdulkareem[2] and Nabeel Salih Ali[3]
[1]Centre for Advanced Computing Technology, Faculty of Information and Communication Technology, University Technical Malaysia Melaka, Melaka, Malaysia
[2]Agriculture College, University of Al-Muthana, Iraq
[3]Information Technology Research and Development Centre, University of Kufa, Iraq
E-Mail: Almohaiqny@gmail.com

ABSTRACT

Cyber-Physical Systems (CPSs) are currently widely used in people's daily lives but present risks and threats, especially when used by cybercriminals against the governments, corporations, organizations, or individuals. CPS applications are increasingly becoming attractive and are targeted by cyber-attacks. Tools and theories that can be used by organizations and researchers to understand the types of new threats and the impacts that each threat can cause to the physical systems are lacking at present. In this research, current physical security threats of CPSs for the last few years are investigated to briefly describe the usage, application domains, and security challenges of CPSs in their field of application. This work serves a basis for further studies on cyber physical security.

Keywords: cyber-physical systems, physical security attacks, cyber attacks, CPS application domains, security threats, CPS security challenges.

INTRODUCTION

Cyber-Physical Systems (CPSs) enable interaction between computers and the real world and are widely used in people's daily lives. The majority of modern computing devices are ubiquitous embedded systems and are used to manage physical processes and monitor, such as airplane, car, air traffic management, and automotive highway systems (EzioBartocci, Oliver Hoeftberger, 2014). Research on embedded systems has shifted the focus from the optimization problem design of these computational components to the complex cooperation between the physical environments and the computational elements with which they communicate. The term CPS was coined to refer to interactions. In CPS, communication devices and embedded computation, together with actuators and sensors of the physical substratum, are combined in the heterogeneous, open, and system of system (EzioBartocci, Oliver Hoeftberger, 2014). Activists, terrorists, or criminals are always looking for new and innovative techniques and targets to accomplish their goals; CPSs are mostly targeted by attackers because of the high impacts of these systems (Applegate, 2013). Security against such attacks must be well organized, quick, and effectively communicated (Ali, N.S, 2016). Malwares, new physical security attacks, and other security challenges may threaten and derail new strategies from the government (Dan Lohrmann, 2012). In this study, the concept of CPSs and the role they play in easing peoples' daily lives are discussed. The most important CPS domains at present are also presented. In addition, current security challenges of CPSs are highlighted. This study serves as a reference for further studies on cyber physical security and mechanisms for preventing, detecting, and recovering from attacks.

PREVIOUS WORKS

Many authors have surveyed, reviewed, and investigated CPSs and their directions. Their studies focus on various aspects of CPSs, such as challenges, attacks, threats, security issues, security challenges, domains, Medical CPSs (MCPSs), present works, and characteristics. Wang *et al*. (2010) discussed the challenges of CPSs in general. They abstracted and modelled the general workflow of CPS into four main steps: monitoring, networking, computing, and actuation. Attacks were also categorized into four types: eavesdropping, compromised-key attack, man-in-the-middle attack, and denial-of-service attack. Ly *et al*. (2016) discussed three challenges of CPSs, namely, security, correctness, and resource constraints. A case study on power grids was also conducted to determine the impact of problems and provide possible solutions. Liu *et al.* (2017) first introduced the concept and characteristics of CPSs and analysed the present situation of CPS studies. The development of CPSs was discussed from many perspectives of system model, such as information processing technology and software design. The main obstacles and key works in developing CPSs were analysed, and minimal CPS challenges were presented, such as pattern abstraction, scale and efficiency, and robustness. Reddy (2015) discussed security requirements in the future engineering systems and reviewed some of CPS challenges in design, such as reliability, safety, security, Quality of Service (QoS), and software engineering processes. Wan (2010) analysed and described the limitations of the current tools and methods by illustrating a motivating example of healthcare systems and proposed a unified framework for designing, simulating, and verifying.

Table-1. Previous studies on cpss and their trends**.**

Author	Year	Cyber-physical systems			
		Challenges	Security	Domains	Characteristics and concepts
Rawung	2007	×	×	✓	×
Pal *et al.*	2009	✓	×	×	×
Wan	2010	✓	×	×	×
Wang *et al.*	2010	✓	✓	×	×
Raj	2010	✓	×	×	×
Hatcliff *et al.*	2011	✓	×	×	×
Shi	2011	×	×	✓	×
Shafi *et al.*	2012	×	✓	×	×
Kim and Kumar	2012	×	×	✓	×
Mosterman and Zander	2015	✓	×	×	×
Reddy	2015	✓	✓	×	×
Mangharam *et al.*	2016	✓	×	×	×
Ly *et al.*	2016	✓	×	×	×
Liu *et al.*	2017	✓	×	×	✓

They also identified the needs and challenges for designing and operating CPSs along with corresponding technologies to address the challenges and their potential impact (challenges when embedded software systems are collaborated). Hatcliff *et al*. (2011) analysed the challenges of MCPSs, which are life critical context-aware, networked systems of medical devices. These systems are increasingly used in hospitals to provide high-quality continuous care for patients. The need to design complex MCPSs that are safe and effective has presented numerous challenges, including achieving high assurance in system software, inoperability, context-aware intelligence autonomy, security and privacy, and device verifiability. The said authors also discussed these challenges in developing MCPSs, some works that address these systems, and several open research issues. Pal *et al.* (2009) explored CPS security issues, such as data interpretation, information and control sharing, containing compromises, maintaining timeliness, and validation. Meanwhile, Shi (2011), Kim and Kumar (2012), and Rawung (2007) conducted studies that focused on CPS domains, such as healthcare and medicine, electric power grid, network sensors in CPS, energy, transportation, and integrated intelligent road with an unmanned vehicle. Shafi *et al*. (2012) bibliographically reviewed existing literature on CPS security, identified key research challenges, and discussed future directions on open research issues. Raj (2010) described the design, construction, and verification of CPSs that pose a multitude of technical challenges that must be addressed by a cross-disciplinary community of researchers and educators. Challenges, such as robustness, safety, and security of CPS; control and hybrid systems; computational, architectural, and real-time embedded system abstractions; sensor and mobile networks; model-based development of CPS; verification, validation, and certification of CPS; and education and training were specifically explored in the case of an electric power transmission grid. All previous works have focused only on either application domains (e.g., transportation, healthcare, and energy) or challenges (e.g., design and security issues) of CPSs. Only a few application domains and challenges have been discussed; thus, further details on other domains and challenges are lacking and must be provided. The current study simultaneously examines two main areas in CPS, namely, application domains and security challenges. The characteristics of CPSs are also comprehensively discussed.

CHARACTERISTICS AND ADVANTAGES OF CPSs

Characteristics of CPSs

CPS characteristics have been identified, but their properties have not been defined. Some of the main characteristics are discussed below with their own bodies of literature and design communities (Helps and Mensah, 2012).

A. Separated development and targeted systems

This CPS characteristic leads to design issues, specifically "limited controllability and observability" (Wolf, 2012).

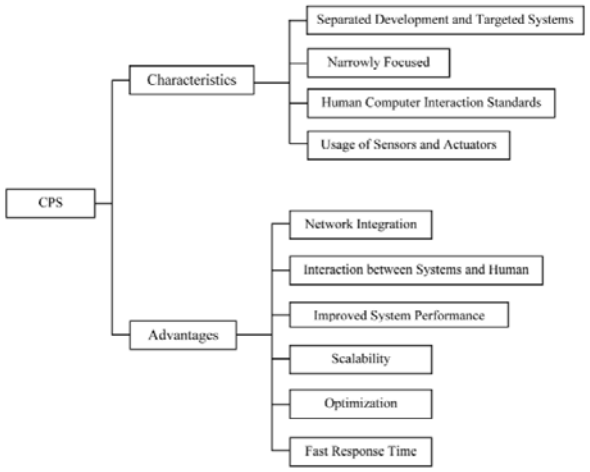

Figure-1. Characteristics and advantages of CPSs.

B. Narrowly focused

Embedded systems are not intended for general purposes. Smartphones, cellular multi-processing-enabled devices, and modern tablets are stretching the limitation with the use of thousands of "apps"; many other CPS characteristics are shared by these systems (Helps and Mensah, 2012).

C. Human and computer interaction standards

Human and computer interaction standards and guidelines are well defined and available for conventional computer systems, but custom designs are required by most CPSs (Nabeel Salih Ali, Mohammed Nasser, 2017).

D. Usage of sensors and actuators

This characteristic is common to CPSs but uncommon to conventional systems. Microcontrollers usually use actuators and sensors as the essential or sole user and world interfaces.

Advantages of CPSs

CPS is a promising integrated solution for the physical and cyber world due to its several benefits as follows:

A. Network integration

CPSs can be interoperated with wireless sensor networks (WSNs) and cloud computing to satisfy network standards. CPSs involve multiple computational platforms when interacting over communication networks. Network integration characteristics provided by CPS, such as media access control techniques and their effectiveness on system dynamics, middleware, and software, provide coordination on the network control over network transaction timing and fault tolerances (Haque *et al*., 2014).

B. Interaction between systems and human

Measuring and modelling situational awareness and human perception for systems and their changes of environments in their parameters are essential for decision making especially for dynamic and complex systems. Some CPSs involve humans as an important part of the systems, thereby resulting in ease of interaction as humans are difficult to model using a standalone system (Mehedi Hassan *et al*., 2014).

C. Improved system performance

CPSs can obtain improved performance in terms of automatic redesign and feedback because of a close interaction between cyber infrastructure and sensors. Cyber subsystems and computational resources in CPSs ensure multiple mechanisms of communication, multiple sensing entities, high-level program languages, and end-user maintenance; thus, the system performance is guaranteed (Haque *et al*., 2014).

D. Scalability

CPSs can be scaled according to the demand by utilizing cloud computing properties. Users can obtain the necessary infrastructure without investigating the additional resources. CPSs are inherently heterogeneous as they can combine computational processes with physical dynamics. The physical domains can combine mechanical–chemical processes, motion control, human involvement, and biological processes. The cyber domains can combine programming tools, software modeling, and networking infrastructure (Mehedi Hassan *et al.,* 2014).

E. Optimization

The use of biomedical sensors and cloud infrastructures can enable large optimizations for various applications (Haque *et al*., 2014). This capability enables optimizing CPSs in a wide extent.

F. Fast response time

CPSs can achieve fast response time due to their fast processing and the communication between sensors and cloud infrastructures; fast response time facilitates early detection of remote failures and proper utilization of shared resources (e.g., bandwidth) (Haque *et al.,* 2014).

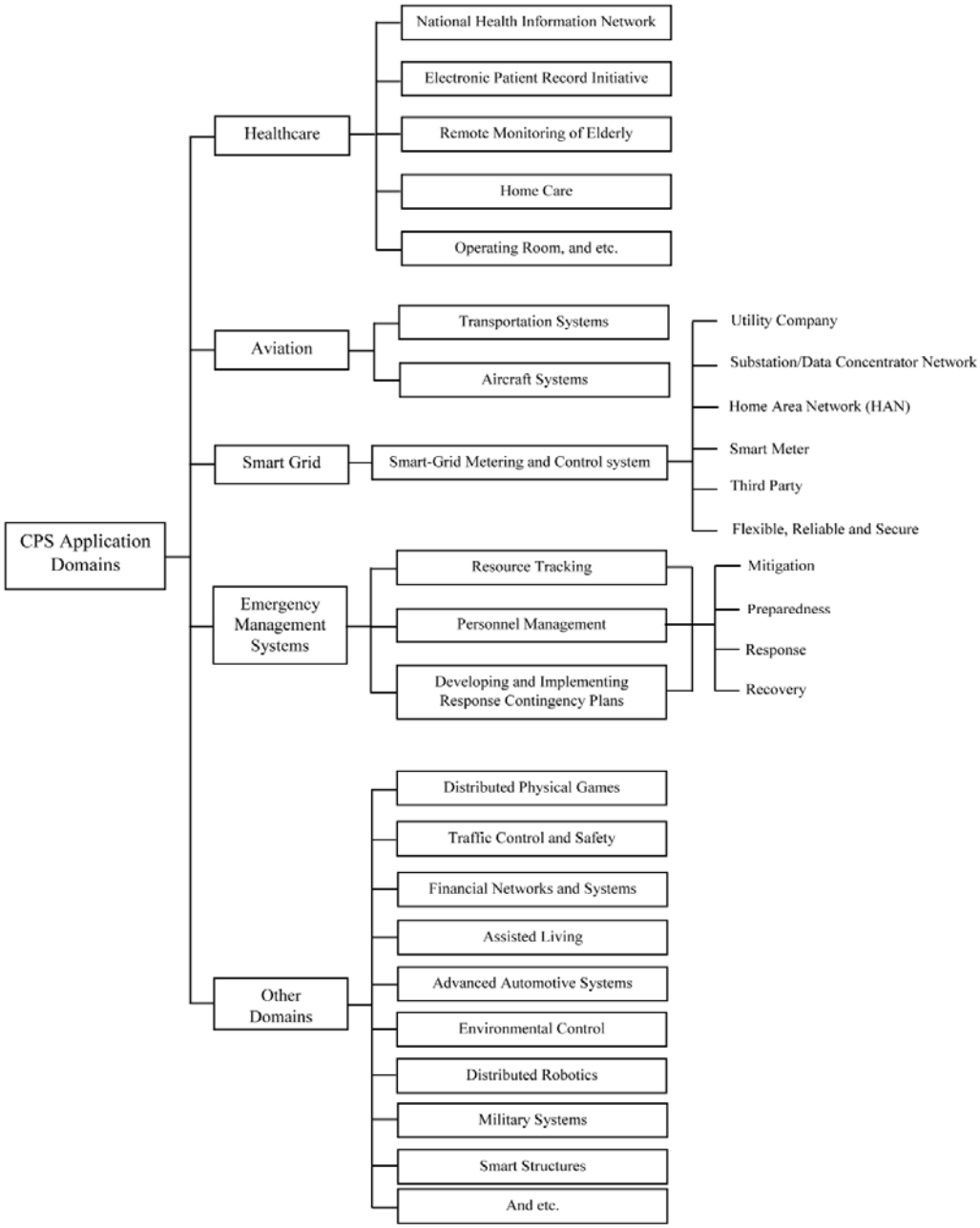

Figure-2. Application domains of CPSs and their characteristics.

APPLICATION DOMAINS OF CPSs

A. Healthcare

Healthcare and medicine domain includes information network of national health, electronic patient record initiative, remote monitoring of elderly (body area networks), operating room, and homecare; some of which are increasingly controlled by computer systems with software and hardware components, and they are real-time systems with timing and safety requirements (Shi *et al.*, 2011). The use of new advances, such as cloud computing and WSNs, in medical sensors are powerful applications of CPSs in healthcare, including homecare and in-hospital care for patients. These advances provide CPSs with capabilities to remotely observe the condition of patients and can help in taking right measures regardless of the location of patients (Haque and Aziz, 2013). Access to the above-mentioned devices and corresponding data is highly demanded by patients, payers, employees, and providers and is a potential risk and security target.

B. Aviation

Aviation industries are renowned for their safety record. Aviation is the safest transportation mode in the

world and is a safe, highly efficient, and resilient system; however, people will not fly aboard this transport if the risk is high (Aviation, 2013).

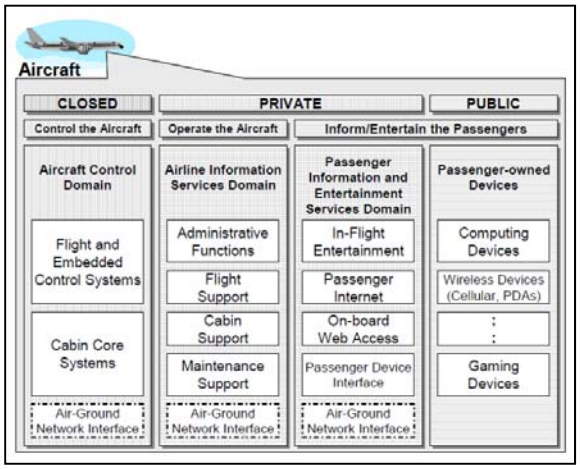

Figure-3. CPS usage in aviation (Muller *et al*., 2012).

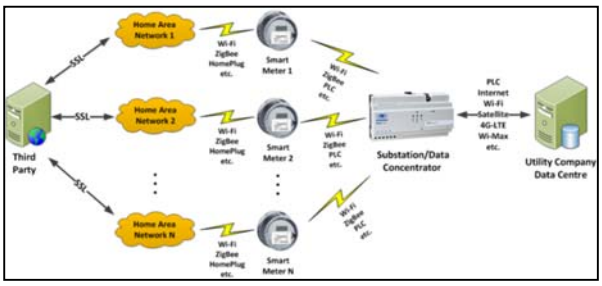

Figure-4. CPS usage in smart grid (Fan *et al*., 2013).

ARINC 811 "Commercial Aircraft Information Security Concepts of Operation and Process Framework" has defined new aircraft systems (Cerchio *et al*., 2011) and divided them into airline information systems, control domain of the aircraft, and the systems of passenger's info/entertainments. These aircraft systems possess internal and external (direct or indirect) connections and crews/passengers-owned devices (e.g., SatComm links, Internet, and Gatelink) that may introduce vulnerability.

C. Smart grid

Study proposed by (Fan *et al*., 2013) shown the purpose of each part of a smart-grid metering with the following control systems.

a) Utility Company: this part connects to the substation through the WAN interface in the communication channel, such as Wi-Fi, satellite, 4G-LTE, and Wi-Max. This part functions to process alarms and alerts, manage the meter data, and generate bills offered by the company. A web portal that allows customers to view their monthly energy consumption and bills should be provided by the utility company (Fan *et al*., 2013).

b) Data-Concentrator Network or Substation: this part is composed mainly of a set of smart meters in specific area and a data collector. The connection between the data collector and smart meter is achieved through Wi-Fi, ZigBee, and power line carrier. The process is conducted by creating a wireless mesh network and forwarding the meter readings through multi-hop communications. The accumulated data received by the collector are then transmitted to the utility company (Fan *et al*., 2013).

c) Home Area Network (HAN): consumers can control and monitor their real-time power consumption through access points provided by use of HAN. This part consists of a home gateway to enable receiving power consumption data stored in the smart meter and displaying them on the household consumers' devices, such as laptop, tablet, and smartphone. The home gateway can send power consumption data to a third party for other services, such as efficiency advice and supplier selection. HAN also comprises a controller that enables consumers to control and monitor the status of their home appliance remotely.

d) Smart Meters: these components are composed of the microcontrollers, a communication board, and a metrology board with their respective functions. The microcontroller controls the meter, the metrology board measures the real-time power consumption, and the substation network and HAN transmit the meter data through the communication board. Wi-Fi, ZigBee, Ethernet, Home Plug, and Wireless M-Bus are used to achieve the connection between the smart meter and home appliances. The smart meter also includes a disconnection function (if enabled) that can allow companies or customers to connect or disconnect home appliances and services remotely.

e) Third Party: this part solely depends on precise meter reading in offering additional valuable services (e.g., supplier selection and efficiency power advice) to household consumers; when these services are provided, the household consumers can check their power usage in cost-effective and regular ways (Fan *et al*., 2013). The said components enable smart grid to be incorporated and interacted to other grids, such as electric grid. With these components, the smart grid is thus smart in identifying surges, line outages, and failure points; resilient in providing information regarding damages and power rerouting around failures; reliable in achieving dynamic load balancing; flexible in accommodating new off-grid alternative

energy sources; and secure in being less vulnerable to malicious harms or accidents (Nabil Adam, 2010).

D. Emergency management systems

Emergency planners are currently becoming the first responders and relief workers. These systems highly depend on the computational and communication systems, which include the whole aspects of the emergency management (EM) preparedness and mitigation to recovery and response (Loukas *et al.,* 2013). EM highly relies on the computational and communication systems in their coordinating, information gathering, communicating, training, and planning tasks. For example, WSNs can achieve early detection of emergency events, individual buildings, or vast geographical areas, thereby improving situational awareness during rescue and search operations. Autonomous systems (e.g., autonomous vehicles) are mostly used for EM.

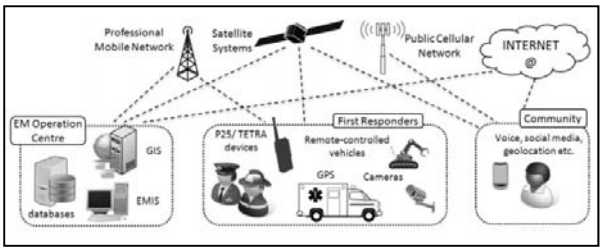

Figure-5. CPS usage in EM (Loukas *et al.*, 2013).

EM information systems (EMIS) offer EM with Internet-based services, such as tracking of resources, management of personnel, development and implementation of response contingency procedures. The primary contribution of EMISs to EM is the quantification of the true cost of emergencies. Another service provided is the development of a uniform community where valuable information of EM personnel that can be implemented in future EM mitigation activities is provided by remotely connected sensors (Walker, 2012).
EM systems (EMSs) are divided into the following phases.

a) Mitigation

Mitigations refer to actions that are taken to minimize the occurrence probability of emergency cases and to reduce their impacts. Geographical information systems (GISs) are mostly used to recognize high risks of geographical areas that must be prioritized during emergency. Disaster databases are used to develop informing policies and emergency planning activities (Loukas *et al*., 2013).

b) Preparedness

Preparedness is defined as the developments of protocols and policies, planning, coordination, training, and public awareness that should be considered to minimize emergency potential. Computer software can be used for analysis and training, and relevant disaster resource databases and GISs can be used for identification, such as ascertaining evacuation routes and shelters (Loukas *et al*., 2013).

c) Response

Response actions mainly aim to properly handle and resolve an emergency after its occurrence. They mostly include the mobilization of many emergency services, such as the police, fire fighters, specialist rescue teams, ambulances, and volunteers. The success of operations depends on EM plans and processes that have been defined during the mitigation phase and rehearsed during the preparedness phase. A set of technologies is used when an emergency case occurs. The Internet and social networks are used to report damage and casualties. Space technologies are used to communicate with volunteers, conduct asset tracking, and establish communications in areas where terrestrial systems fail to perform. A professional mobile radio is used for communications among EM practitioners. Sophisticated vehicles and devices are also used for tracking or communicating to transport the affected people.

d) Recovery

Recovery is referred to as the helping process for the affected community and the process of restoring the infrastructure. This task mostly depends on the current EM organizational processes and systems. GISs and geospatial data can be used for planning and monitoring. Recovery may also include disaster medication, which relies on interconnected infrastructures in gathering health information and providing early warning to the public and the authorities. Healthcare solely relies on computerized equipment, which is exposed to cyber threats and can be disabled easily by the malware "borne." Such incident occurred in the heart monitors and MRI machines in Sweden in 2009. Harries and Yellowlees (2013) and Loukas *et al*. (2013) demonstrated that cyber-terrorism risks targeting healthcare systems in the United States are increasing, and they proposed best practices that can be adopted by healthcare organizations.

e) Other application domains

CPSs are also applied in several other areas, such as safety and traffic control, distributed physical games, systems and financial networks, advanced automotive systems, assisted living, distributed robotics, environmental control, smart structures, and military systems. CPS applications are promising for the national competitiveness of global economies. These systems not only revitalize traditional industry sectors but also create new industries. CPS advances exert a profound social impact on several areas from blackout-free generation of electricity and distribution to CPSs self-correcting for "one-off" applications (Raj *et al*., 2010).

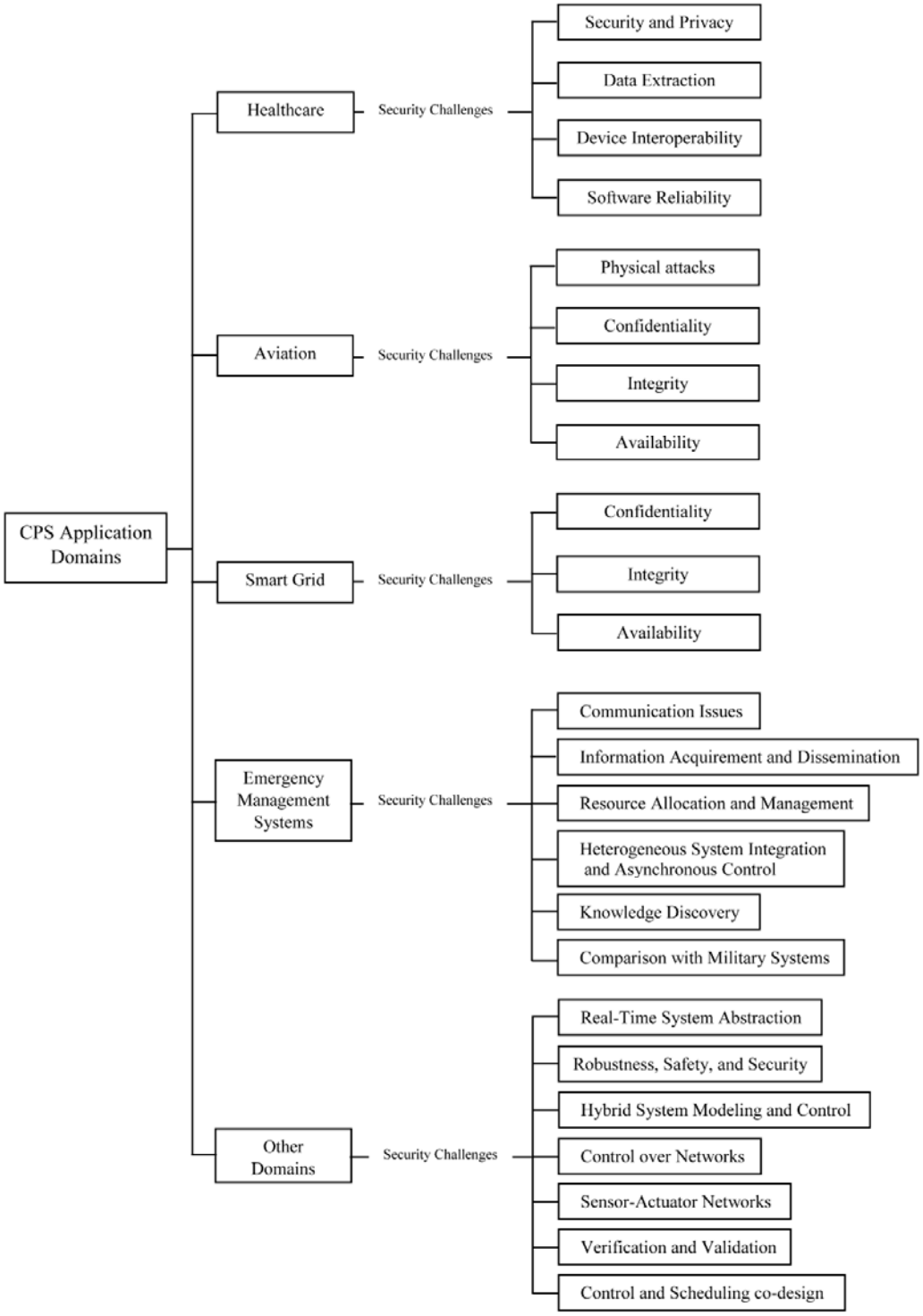

Figure-6. Security challenges of CPS application domains.

SECURITY CHALLENGES OF CPSs

A. Healthcare

As shown in Figure-7, designing CPSs for healthcare is a very challenging task because it involves many problems, such as system interoperability, software reliability, security and privacy, context awareness, and computational intelligence. Privacy and security are indeed critical tasks to ensure privacy of collected patient data. Unlawful use of patient data may cause loss of personal privacy and damage in reputation. Mental unrest can also occur, thereby leading to physical illness or even

death of patients. This incident occurred in Italy; in particular, a "mob boss, who was shot but survived the shooting, while he was in the hospital, the assassins hacked into the hospital computer and changed his medication so that he would be given a lethal injection. He was a dead man a few hours later" (Haque *et al.*, 2014).

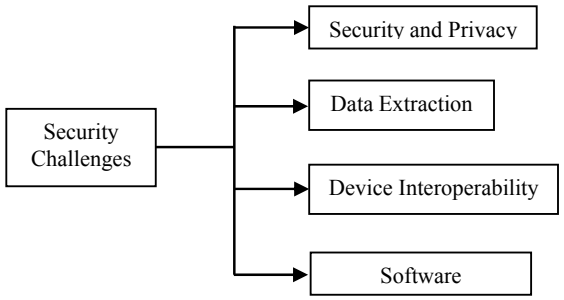

Figure-7. CPS security challenges in healthcare.

B. Aviation

Physical attacks are leading threats encountered in aviation. However, common threats (e.g., hacking), during which any risk exposes aviation facilities and operations, have been diminished in the recent decades. Technologies applied in transportation system infrastructures of aviation are unsafe from cyber-attacks. Networks enhancing critical information of airport assets are also exposed to virtual and physical threats. Cyber threats have increased in the 21st century and have thus increased the need to assure integrity, confidentiality, and availability of system information with the increase in the number of passengers globally (Iasiello, 2013). Breaking in an air traffic control system and messing up with the system can make airplanes crash and result in massive death or prevent the plane from landing. Existing models and approaches for analysing safety and security in aerospace significantly differ. According to Nabil Adam (2010), common safety approaches are used in the development, design, and certification of aircraft. Avionics software is perceptible and probabilistic, and continuous and dynamic controls are separately considered. Furthermore, common security analysis in the cyber world depends solely on discrete domains. Meanwhile, security risks are not being properly fixed, and their effects change with time. An example discovering of the exploit can expose the integrity of distributed aircraft software to risk (Sampigethaya and Bushnell, 2009). Newly developed technologies and narrow experience of IT personnel increase the potential security matters, which are uncommon in the civil aviation industry (CPNI, 2012). Current IT systems are increasingly becoming embedded, interconnected, and interdependent; hence, organizations are threatened by risks produced by the weakness of other systems (CPNI, 2012).

C. Smart grid

According to scientific and technological viewpoints, future control system should be well designed, constructed, worked, and regularly maintained to avoid human error, natural disaster, or international Internet threats without loss of important functions. This task is difficult for energy/electric sectors, which are complex and highly interconnected with a set of access points (Nabil Adam, 2010). Any noise or disturbance to an electric sector produces consequential effects to other sectors. Internet security, human interaction, and network complexity should be investigated to identify threats and thus make the systems flexible and functional. Mixed initiative control, data fusion, and control system of hierarchical design must also be explored. Considering that smart grid is recently developed, privacy risks can be properly determined by use of a combination of sound technology choices and laws (Mulligan *et al.*, 2011). Smart grid players must consider privacy when choosing technologies to avoid costly retrofits and replacements of equipment and services. Figure 8 shows current private risks that should be given attention.

D. Emergency management systems

a) Communication Issues: many-to-many data connection and opportunistic flow are unavoidable in EMSs. For example, search safe methods during fire emergency may need to send sensing information from several sensors to several evacuees remotely. This task may be difficult because communications may break down and evacuees may move to escape. Communications of query-and-reply may also occur between totally different groups of people, such as evacuees, first responders, members of the robots and press. General communication protocols, such as broadcast, unicast, converge cast, and multicast, cannot deal with these various requirements of communication (Gelenbe and Wu, 2013).

b) Information Dissemination and Acquirement: cross-domain sensing and heterogeneous information flow are inherent features in EMSs. To guarantee the safety of people, information in different domains must be acquired (e.g., ultrasonic sensors for localizing people, temperature and gas sensors for identifying hazards, camera sensors for counting civilians, and life detectors for searching civilians). Sensors are no longer the only information contributors as in situ interactions among sensors, actuators, people, objects, and events can also be involved in disseminating and contributing high-level information. These features can cause difficulty in efficiently acquiring and disseminating information (Gelenbe and Wu, 2013).

c) Knowledge Discovery: dynamic changes and partial information are also inherent in EMSs. In a rough environment, possible and fast responses rely on data analysis technologies in extracting knowledge from data sensing (e.g., discovery, counting, civilians

tracking, and localization). Forecast of environmental changes and dynamic prediction must be conducted to avoid unnecessary casualties.

d) Resource Management and Allocation: limited resources cause difficulty in timely responses. Contrary to alternative sensor-aided applications, intelligent actuation, efficient resource allocation, and scheduling are required in EMSs. Intelligent scheduling is required to choose the best action and to efficiently allocate scarce resources (Gelenbe and Wu, 2013).

e) Heterogeneous System Asynchronous Control and Integration: multi-domain technologies are required to enhance the potential of EMSs. Separated functionality tasks, such as storage, sensing, computation, and decision making, are required to be managed by a functional independent unit to facilitate multiple technologies integrating asynchronous control.

f) Comparison with Military Systems: rescue and search systems mainly aim to achieve quick responses during emergency. On the contrary, military systems focus on extensive simulations for decision and tactical planning. Rescue and search systems are composed of heterogeneous nodes, whereas military systems are subsystems of mission-oriented collection with capabilities and resources that exhibit more complex functionalities than the constituent systems (Gelenbe and Wu, 2013).

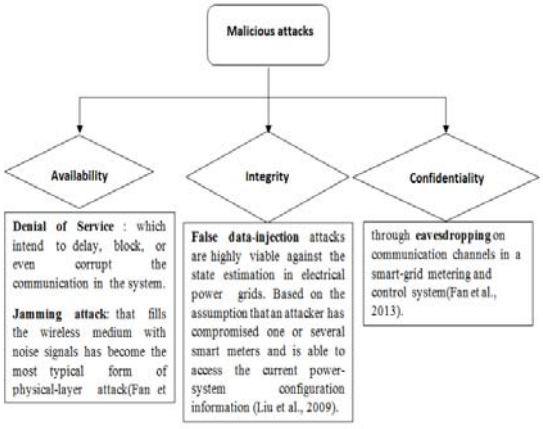

Figure-8. Types of malicious attacks and their risks and threats.

E. Other security challenges

A few general CPS research challenges are discussed as follows.

a) Real-Time System Abstraction: given the massive amount of actuators and sensors and computer-based information exchange of various information classes, new frameworks that allow abstracting salient system options in real time should be developed (Park *et al*., 2012). For example, network topologies for CPSs may be dynamically modified according to the physical environment.

b) Robustness, Security, and Safety: unlike logical computations in cyber systems, interactions with the physical world inevitably exhibit particular levels of uncertainty because of issues, such as environmental randomness, errors on physical devices, and possibility of security threats (Park *et al.,* 2012).

c) Hybrid System Control and Modeling: cyber and physical systems differ in that the former evolves continuously in real time whereas the latter changes consistently with discreet logic. Hybrid systems and control techniques, which include cyber and physical elements, should be developed for CPSs (Park *et al.,* 2012).

d) Control over Networks: the implementation and design of CPS network control pose many issues, such as time- and event-driven computations, transmission failures, time-varying delays, and system reconfigurations.

e) Sensor–Actuator Networks: WSNs have been extensively studied in the last decade. On the contrary, wireless sensor–actuator networks have been rarely explored, especially from the CPS perspective (Park *et al.,* 2012).

f) Validation and Verification: hardware and software, OS, and middleware components must undergo complete testing and integrative verification to ensure that the overall requirements of CPS are satisfied (Park *et al*., 2012).

g) Scheduling Co-Design and Control: scheduling and control co-design is a well-studied field in embedded systems and real-time communities. Various aspects of co-design have been reconsidered with the emergence of CPSs.

CONCLUSIONS

CPSs are currently widely used in several public and industry services. Failure of CPSs can cause significant damage on the global economy and vital business missions. The reason is that system operation in the real world can affect the physical safety or even lead to

the loss of life. In this research, the security threats, challenges, advantages, features, and application areas of CPSs are discussed. Similar studies have been conducted in the past; however, tools and theories that can be used by organizations and researchers to understand the types of new threats, security challenges, and the impacts that each threat can cause to the physical systems are lacking. In the future, CPS mechanisms for preventing, detecting, and recovering from attacks will be examined. In particular, tools that can be used to prevent hackers from gaining access to these systems will be explored. Recovery systems will also be improved to reduce the impact of attacks, especially those in oil industries or other utility services.

REFERENCES

Ali N.S. 2016. A four-phase methodology for protecting web applications using an effective Real-time technique. Int. J. Internet Technology and Secured Transactions. 6(4): 303-323.

Applegate S.D. 2013. The Dawn of Kinetic Cyber. Cyber Conflict (CyCon), 2013 5th International Conference. 2013 NATO CCD COE, Tallinn.

AVIATION A. 2013. The Connectivity Challenge: Protecting Critical Assets in a Networked World. The American Institute of Aeronautics and Astronauts (AIAA) Aviation. 2013 Los Angeles, CA.

Bartocci E., Hoeftberger O. & Grosu R. 2014. Cyber-Physical Systems: theoretical and Practical Challenges. ERCIM News. 2014(97).

Cerchio R. De, Administration F.A. and Riley C. 2011. Aircraft Systems Cyber Security. IEEE 30th Digital Avionics Systems Conference (DASC). 2011 Seattle. pp. 1-7.

Dan Lohrmann 2012. 2012 NASCIO recognition award nomination Integrating Cyber and Physical Security: Ending the Divide Using a Comprehensive Approach to Risk Nomination Category: Michigan.

Ezio Bartocci Oliver Hoeftberger R.G. 2014. Cyber-Physical Systems. (97).

Fan X., Gong G. and Locke G. 2013. Security Challenges in Smart-Grid Metering and Control Systems. Technology Innovation Management Review, 3(July): 42-49. Available at: http://timreview.ca/article/702.

Gelenbe E. and Wu F.-J. 2013. Future Research on Cyber-Physical Emergency Management Systems. Future Internet, 5(3): 336-354. Available at: http://www.mdpi.com/1999-5903/5/3/336/ [Accessed: 11 October 2014].

Haque, S.A. and Aziz, S.M., 2013. False Alarm Detection in Cyber-physical Systems for Healthcare Applications. AASRI Procedia, 5, pp. 54-61. Available at: http://linkinghub.elsevier.com/retrieve/pii/S2212671613000590 [Accessed: 11 December 2014].

Haque S.A., Aziz S.M. and Rahman M. 2014. Review of Cyber-Physical System in Healthcare. International Journal of Distributed Sensor Networks, pp. 1-20. Available at: http://www.hindawi.com/journals/ijdsn/2014/217415/.

Harries D. & Yellowlees P. M. 2013. Cyberterrorism: Is the US healthcare system safe?. Telemedicine and e-Health. 19(1): 61-66.

Helps R. and Mensah F.N. 2012. Comprehensive design of cyber physical systems. Proceedings of the 13th annual conference on Information technology education - SIGITE '12, p. 233. Available at: http://dl.acm.org/citation.cfm?doid=2380552.2380618.

Iasiello E. 2013. Getting ahead of the threat : and cyber. aerospace America, (August), pp. 22-25. Available at: http://tinyurl.com/qhjxaq4.

Kim K. D. & Kumar P. R. 2012. Cyber–physical systems: A perspective at the centennial. Proceedings of the IEEE. 100(Special Centennial Issue): 1287-1308.

Lee I., Sokolsky O., Chen S., Hatcliff J., Jee E., Kim, B. ...& Venkatasubramanian K. K. 2012. Challenges and research directions in medical cyber-physical systems. Proceedings of the IEEE. 100(1): 75-90.

Loukas G., Gan D. and Vuong T. 2013a. A Review of Cyber Threats and Defence Approaches in Emergency Management. Future Internet. 5(2): 205-236. Available at: http://www.mdpi.com/1999-5903/5/2/205/ [Accessed: 22 December 2014].

Loukas G., Gan D. and Vuong T. 2013b. A taxonomy of cyber-attack and defence mechanisms for emergency management networks. Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference. 2013 IEEE, San Diego, CA. pp. 534-539.

Liu Y., Peng Y., Wang B., Yao S. & Liu Z. 2017. Review on cyber-physical systems. IEEE/CAA Journal of Automatica Sinica. 4(1): 27-40.

Ly K., Sun W. & Jin Y. 2016, April. Emerging challenges in cyber-physical systems: A balance of performance, correctness, and security. In Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on (pp. 498-502). IEEE.

Mangharam R., Abbas H., Behl M., Jang K., Pajic M. & Jiang Z. 2016, January. Three challenges in cyber-physical

systems. In Communication Systems and Networks (COMSNETS), 2016 8th International Conference on (pp. 1-8). IEEE.

Mehedi Hassan M., Pathan A.-S.K., Huh E.-N. And Abawajy J. 2014. Emerging Sensor-Cloud Technology for Pervasive Services and Applications. International Journal of Distributed Sensor Networks, pp. 1-2. Available at: http://www.hindawi.com/journals/ijdsn/2014/610106/ [Accessed: 23 December 2014].

Mosterman P. J. & Zander J. 2016. Cyber-physical systems challenges: a needs analysis for collaborating embedded software systems. Software & Systems Modeling. 15(1): 5-16.

Muller K., Paulitsch M., Tverdyshev S. and Blasum H., 2012. MILS-related information flow control in the avionic domain: A view on security-enhancing software architectures. IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN 2012). June 2012 IEEE, Boston, MA, pp. 1-6.

Mulligan A.D.K., Wang L. and Burstein, A.J. 2011. Privacy in the Smart Grid : An Information Flow Analysis, Berkeley.

Nabil Adam, 2010. Workshop on Future Directions in Cyber-Physical Systems Security, New Jersey.

Nabeel Salih Ali, Mohammed Nasser. 2017. Review of Virtual Reality Trends (Previous, Current, and Future Directions), and Their Applications, Technologies and Technical Issues. ARPN Journal of Engineering and Applied Sciences. 12(3): 783-789.

Park K.-J., Zheng R. and Liu X. 2012. Cyber-physical systems: Milestones and research challenges. Computer Communications, 36(1): 1-7. Available at: http://linkinghub.elsevier.com/retrieve/pii/S0140366412003180 [Accessed: 1 December 2014].

Pal, P., Schantz, R., Rohloff, K., &Loyall, J. (2009, July). Cyber physical systems security challenges and research ideas. In Workshop on Future Directions in Cyber-physical Systems Security.

Raj, R., Lee, I. and Stankovic, J., 2010. Cyber-Physical Systems : The Next Computing Revolution. Automation Conference 2010, 2010 ACM, California, pp. 0–5.

Rawung R. H., & Putrada A. G. 2014, September. Cyber physical system: Paper survey. In ICT for Smart Society (ICISS), 2014 International Conference on (pp. 273-278). IEEE.

Reddy Y. B. 2015, April. Security and design challenges in cyber-physical systems. In Information Technology-New Generations (ITNG), 2015 12th International Conference on (pp. 200-205). IEEE.

Sampigethaya K. and Bushnell L. 2009. A Framework for Securing Future e-Enabled Aircraft Navigation and Surveillance∗. AIAA infotech@Aerospace Conference. 2009 American Institute of Aeronautics and Astronautics, Washington.

Shafi Q. 2012, June. Cyber physical systems security: A brief survey. In Computational Science and Its Applications (ICCSA), 2012 12th International Conference on (pp. 146-150). IEEE.

Shi J., Wan J., Yan H. & Suo H. 2011, November. A survey of cyber-physical systems. In Wireless Communications and Signal Processing (WCSP), 2011 International Conference on (pp. 1-6). IEEE.

Walker J.J. 2012. Cyber Security Concerns for Emergency Management. In: Emergency Management. In TechOpen, Pine Bluff. p. 39.

Wan K., Man K. L. & Hughes D. 2010. Specification, analyzing challenges and approaches for cyber-physical systems (CPS). Engineering letters, 18(3), 308.

Wang E. K., Ye Y., Xu X., Yiu S. M., Hui L. C. K. & Chow K. P. 2010, December. Security issues and challenges for cyber physical system. In Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing (pp. 733-738). IEEE Computer Society.

Wolf W. 2012. Computers as Components Principles of Embedded Computing System Design Second Edi., Elsevier, Burlington.

Gianni D.; Loukas G.; Gelenbe E.2008. A Simulation Framework for the Investigation of Adaptive Behaviours in Largely Populated Building Evacuation Scenarios. In Proceedings of the Seventh International Joint Conference on Autonomous Agents and Multi-Agent Systems (AAMAS 08), Estoril, Portugal.

Galea E.R.; Sharp G.; Lawrence P.J.; Holden R. 2008. Approximating the evacuation of the World Trade Center north tower using computer simulation. J. Fire Prot. Eng. 18, 85-115.