Technical Sciences
Academy of Romania
www.jesi.astr.ro

Journal of Engineering Sciences and Innovation
Volume 8, Issue 4 / 2023, pp. 433-450
http://doi.org/10.56958/jesi.2023.8.4.433

F. Electrical, Electronics Engineering, Computer Sciences and Engineering

Received ***27 August 2023*** *Accepted* ***4 December 2023***
Received in revised form ***27 October 2023***

Dependable Cyber-Physical Systems: concepts, challenges, and case studies

LIVIU-CRISTIAN MICLEA*, ALEXANDRU CIOBOTARU, MARIUS MISAROS, COSMINA CORCHES

Department of Automation, Faculty of Automation and Computer Science, Technical University of Cluj-Napoca, 400114, Romania

Abstract. As the integration of cyber and physical components becomes increasingly prevalent in modern systems, ensuring the dependability of Cyber-Physical Systems (CPS) has emerged as a critical research area. The present paper aims to present a comprehensive analysis of the recent advances in the field of dependable CPS. Firstly, we present an analysis on the evolution of the published papers in the past years and introduce the concepts of dependability and CPSs in the context of Industry 4.0. Secondly, some strategies and challenges that have been encountered in the recent literature for enhancing the dependability of CPS are also presented. Finally, two case studies that highlight the interdependencies between the concepts of dependability and CPS are reviewed. The first one presents the dependability of an object identification system that relies on radio frequency identifier, which can be used in medical services. The second case study shows various techniques for predicting the remaining useful life of a turbofan jet engine using Machine Learning and Deep Learning techniques.

Keywords: dependability, Cyber Physical Systems, availability, reliability.

1. Introduction

As the microcontroller evolved in having more computational resources (i.e., increased memory and processor frequency), embedded devices started to be developed. By integrating a microcontroller, the devices started to fulfill a wider range of functionalities, from monitoring, triggering alarms, to scheduling actions. The next step was for the developed system to get even smarter and start to interact with the physical world. In the case of such systems (Cyber-Physical Systems),

*Correspondence address: liviu.miclea@aut.utcluj.ro

physical and software components are deeply intertwined, as the interaction with each other changes with context.

Compared to an embedded system, Cyber-Physical Systems (CPS) are using computations and communication deeply embedded in and interacting with physical processes to add new capabilities to physical systems [1]. At first glance, CPS resemble to the Internet of Things (IoT), where objects (e.g., devices, sensors, wearable computers, and autonomous physical systems) are connected via a communication network. Even if IoT and CPS are sharing the same basic architecture, in order for CPS to transform the world through systems that respond more quickly, are more precise, and provide large-scale and distributed coordination, it is clear that a higher combination and coordination between physical and computational elements is needed [2].

From the previous statement, it can be observed that during CPS implementation, dependability analysis is of great importance, as the final products involve dependable services that are accountable and adaptable, and through which the interaction with the physical world must be safe [3]. All the previous attributes are components of the dependability tree, which will be presented later in the paper.

The following is the structure of the paper. Section two presents a literature analysis that shows the evolution of the published papers in dependable CPSs. Section three introduces the concepts of dependability and CPSs. Section four presents the strategies and challenges that are encountered while developing dependable CPSs. Section five presents two case studies, that is, the dependability of a radio frequency identifier (RFID) Object-Identification System and machine learning (ML) based techniques for predicting the remaining useful life (RUL) of a turbofan jet engine. Finally, section six presents the conclusions.

2. Literature analysis of Dependable Cyber-Physical Systems

Through a systematic analysis of publications in the IEEE database using the specific keywords "dependable cyber-physical systems", a graph was generated to present the number of scientific publications on the topic of CPS dependability. As illustrated in Fig. 1, the number of publications began to rise in 2008, with a steady increase observed until 2014, followed by a peak in activity from 2014 to 2017. This trend, aligning with technological advancements, showed a brief decline from 2017 to 2019 before experiencing a significant surge, maintaining a high level of interest in academic research until the end of 2021.

An analysis of the IEEE database is presented in Fig. 2 in terms of the number of publications according to types of scientific publications. The study of dependability CPSs had the highest interest in conferences, with 317 published papers. Journals had the second-highest interest, with 227 published papers.

Additionally, four publications were identified in magazines, and three were identified in early access articles.

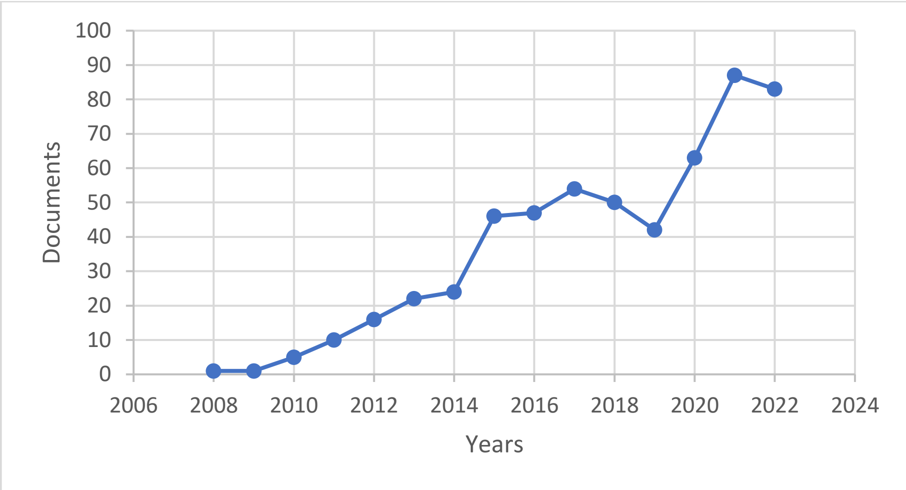

Fig. 1. The total number of publications on Dependable Cyber-Physical Systems between 2008 and 2022.

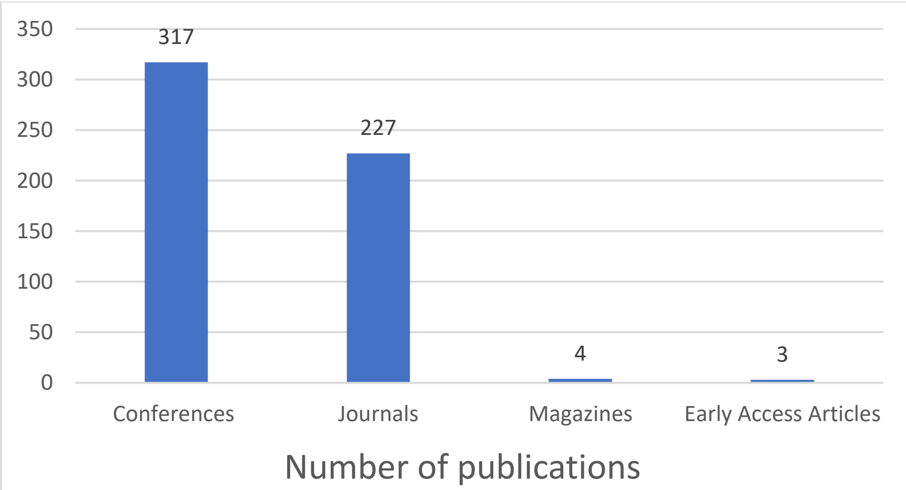

Fig. 2. Distribution of publication types on Dependable Cyber-Physical Systems.

The chart in Fig. 3 displays data from IEEE's research on CPS dependability publication topics, organized by percentage.

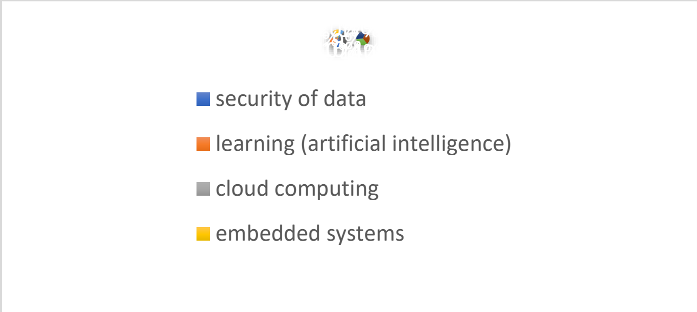

Fig. 3. Representation of research paper topics in Cyber Physical Systems.

From the chart, we can observe that data security holds the greatest percentage (20%) of this study. Another significant percentage (17%) was dedicated to the topic of artificial intelligence. Cloud computing ranks third with the highest percentage at 14%, behind other important topics including embedded systems (10%), the Internet of Things (10%), adaptive control (10%), control system synthesis (10%), and nonlinear control systems (9%).

3. Fundamentals of dependability and Cyber-Physical Systems

3.1. Overview of Dependability

Through the years, multiple definitions of dependability have been stated [4]. Each one of them attempted to define dependability based on the available systems at that time and the services that were provided. A new definition for dependability, considering the current developments, is proposed in [5]: „The dependability of a computer system is the ability to deliver a service that can justifiably be trusted. The service delivered by a system is its behavior as it is perceived by its user(s); a user is another system (physical or human) that interacts with the former at the service interface".

From the previous definition, it can be observed that dependability is a complex analysis that involves considering, in addition to the physical, technological, and structural characteristics of a system, the effects of the environment and operating conditions [6]. All these details are needed to properly model and analyze the dependability of a system while trying to pinpoint its potential weaknesses and improve its capability to operate correctly.

To achieve a system characterization from a dependability perspective, proper measurable quantities are needed to predict with the lowest possible degree of uncertainty the following behaviors of the system [6]:

- What is the system's behavior in operation during its entire useful life?

- What will cause malfunctions or failures during operation, and with what frequency?
- What might be the outage duration?
- What resources are needed to maintain the system in a correct operating state and the resources needed?

The International Federation for Information Processing working group 10.4 describes dependability in terms of three aspects: attributes, means, and threats. The three from Fig. 4 describe the threats to, the attributes of, and the means to achieve dependability [7].

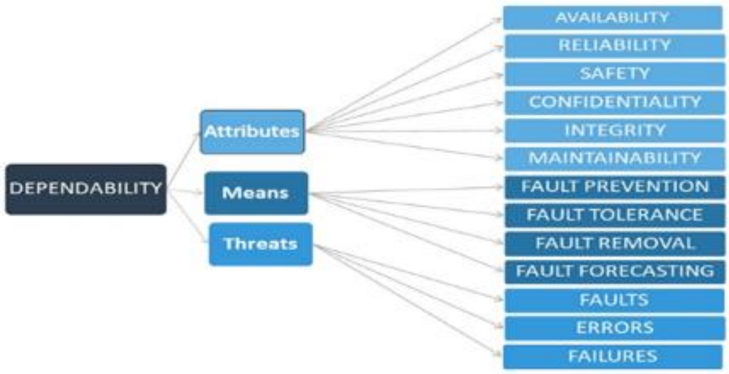

Fig. 4. The dependability Tree - A schematic representation of dependability attributes, threats, and means.

As the services evolved, being provided through an internet connection, security was included as a component of dependability [6]. When it comes to assessing the dependability attributes, the most used when evaluating the dependability of a system are:

- reliability – from a computing point of view, attribute reliability would refer to the probability of having the system operating continuously, without failure, in a given interval and under specified operating and environmental conditions.
- availability – from a computing point of view, attribute availability describes the probability of a system operating at a given point in time independently of the number of failures already sustained by the system.
- maintainability – from a computing point of view, attribute maintainability refers to the probability of a system being recovered to an operating state because of failures.

3.2 Overview of Cyber-Physical Systems

Cyber-Physical Systems (CPS) merge computational and physical capabilities to interact with the human environment through various mechanisms, integrating a range of communication and control features that enhance their application [8-10].

Unlike traditional embedded systems, CPS uniquely benefit from utilizing multiple devices within a network [11]. Consequently, networks and embedded computers within CPS control and monitor physical processes, engaging with these systems through a feedback loop. This interaction significantly influences both the computations and the physical processes, creating a dynamic interplay [12].

CPS are commonly used in areas with direct interaction in various activities, including but not limited to smart assisted living, advanced automotive systems, highly reliable medical systems, defense systems, traffic safety and control, aeronautics, process control, environmental control, energy conservation, and distributive robotics and manufacturing [13].

The CPS connection mode is interpreted by [16] as a multitude of interconnected devices that perceive the physical environment through actuators and sensors. The operation of these types of systems is considered by [17] as a larger, well-defined, secure system that processes and receives information from the physical environment in real time. CPS benefits from an interdisciplinary capability, merging engineering areas with models, such as mechanical, biomedical, environmental, chemical, electrical, aeronautical, and industrial engineering, with computational methods and models [10]. In [18], it is said that an important perspective on these systems is related to the management of physical processes by monitoring the received values based on computational intelligence, aiming at a good perception of the analyzed environment, and ensuring real-time decisions with a high degree of accuracy.

The integration of CPS inside the manufacturing sector, as well as in logistics and services, has the potential to bring about a significant transformation in the context of Industry 4.0. This integration has the capability to autonomously generate significant economic opportunities [19]. The significance of CPSs and big data in the context of Industry 4.0 is explained in paper [20]. This explanation serves as an illustration of the substantial potential for advancement in industry, particularly in terms of enhancing resources.

4. Strategies and Challenges for Enhancing Dependability of CPSs

This section aims to present a non-exhaustive collection of strategies that are used in the recent literature to increase the dependability of CPSs as well as some research challenges [21].

Various frameworks are being developed to increase the dependability of CPSs in a wide range of applications such as: IoT systems [22] , water-based systems [25], [26] or cloud-based systems [27], [28]. In paper [22] the technique used to increase the dependability of a CPS is represented by an end-to-end application capable of detecting the failures of the CPS as well as the associated risks. The CPS is represented by a set of Wi-Fi sensors interconnected to a wireless network that can send data measuring temperature, humidity, pressure, carbon dioxide, and light intensity to a server application that interprets the results using a dependability ontology.

Paper [23] addresses the issue of dependability in CPS by using mathematical epidemiology theory to create a model for monitoring CPS-IoT systems. This study presents a unique reconfiguration strategy that incorporates network segmentation, clustering, and node migration to improve the safety of CPS-IoT subsystems. The CPS-IoT monitoring model, which is being developed, has significant importance inside a CPS orchestration system. It utilizes a closed loop mechanism to enable thorough surveillance and actuation.

The study conducted by Ermeson Andrade et al. [25] presents an approach that employs stochastic Petri nets (SPNs) for the purpose of modeling and evaluating the reliability of intelligent CPSs. The models consider a range of cyber and physical components, allowing the examination of measures like availability, downtime, dependability, and message delivery probability. The viability of this methodology is shown via the assessment of an intelligent CPS implemented inside a water treatment facility. The result is the reduction of the downtime from 12 hours to 8 minutes.

ML, DL and Transfer Learning (TL) play a crucial role in dependable systems, contributing to various aspects of system reliability, security [29], [30], and fault prognosis and diagnosis [31], [32]. For instance, the study conducted by Dhanke J.A. et. al. [30] presents a theoretical framework for improved communication, more specifically, issues related to communication failures and various forms of network attacks in the context of IoT based CPS. To classify the attacks, the authors used supervised learning-based algorithms such as: Naïve Bayes, multilayer perceptron (MLP) or multinomial logistic regression, obtaining an accuracy of 85% on the test set. Paper [31] presents a study that examines the use of correlation and causation metrics to identify and measure the level of dependent connections across the various components of a CPS and predict imminent faults using Artificial Neural Networks (ANNs). The authors conducted experiments on two smart power grids, that is, IEEE 14-bus and IEEE 57-bus test systems [33].

In addition, ML, DL and TL techniques are used to increase the dependability to Fault-Tolerant Control CPSs. More specifically, supervised ML algorithms such as K-Nearest Neighbors (KNN), Support Vector Machines (SVM) or decision trees are used to predict faults in rolling bearings [34], [35], automotive and automobile gearbox [36], [37] or wind turbines [38], [39] fault detection.

Convolutional Neural Networks (CNN) is a branch of DL algorithms that falls under the category of supervised learning as well. The efficacy of this approach has been shown in the domains of image processing, computer vision, and object detection and recognition. When considering fault diagnostic models that use CNNs, it is observed that 2D CNNs encounter challenges related to the curse of dimensionality when applied to 1D inputs such as time series. This open problem was successfully addressed in paper [40] using the wavelet transform. Table 1 presents a summarized overview of the previously presented papers, highlighting the strategies that were used to enhance the dependability of CPSs as well as the objective or the CPS that was used.

Apart from the classical centralized approaches, Federated Learning (FL) is also used to increase the dependability for CPSs. FL is a ML-based technique that involves training a model on decentralized edge devices, such as mobile phones, IoT devices, or local servers. This training process occurs without the need for data exchange between these devices, since each keeps their own local data samples [41].

For instance, paper [42] proposes an FL-based framework for intrusion detection in IoT networks. In a more precise manner, the authors put up a scoring system with the objective of assessing participants by using the Manhattan similarity measure. Next, the anomalous data is eliminated via the use of clustering methods.

Table 1. Summarized Overview of the Strategies used to Enhance Dependability in CPSs

Paper	Strategies	CPS
[22]	Failure Mode and Effects Analysis (FMEA)	A set of Wi-Fi sensors interconnected to a wireless network that can send data measuring environmental information.
[23]	Epidemic states and diffusion sets	IoT based system used for monitoring of an industrial area.
[25]	SPNs	Water treatment facility
[30]	Naïve Bayes, MPL and Multinomial Logistic Regression	A digital platform integrated with electrical devices that facilitates the provision of services.
[31]	ANNs	IEEE 14-bus and IEEE 57-bus test systems
[34]	Hierarchical symbol dynamic entropy and binary tree SVM	Rolling Bearings
[35]	Fusion between CNNs and SVM	Rolling Bearings
[36]	Linear discriminant analysis and SVM	Steering actuator
[37]	Finite element analysis and KNN	Spur gears
[38]	Variational mode decomposition and KNN	Wind Turbine
[39]	Shannon-Wavelet SVM	Wind Turbine
[40]	Wavelet packet transform and CNN	Rolling Bearings

5. Case Studies from literature

5.1. Dependability of an RFID Object-Identification System

One industry that benefits from CPS evolution is the medical industry. CPS can be used for tagged medications, where RFID is used to monitor the drugs administered to patients and to monitor patients and their live signs (e.g., temperature, heartbeats, blood pressure) [6]. Through such implementations, not just the patients are benefiting from improved medical services that are focused on their needs, but also the hospitals by alleviating the burden of inventory management. Additionally, through monitoring patients, it is possible to design CPS capable of identifying or predicting whether hospital staff can be overwhelmed by current and new patients [43], [44].

A system combining the previously mentioned capabilities of medical CPS, designed to monitor patients' activity, was proposed in [45]. By using a Peper robot and radio-frequency identification tags, the authors have developed an object-identification system that can be used in the monitoring of drug administration among the elderly, Fig. 5.

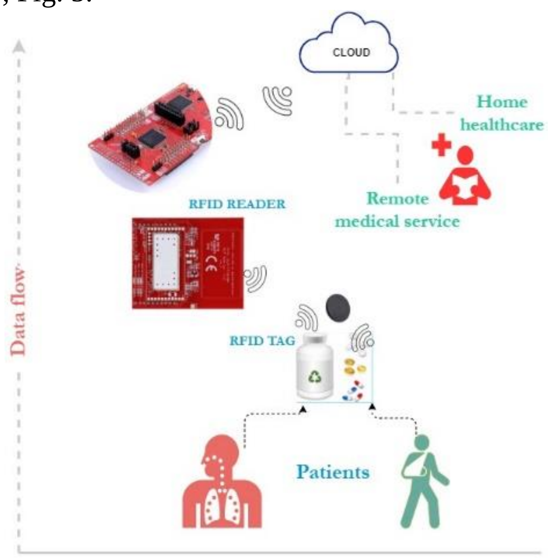

Fig. 5. Patient-monitoring architecture.

To identify the system's weakest components and their impact on system availability, reliability block diagrams (RBD) analysis was performed [46]. However, the RBD analysis does not allow for the evaluation of the impact processes that take during RFID communication, such as tag identification or solving the collision process that might appear during this process. Such events can have a great impact on the availability of the system.

When looking to compute the availability of the system by including the relationships between operating conditions and the events that are occurring during operation, a different approach is needed to model the events and time conditions. Such approach is exemplified by the SPNs [47], which facilitate the creation of a graphical representation for the formal description of systems, while the dynamics are characterized by concurrency, synchronization, mutual exclusion, and conflicts.

Through SPN, the system was described by symbols that describe the events, transitions, and states of the system, Fig. 6.

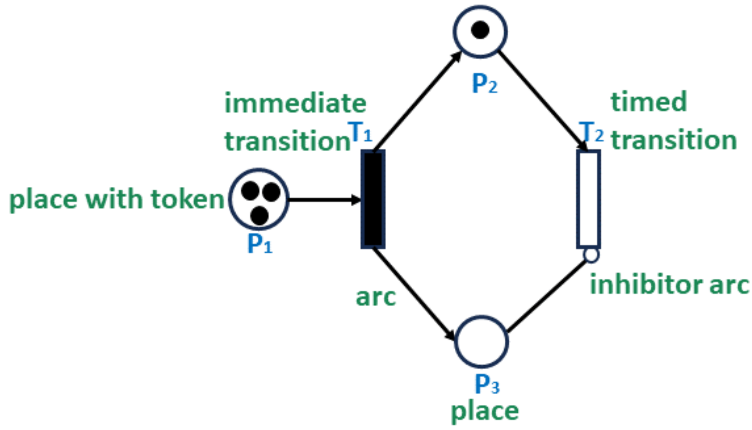

Fig. 6. Basic graphical symbols of SPNs.

Through the analysis performed, it was revealed that when it comes to RFID monitoring, a compromise between the number of tags and the system responses needs to be made. Most papers when discussing RFID object identification focus on determining the maximal throughput that can be obtained based on the number of slots present in a query frame and the number of tags present within the range of the RFID reader's antenna. However, throughput can be seen from two perspectives, either as the number of queries per second or the number identified in an amount of time. To solve this issue, the authors proposed a cost function that has the purpose of identifying the optimal system tag number that can be identified in the shortest identification time while attending to the highest possible probability of achievement.

Through the performed analysis and proposed models, it was revealed that even if an increased number of tags around the RFID reader would translate into a reduced cost value, the probability of the event happening is quite small. Another disadvantage was also the uncertainty of such an event occurring, as there were scenarios that had the same probability of occurrence. In the end, the analysis revealed that without a proper analysis, it is possible to implement a system that would have a high throughput but with large time delays to achieve it.

5.2. Remaining Useful Life Prediction for Turbofan Jet Engines

Prognostics and Health Management (PHM) is a subject that leverages historical, current, and future data about the environmental, operational, and utilization aspects of equipment [48]. Its primary objective is to identify and assess the deterioration, diagnose defects, and implement proactive measures to effectively manage failures. One way to enhance the dependability of CPS is to increase its maintainability. Therefore, Predictive Maintenance (PdM) is one of the most studied approaches to increase the maintainability of the CPSs as by using technique one predict failures before their occurrence using ML or DL [49]. This case study aims to present various ways to predict the Remaining Useful Life (RUL) of a Turbofan Jet Engine CPS using ML and DL techniques. One of the most popular datasets for predicting the RUL of a turbofan jet engine in the literature is the one provided by NASA [52]. The dataset was simulated using the Commercial Modular Aero-Propulsion System Simulation (C-MAPSS) tool and divided into four subsets denoted FD001, FD002, FD003 and FD004 respectively [53]. Regarding the operational conditions, it is noteworthy that each subset has the potential to include either one or six distinct operating conditions. These conditions are determined by three key factors: altitude, which ranges from 0 to 42,000 feet; throttle resolver angle, which spans from 20 to 100 degrees; and Mach, which varies between 0 and 0.84. Regarding failure modes, each dataset may exhibit either one or two modes, namely HPC deterioration and fan degradation. Every subset comprises measurements obtained from a total of 21 sensors attached to different parts of the degrading engine which represent the dependent variables while the independent variable is the value RUL expressed in hours.

The data preprocessing step is crucial in any ML-based algorithm to make sure that the model can learn the data correctly. Therefore, one common preprocessing technique involves the construction of a health index curve using autoencoders [54] or semi-supervised learning [55]. Regarding models that are suitable for this task, the literature mainly covers Recurrent Neural Networks [56], Long-Short Term Memories (LSTMs) or CNNs. Paper [57] introduced a supervised domain adaptation methodology that leverages labeled data from the target domain to refine a bidirectional LSTM model, which was first trained on the source domain. Additionally, paper [58] introduced hybrid models by integrating the CNN layers with LSTM layers. The use of such ensemble models has shown a superior level of precision compared to other conventional techniques.

6. Conclusion

In conclusion, the investigation into dependable CPSs uncovers a terrain abundant in challenges, opportunities, and inventive resolutions. The challenges that have been discovered highlight the necessity of multidisciplinary collaboration, which involves the integration of professionals from the fields of computer science, engineering, and artificial intelligence.

Even though the ML and DL provide great advantages when it comes to enhancing dependability in CPS, some drawbacks stand out. Firstly, ML techniques are strongly dependent on the availability and quality of data. One of the primary challenges faced by professionals in this field is the scarcity of data that is not biased and is correctly collected and labeled. Secondly, no matter how qualitative the data is, in the future there is the potential for the model to become ineffective as the volume of data grows. Hence, to maintain the functionality of the algorithm, it is necessary to engage in ongoing monitoring and maintenance.

This paper contributes to the existing body of knowledge by integrating theoretical perspectives with real case studies, providing guidance for researchers and practitioners in their efforts to develop CPSs that are both robust and secure.

References

[1] Švéda M., Ryšavý O., *Dependable Cyber-Physical Systems Networking: an approach for Real-Time, software intensive systems*, 12th IFAC Conference on Programmable Devices and Embedded Systems, 2013, p.116-119.

[2] https://www.nsf.gov/pubs/2021/nsf21551/nsf21551.htm (accessed on 10 March 2023).

[3] Wan K., Alagar V., *Dependable Context-Sensitive Services in Cyber Physical Systems, 2011IEEE 10th International Conference on Trust*, Security and Privacy in Computing and Communications, Changsha, China, 2011, p. 687-694.

[4] Avizienis A., Laprie J., Randell B., Landwehr C., *Basic concepts and taxonomy of dependable and secure computing, IEEE Transactions on Dependable and Secure Computing*, **1**, 1, 2004, p.11–33.

[5] IEC 60050, International Electrotechnical Vocabulary: Chapter 191: Dependability and Quality of Service. IEC Standard No. 60050-191, 2nd edn., 2001.

[6] Trivedi K., Bobbio A., *Reliability and Availability Engineering: Modeling, Analysis, and Applications*, Cambridge: Cambridge University Press, 2017.

[7] Technical Committee #176 of the International Organization for Standardization, Quality management and quality assurance, ISO/TC176/SC 1/ Concepts and Terminology. Available online: https://www.iso.org/standard/45481.html?browse=tc (accessed on 22 September 2023).

[8] Alguliyev R., Imamverdiyev Y., Sukhostat L., *Cyber-physical systems and their security issues*, Computers in Industry, **100**, 2018, p. 212-223.

[9] Wolf W., *Cyber-physical systems*, Computer, 42.03, 2009, p. 88-89.

[10] Shi J., et al. A survey of cyber-physical systems. Proceedings of IEEE International Conference on Wireless Communications and Signal Processing, 2011, p. 1-6.

[11] Zanero S., *Cyber-physical systems*. Computer, **50**, 4, 2017, p. 14-16.

[12] Lee E.A., *Cyber physical systems: Design challenges*, Proceedings of 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC). IEEE, 2008, p. 363-369.

[13] Liu Y. et al., *Review on cyber-physical systems*, IEEE/CAA Journal of Automatica Sinica, **4**, 1, 2017, p. 27-40.

[14] Kayan H. et al., *Cybersecurity of Industrial Cyber-Physical Systems: A Review*, ACM Computing Surveys (CSUR), 54.11s, 2022, p. 1-35.

[15] Kim S., Park K.J., Chenyang L.U., *A survey on network security for cyber–physical systems: From threats to resilient design*, IEEE Communications Surveys & Tutorials, **24**, 3, 2022, p. 1534-1573.

[16] Alur R., *Principles of cyber-physical systems*, MIT Press, 2015.

[17] Kalluri B., Chronopoulos C., Kozine I., *The concept of smartness in cyber–physical systems and connection to urban environment*, Annual Reviews in Control, **51**, 2021, p. 1-22.

[18] Delicato F.C. et al., *Smart Cyber–Physical Systems: Toward Pervasive Intelligence Systems*, Future Generation Computer Systems, **107**, 2020, p. 1134-1139.

[19] Lee J., Bagheri B., Kao H.A., *A Cyber-Physical Systems Architecture for Industry 4.0-Based Manufacturing Systems*, Manufacturing letters, **3**, 2015, p. 18-23.

[20] Xu L.D., Duan L., *Big data for cyber physical systems in industry 4.0: a survey*, Enterprise Information Systems, **13**, 2, 2019, p. 148-169.

[21] Adedjouma M., Yakymets N., *A Framework for Model-based Dependability Analysis of Cyber-Physical Systems*, Proceedings of 19th International Symposium on High Assurance Systems Engineering, 2019, p. 82-89.

[22] Sanislav T., Mois G. and Miclea L., *A new approach towards increasing Cyber-Physical Systems dependability*, Proceedings of the 16th International Carpathian Control Conference, 2015, p. 443-447.

[23] Bagula A., Ajayi O., Maluleke H., *Cyber Physical Systems Dependability Using CPS-IOT Monitoring*, Sensors, 2021.

[24] Kleanthis T., Christoulakis F., UML4IoT—A UML-*based approach to exploit IoT in cyber-physical manufacturing systems*, Computers in Industry, 2016, p. 259-272.

[25] Andrade E., Nogueira B., Callou G., Alves G., *Dependability analysis of a cyber-physical system for smart environments*, Concurrency and Computation, 2019.

[26] Xinyue C., *Cyber-Physical System (CPS) architecture for real-time water sustainability management in manufacturing industry*, Proceedings of 14^{th} International Conference on Intelligent Computation in Manufacturing Engineering, 2021, p. 543-548.

[27] Muhammad A. et al., *Soft Computing Techniques for Dependable Cyber-Physical Systems*, IEEE Access, 2019.

[28] K. Gai, M. Qiu, H. Zhao and X. Sun, *Resource Management in Sustainable Cyber-Physical Systems Using Heterogeneous Cloud Computing*, IEEE Transactions on Sustainable Computing, 2018, p. 60-72.

[29] Cheng F., Shen J., *Machine learning for securing Cyber–Physical Systems under cyber-attacks: A survey*, Franklin Open, 2023.

[30] Dhanke J.A., Kamalraj R, Ramesh G, Sakthidasan K.S., Sharma S., Khasim S., *A machine learning based IoT for providing an intrusion detection system for security*, Microprocessors and Microsystems, 2021.

[31] Koosha M., Sahra S.S, Ali R.H., *Identification of interdependencies and prediction of fault propagation for cyber–physical systems*, Reliability Engineering and System Safety, 2021.

[32] Arslan A.A,, Muhammad S.I., Muhammad H.S., *Development of Intelligent Fault-Tolerant Control Systems with Machine Learning, Deep Learning, and Transfer Learning Algorithms: A Review*, Expert Systems with Applications, 2023.

[33] University of Washington. Power systems test case archive. Available at: http://www.ee.washington.edu/research/pstca/. Last accessed 19 November 2023.

[34] Li Y., Yang Y., Wang X., Liu B. & Liang X., *Early fault diagnosis of rolling bearings based on hierarchical symbol dynamic entropy and binary tree support vector machine*, Journal of Sound and Vibration, 2018, p. 72–86.

[35] Lu C., Wang Z., Zhou B., *Intelligent fault diagnosis of rolling bearing using hierarchical convolutional network-based health state classification*, Advanced Engineering Informatics, 2017, p. 139–151.

[36] Shi Q., Zhang H., *Fault diagnosis of an autonomous vehicle with an improved SVM algorithm subject to unbalanced datasets*, IEEE Transactions on Industrial Electronics, 2021, p. 6248–6256.

[37] Park S., Kim S., Choi J.-H., *Gear fault diagnosis using transmission error and ensemble empirical mode decomposition*, Mechanical Systems and Signal Processing, 2018, p. 262–275.

[38] An X., Tang Y., *Application of variational mode decomposition energy distribution to bearing fault diagnosis in a wind turbine*, Transactions of the Institute of Measurement and Control, 2017.

[39] Tang B., Song T., Li F., Deng L., *Fault diagnosis for a wind turbine transmission system based on manifold learning and Shannon wavelet support vector machine*, Renewable Energy, 2014.

[40] Islam M. M. M., Kim J.-M., *Automated bearing fault diagnosis scheme using 2D representation of wavelet packet transform and deep convolutional neural network*, Computers in Industry, 2019.

[41] Mashal K., Frank G.G, Matthias N., *Federated Learning as a Provacy Solution*, Proceedings of the 4th International Conference of Industry 4.0 and Smart Manufacturing, 2023, p. 316-325.

[42] Yang R., Hui H., Yulong W., Yue Q., Weizhe Z., *Dependable federated learning for IoT intrusion detection against poisoning attacks*, Computers & Security, 2023.

[43] Mahulea C., García-Soriano J.-M., Colom J.-M., *Modular Petri net modeling of the Spanish health system*, Proceedings of 2012 IEEE 17th International Conference on Emerging Technologies & Factory Automation (ETFA 2012), Krakow, Poland, 2012, p. 1-8.

[44] Dotoli M., Fanti M.P, Iacobellis G., Martino L., Moretti A. M., Ukovich W., *Modeling and management of a hospital department via Petri nets*, IEEE Workshop on Health Care Management (WHCM), Venice, Italy, 2010, p. 1-6.

[45] Corches C., Daraban M., Miclea L., *Availability of an RFID Object-Identification System in IoT Environments*, **21**, 18, 2021, p. 6220.

[46] Corches C., Donca I.C., Stan O., Miclea L., Daraban M., *Analyzing the RFID Failure Impact on Availability of IoT Services*, IEEE 26th International Symposium for Design and Technology in Electronic Packaging (SIITME), Pitesti, Romania, 2020, p. 163-168.

[47] Maciel P. et al., *Mercury: Performance and Dependability Evaluation of Systems with Exponential, Expolynomial, and General Distributions*, IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC), Christchurch, New Zealand, 2017, p. 50-57.

[48] Zio E., *Prognostics and Health Management of Industrial Equipment*, Seifedine Kadry. Diagnostics and Prognostics of Engineering Systems: Methods and Techniques, IGI Global, 2012, p. 333-356.

[49] Qiu S., Cui X., Ping Z., Shan N., Li Z., Bao X., Xu X., *Deep Learning Techniques in Intelligent Fault Diagnosis and Prognosis for Industrial Systems: A Review*, Sensors, 2023.

[50] Nunes P., Santos J., Rocha E., *Challenges in predictive maintenance – A review*, CIRP Journal of Manufacturing Science and Technology, 2023.

[51] Tiago Z. et. al., *Predictive maintenance in the Industry 4.0: A systematic literature review*, Computers & Industrial Engineering, 2020.

[52] Saxena A., Goebel K., Simon D. and Eklund N., *Damage propagation modeling for aircraft engine run-to-failure simulation*, Proceedings of the International Conference on Prognostics and Health Management, 2008, p. 1-9.

[53] C-MAPSS Jet Engine Data. Available at: https://data.nasa.gov/Aerospace/CMAPSS-Jet-Engine-Simulated-Data/ff5v-kuh6. Last accessed: 11 November 2023.

[54] Pillai S., Vadakkepat P., *Two stage deep learning for prognostics using multi-loss encoder and convolutional composite features*, Expert Systems Applications, 2021.

[55] Berghout T., Mouss L.H, Kadri O, Saïdi L., Benbouzid M., *Aircraft engines remaining useful life prediction with an improved online sequential extreme learning machine*, Applied Sciences, 2020.

[56] Yuan M., Wu Y.-T., Lin L., Fault Diagnosis and Remaining Useful Life Estimation of Aero Engine Using LSTM Neural Network, Proceedings of the IEEE International Conference on Aircraft Utility Systems, 2016, p. 135–140.

[57] Zhang A., Wang H., Li S., Cui Y., Liu Z., Yang G., Hu J., *Transfer Learning with Deep Recurrent Neural Networks for Remaining Useful Life Estimation*, Applied Sciences, 2018.

[58] Kong Z., Cui Y., Xia Z., Lv H., *Convolution and Long Short-Term Memory Hybrid Deep Neural Networksfor Remaining Useful Life Prognostics*, Applied Sciences, 2019.