Augmenting Cyber Physical Systems through Data Collection & Machine Learning: A Perspective

Siddiq Moideen[1*], Haritha Deepthi[2*], Jacquline Dorothy[3†]

[1*]siddiqmoideen07@gmail.com, [2*]harithadeepthibtech@gmail.com, [3†]jacqulinedorothy@gmail.com

Abstract:
Industry 4.0, destined to an astounding breakthrough in the field of Production & Manufacturing through leading-edge Cyber Physical Systems, Monitoring systems & Automation. The next big Industrial Revolution focuses on digitalizing industries which are popularly known as Digital Twinning, any changes to the Digital Twin reflects the Real Physical World. Cyber Physical Systems are the key players in the 4th industrial Revolution, Cyber Physical Systems are an amalgamation of Theory of Cybernetics & Mechatronics where Physical Plant i.e., Full-Fledged Hardware components Controlled/Monitored by Computational platforms i.e., Computer-Based Algorithms moderated by Network Fabrics & Sensors. CPS integrates the dynamics of physical processes, software & networking. Where components of Physical and Computational elements are deeply intertwined. The Backdoors of the system aren't robust enough to tackle modern-day Cyber Threats. Digital Twinning gives us an upper-hand in both Security and Production perspectives. Our paper aims at enhancing the production & security of the CPS through Machine learning approach, analysing the digital assets statistically to set a favourable pay.

Keywords: Industry 4.0, Cyber Physical Systems, Game Theory, Deep Learning, Transfer Learning, Simulated Systems, Digital Twin, Security Mechanisms, Cloud Manufacturing, Big Data Analytics, NoSQL

I. INTRODUCTION TO CPS

Cyber Physical Systems are multidisciplinary systems that conduct feedback control over widely distributed embedded computing systems through a mixture of control, communication and computation. Modern CPS are highly collaborative, synchronised in real-time, solid and dynamic; bolstered through network systems & physical systems represented through a traditional tightly coupled embedded system comprising a vast set of intelligent wired/wireless actuators & sensors. Working with CPS, any changes to the system in cyberspace will affect & reflect the system in the physical world in real-time through IoT and IoS.

The invergence of 3C technologies leads to next-gen engineered systems that are wide ranging and highly transformative via efficient computation, distributed sensing, high-level decision-making algorithms, control over wireless/wired communication networks and multi-object optimization; engineered cyber physical systems are implied in branches of mechatronics, biology, computer science and chemistry which are integrated into many societal critical realms such as construction, energy, transportation and med systems. Physical & Technical systems are developed and designed to be more & more reliable, smart, robust, efficient and secure.

With such high notions, the scope of CPS and integration of Cloud computing are about to bring the next big Industrial Revolution, Industry 4.0. The complete ecosystem, contrived into a digital twin in cyberspace, any changes in the cyber twin will reflect in the physical world which could boost the production & efficiency in the field of avionics, distributed robotics, energy conservation, process control, smart structures, defence systems, critical infrastructure control, assisted living, environmental control, med tech, manufacturing and traffic safety & control.

II. INDUSTRY 4.0

Industry 4.0, the futuristic stage in controlling and organising the entire industrial value stream along with the lifecycle of the end product based on dynamicity, self-organizable, cross-organizational, real-time optimized value networks, which can be optimized according to availability, demand, costs and consumption of resources.

Thereafter, solving the existing problems in social infrastructure, safety, security, resource efficiency, standardization, work design, training & organization, and regulatory framework. "Industry 4.0 is a collective term for technologies and concepts of value chain organization"

Within the modular structured smart factories of Industry 4.0, CPS monitors the physical processes, makes a virtual copy of the physical world and makes decentralized decisions, on which they communicate and cooperate with each other & humans in real-time powered through internal/cross organisational services via IoT & IoS.

In a smart factory, each and every entity in the ecosystem are equipped with a feedback system controlled & co-ordinated by software that are connected through the Internet, therefore forming a seamless interconnected co-operative production system in real-time where all physical production elements in the physical world have a cyber twin in the

cyberspace destined to achieve the global optimization of production and utilisation which gives rise to a novel CPS platform that would collaborate different business networks into a singleton face.

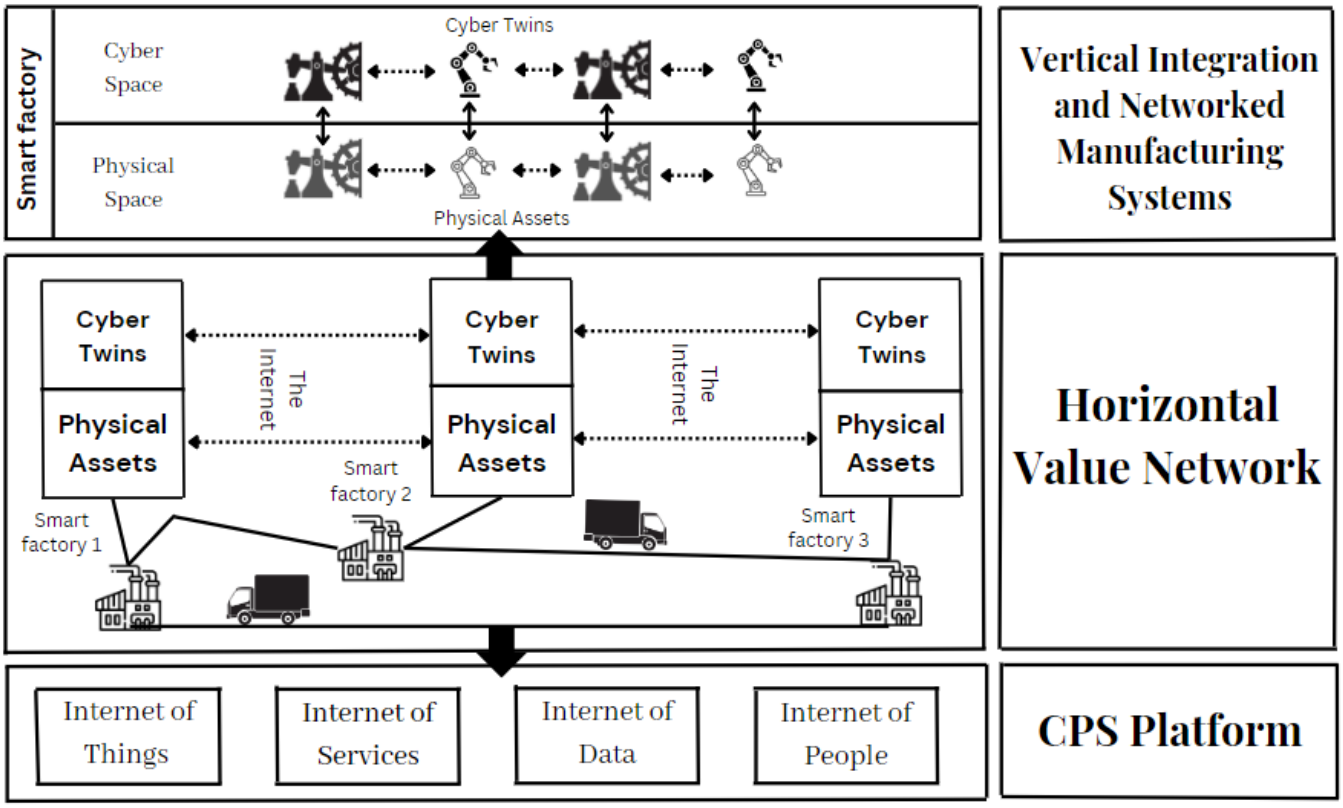

Figure 1: Industry 4.0 Principles

CPS paves a vital bridge between the horizontal & vertical network manufacturing sectors. The widespread application of CPS gives rise to the generation of industrial big data, which requires big data analytics and cloud technology for analysis, storage and computational resources.

III. CLOUD MANUFACTURING

Cloud Manufacturing is a new networked manufacturing paradigm that establishes the cyber face of Industry 4.0 by organising production elements over the networks according to the client's requirements in order to provide on-demand manufacturing services via cloud service platforms thus, enabling omnipresent & flexible on-demand network access to a shared pool of virtual configurable manufacturing resources that can be easily upgraded in need.

In cloud manufacturing mode, providers supply the requirements to the platform according to the requested service i.e., servitization to cyber manufacturing-end for all kinds of product life-cycle stages such as product design, management, manufacturing and testing, later transformed into pooled services & are simulated in real-time. This is an advanced manufacturing business approach directly spotlights over the core manufacturing issues and pays less attention towards issues like demographic change and urban production, altogether which is game-changing.

Cloud manufacturing relies on Process and Digital Twin Modelling Solutions with modernized connection protocols and communication frameworks. The exertion of diverged layers in cloud manufacturing requires different technologies to integrate; such as IoT, H2M interface, virtualization, cloud computing, semantic web and servitization technologies in order to scrutinize the physical production elements and transform them into virtual assets.

These Digital Twins of the physical world are developed and modelled to attain certain extents that mimic the physical systems in real-time which can adapt to wide variety of environmental scenarios and can tackle problems via an open-loop monitoring system in-times even powered with AI-feedback systems for complex operation in the manufacturing process, purely intended to attain an assisted/self-controlled decentralized production system that act and decide autonomously.

A. Simulated Production System

A simulated production system, used to acquire value streams from the virtual factory, each and every manufacturing element such as machine resources, product workpieces and tools are replicated into a cyberworld. Where, workplan is a set of sequential operations accomplished in order to produce a finish product in the physical ecosystem later used to simulate the process in the cyberspace. Each product has its own product type as per its sequential flow towards a final product and each

machine has its own machine type as per their encoded specific requirements to bring out a finish product, so there are contrasting varieties of virtual products and machines as in the physical world.

Moreover, Digital Twins are integrated through real-world recorded fields and tuned-up simulated records sourced from sensors & actuators of the ecosystem. A complete Digital Twin can predict & mimic the system's production and behaviour such as manufacturing time, device microstructure & architecture, part defects and integration of temperature and velocity fields with at most accuracy in real-time.

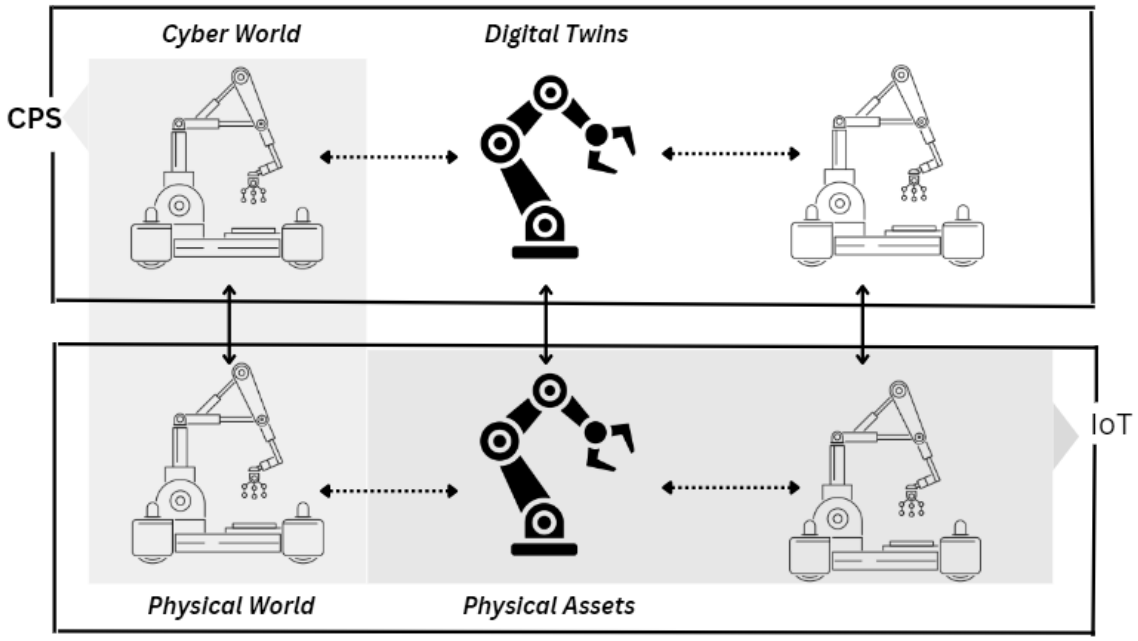

Figure 2: Digital Cloning via CPS implications

In simulation production systems we have an upper hand, an extensive ability to fast forward time as per the recorded sequential growth of the ecosystem in-time with the integration of ML prediction models. Thereby, giving out an exceptional futuristic statistical plot points for the ecosystem, paving the way for improvements and augmentation. There's always an option for trying any newer revisions in the cyberspace i.e., over the simulated model rather than the physical ecosystem probably which could lead to some critical consequences.

B. Security Mechanisms

The major security objectives are Confidentiality, Integrity, Availability and Accountability of the ecosystem; Smarter the ecosystem is, times the more vulnerable it is. Usually, security mechanisms are branched into the following four categories: asset-centric security, network-centric security, data-centric security & user-centric security. Mixing up multiple security mechanisms sets to multiple complications since the security mechanisms must be fused meticulously at every level of the system in order to achieve multi-objective security, if not done correctly; there are chances for undesired security gaps or redundancy that make the system vulnerable for attacks.

a) Asset-centric security revolves around the device or asset, branched over hardware & software security. *Hardware Security* focuses on establishing the validity of physical components; Physical Marking/Watermarking and Crypto processors measures for liability, traceability & counterfeit detection of the intrinsic/extrinsic portion of the components. *Software Security* solutions aims at protecting software against attacks such as observatory & un-observatory attacks, run-time misbehaviours, breakable backdoors that can be columned through Antivirus software, Tamper-resistant software and Digital watermarking.

b) Network-centric Security aims at establishing a secure communication among the nodes in the network, a major facet of cloud-based manufacturing & framework. The objective is hit through HTTPS, Secure multicasting, Virtual private networks, Blockchains, Onion routing and Intrusion detection systems.

c) Data-centric security aims at protecting data along with the lifetime from its origination, transmission, updation and storage that are achieved through Encryption and Steganography models that bags up Symmetric encryption, Asymmetric encryption, Multi-layer encryption, Secret sharing, Secure multiparty computation, Cryptographic hash functions and Digital certification techniques.

d) User-centric security revolves around user privileges over the cyber physical system, achieved through the concept of Authorization, Authentication, Access control and Anonymity that help designers to come up with a more secure architecture that prevents an attack from an intruder or an unauthorised individual.

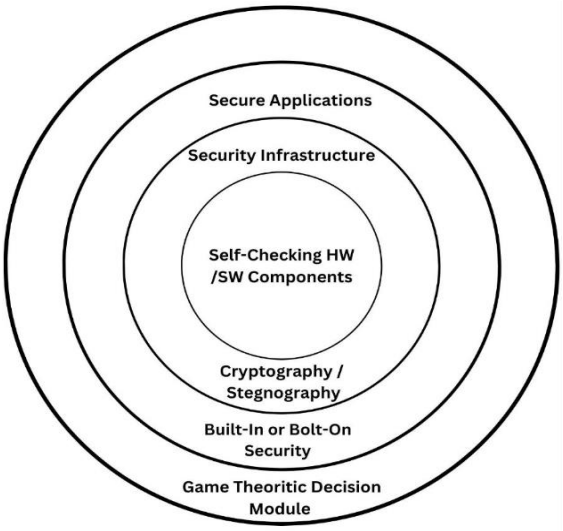

Figure 3: Holistic System Design Approach

C. Data Collection

The virtual simulation approach is the most efficient way for data collection; Each & every measurement of the nodes, entities & products of the ecosystem are accounted in every aspect. Since, the workflow of the system is pre-designed in order to mimic the physical world which adapts and synchronises itself to the real physical world with the help of actuators & sensors. Each account batch bags up the M2M interaction, Resource consumption, M2H interaction, Product lifecycle, Machine temperature, Fault registry, Latency, Idle period, Machine health and System log data in the form of Comma Separated values latter mould into several advanced structural models.

Adopting Not Only Structured Query Language(NoSQL) approach towards Industrial Data Analytics that are diverged through various industry-related applications, network operations, object tracking & asset and data management due to its robustness, extensibility, versatility, efficiency and portability. A perfect environment to manage time-related path properties, mapping dependencies of various system components to capture potential weak points, and communications between various networked elements.

The data models are branched out into the following system entities: dynamic and static. The class of static entities are those entities that do not change in time which covers testbed setup profiles, network interfaces, testbed components and their settings. These entities are normally predetermined or collected in the initialization of each measurement. The class of dynamic entities captures various system events since they tend to change in time which covers network traffic, machine status reports and information flows in the testbed. These entities are dynamically added into the data set whose properties and quantities are determined by the measured data.

IV. INDUSTRIAL DATA ANALYTICS

Industrial data analytics plays a crucial role in attaining the vision of decentralized smart factories and improved decision-making capabilities, implied over diverse industrial applications that avoids costly failures & severe down-times. The main facets of the objective bags up highly distributed data ingestion, repository, management, governance & analytics which improves machinery utilization, predicts production/market demands, reduces defective products, improves product quality, identifies risk factors, augments supply chain efficiency and makes accurate logistic schedules & plans for the manufacturing/production scheme.

A. Visualization

Visualization, an art of presenting data. Visualization helps us in forming a mental map of the production systems in the ecosystem. A cognitive transition from one perception to another is a must, visualisation tends to mitigate different perspectives over the system, latter influencing the decision-making process of the ecosystem through statistical interactions, comparison & workflows by employing data collected through the simulated systems in cyberspace.

The overall goal is the optimization of the production process concerning a diversity of parameters though the optimal solution is that unknown to the user-end, visualization helps the clients to improve the factory ecosystem over a wide range of prospects which would enable the end user to approximate the optimal solution and conclusions to the ecosystem.

B. Game Theory Implementation

Game Theory is primarily a mathematical framework that analyses the decision-making of a player based on how they expect other players to make a decision i.e., determining optimal rational choices given a set of circumstances which can be applied in many fields such as economics, politics, computer science, biology, philosophy & so on where a game is considered to be a set comprising of all possible input moves made by the defence and attacker end. Game theory depicts a game through each player's strategical set and the type of player involved.

A game, interaction between different players according to a set of rules. The player set may consist of individuals, parties, machines, associations or companies. The results of game theory depend on the player's actions & estimated payoff, a measure of satisfaction by each player before making decisions. Thereby, the players perform actions and take decisions in such a way that the individual/player yields the maximum payoff.

In game theory, there are different types of games that help us analyse different problems. They are categorised on the basis of number of players involved, cooperation among players & symmetry of the game.

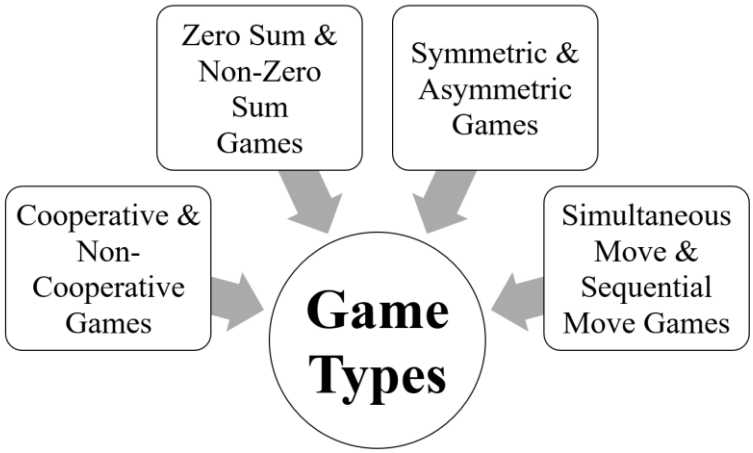

Figure 4: Game Theory Types

The prisoner's dilemma is one perfect example; how a game is analysed in game theory which shows why two completely rational individuals might not cooperate, even if it appears that of their best interests to do so. Prisoner's dilemma is a situation where individual decision-makers always have an incentive to choose in a way that creates a less-than-optimal outcome for the individuals as a group.

Two members of a cartel named Robert & Walter were arrested and imprisoned. Each prisoner is in solitary confinement and they have no means of communicating with each other. The prosecutors lack sufficient evidence to convict the pair on the principal charges.

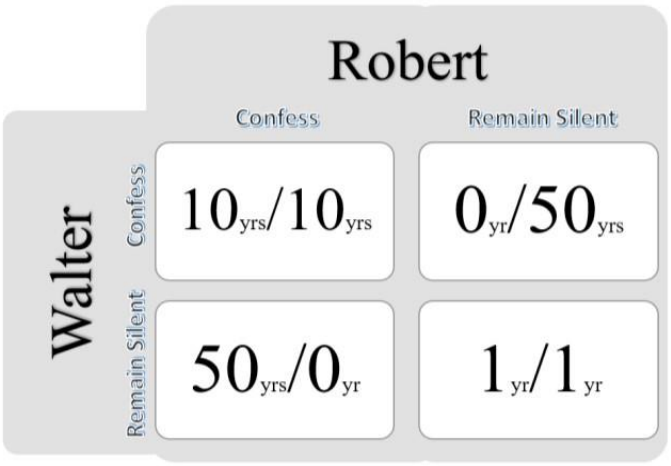

Figure 5: Decision Matrix

Prosecutors hope to get both of them sentenced on a lesser charge. Simultaneously, the prosecutors offer each prisoner a bargain. Each prisoner is given an opportunity either to betray the other by testifying the crimes committed by the other cartel member or to cooperate with the other cartel member by remaining silent. These are the options laid:

- If Robert & Walter, both betray each other i.e., if they both confess, each will serve 10 years in prison.
- If Robert betrays Walter but Walter remains silent, Robert will be set free & Walter must serve 50 years in prison.
- If Walter betrays Robert but Robert remains silent, Walter will be set free & Robert must serve 50 years in prison.
- If Robert & Walter both remain silent, both of them will serve only 1 year in prison each.

Note that it is implied that the prisoners that their decision will not affect their reputation in the future and they have no opportunity to reward or punish their partner other than the prison sentences they get.

We'd feel both remaining silent would be the best option. But the individuals won't opt for it; Both of them will betray each other i.e., they would confess. Because that's the human psychology, confession seems to be the best option for both the parties. Secondly, the prisoner clings on luck that he would be set free, if the other prisoner does not confess & fears that what if I remain silent and the other confesses. Because betraying the partner offers a greater reward than cooperating with them, all pure rational self-interested prisoners will betray the other, meaning the only possible outcome for two rational prisoners is for them to betray each other and that is Nash Equilibrium A.K.A. Optimal state for all the participants. The prisoner's dilemma game can be used as a model for many real-world situations involving a cooperative behaviour.

With respective to the branch chosen in game theory, the Nash equilibrium (i.e., the optimal vulnerable point where the attacker aims at) in the CPS is found, Latter the system is defended via appropriate measures, by integrating the ML techniques; the backdoors of the system will be unbreakable.

C. Deep Learning Approach

Deep Learning, a subset of Machine Learning paradigm. A system, rather than explicitly following the instructions fed to it; The system moulds itself to accomplish the set target implied through Multilayer perceptrons further optimised through Supervised, Unsupervised and Reinforcement approach that sets path to feature extraction, computer vision, advanced security, model prediction & assisted decision-making models which can be engineered into the systems. Transfer learning, a G-factor in model deployment that bridges the cloud and local environments through its profound flexibility and minimal hardware requirements.

Integrating AI into the ecosystem is a pivoting factor in Industry 4.0, each and every path laid were to attain this particular stage of indulging intelligence to the ecosystem to make self-controlled/decentralised decisions. The path laid, journey of amalgamating 3C technologies, integrating embedded computing and cloud manufacturing in order to populate the invergence of Cyber-Physical systems & digital twinning; thereby, making it easier for remote access & data collection via simulation models in real-time which can be used to train the model through several machine learning algorithms latter implied over a wide range of possibilities.

AI systems can be enforced for decision-making, vulnerability check, industrial upgradation, optimal workflow, scope for improvements and optimal power/resource consumption by the analytical & predictive report generated. Combination of Cyber-Physical Manufacturing environment, Simulation systems, Game Theory and Machine Learning models; turns out to have an omnipotent impact over the upcoming years.

V. CONCLUSIONS

With high notions of Smart physical & simulated factories, the heights the production industries are about to reach are 'out of the world'. Virtual factory in the cyberspace gives us an upper-hand over the data collection process, which can be further beautifully laid for analysis. By deploying machine learning algorithms, trained through the collected dataset that give out an accurate predictive model to optimize the production, cut down the cost failures & downtime and develop/upgrade the existing ecosystem which all leans on big data analytics, deployment and cloud manufacturing technologies. The mixture of Game Theory & ML algorithms boils down a robust defence system, securing the backdoors & vulnerable weak points of CPS. Such an approach towards Industrialisation breaks the fabric of present production ecosystem to a more resilient & mature factories.

COMPLIANCE WITH ETHICAL STANDARDS

Funding: This study does not involve any funding.

Conflict of Interest: There is no conflict of interest.

Ethical approval: This article does not contain any studies with animals or human participants performed by any of the authors.

REFERENCES

Hausi A. Müller, "The Rise of Intelligent Cyber-Physical Systems", *IEEE*, https://doi.org/10.1109/MC.2017.4451221, 18 December 2017.

Mahmoud Parto, Pedro Daniel Urbina Coronado, Christopher Saldana and Thomas Kurfess, "Cyber-Physical System Implementation for Manufacturing with Analytics in the Cloud Layer", *ASME*, https://doi.org/10.1115/1.4051663, 14 July 2021.

Zhijia You and Lingjun Feng, "Integration of Industry 4.0 Related Technologies in Construction Industry: A Framework of Cyber-Physical System", *IEEE*, https://doi.org/10.1109/ACCESS.2020.3007206, 6 July 2020.

Yongkui Liu and Xun Xu, “Industry 4.0 and Cloud Manufacturing: A Comparative Analysis”, *ASME*, MANU-16-1445, https://doi.org/10.1115/1.4034667, 6 October 2016.

Kyoung-Dae Kim and P. R. Kumar,” Cyber–Physical Systems: A Perspective at the Centennial”, *IEEE*, https://doi.org/10.1109/JPROC.2012.2189792, 3 April 2012.

Fernando Matsunaga, Vitor Zytkowski, Pablo Valle and Fernando Deschamps “Optimization of Energy Efficiency in Smart Manufacturing Through the Application of Cyber–Physical Systems and Industry 4.0 Technologies”, *ASME*, https://doi.org/10.1115/1.4053868, October 2022.

Siva Chaitanya Chaduvula, Adam Dachowicz, Mikhail J. Atallah and Jitesh H. Panchal, "Security in Cyber-Enabled Design and Manufacturing: A Survey", *ASME*, https://doi.org/10.1115/1.4040341, December 2018.

Tobias Post, Rebecca Ilsen, Bernd Hamann, Hans Hagen and Jan C. Aurich, "User-Guided Visual Analysis of Cyber-Physical Production Systems", *ASME*, https://doi.org/10.1115/1.4034872, June 2017.

Mikhail V. Chester and Braden R. Allenby, "Perspective: The Cyber Frontier and Infrastructure", IEEE, https://doi.org/10.1109/ACCESS.2020.2971960, 05 February 2020.

Vishruti Kakkad, Hitarth Shah, Reema Patel and NishantDoshi, "A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing", ScienceDirect, https://doi.org/10.1016/j.procs.2019.08.097, August 2019.

Manu Suvarna, Ken Shaun Yap, Wentao Yang, Jun Li,Yen Ting Ng and Xiaonan Wang, "Cyber–Physical Production Systems for Data-Driven, Decentralized, and Secure Manufacturing - A Perspective", ScienceDirect, https://doi.org/10.1016/j.eng.2021.04.021, September 2021.