Augmenting Cyber Physical Systems through Data Collection & Machine learning

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

[1*]Department of Information Technology, PSG Polytechnic College, Coimbatore, 641004, Tamil Nadu, India
[2*]Department of Computer Engineer, PSG Polytechnic College, Coimbatore, 641004, Tamil Nadu, India
[3†]Department of Basic Science, PSG Polytechnic College, Coimbatore, 641004, Tamil Nadu, India

E-mail(s) Corresponding authors: harithadeepthibtech@gmail.com; siddiqmoideen07@gmail.com; Contributing author(s): 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 the industries which is 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 amalgamation of Theory of Cybernetics & Mechatronics where Physical Plant i.e., Full-Fledged Hardware component Controlled/Monitored by Computational platform 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 focus on enhancing the production & security of the CPS through Machine learning approach, analysing the digital asserts statistically to set a favourable pay.

Keywords: Industry 4.0, Cyber Physical Systems, Digital Twin, Game Theory, Machine Learning, Simulated Systems, Security Mechanisms

1 Introduction to CPS

Cyber Physical Systems are multidisciplinary systems that conduct feedback control on widely distributed embedded computing systems through combination of communication, computation and control technologies. Modern

CPS are able to realize the real-time, dynamic, safe and reliable collaboration with physical systems represented via embedded system. They are Integral mixture of existing network systems and traditional embedded systems. Where, Physical system data modules collect data by distributed field devices in CPS system, then pass data to the information processing layer as per the complete given tasks and demands of services by information processing technologies such as statistical signal processing, feedback control, data security processing and data uncertainty management. CPS interact with physical system through networks, the end system of CPS is normally traditional centralized tightly coupled embedded computing system, which contains a large number of physical systems composed of intelligent wired/wireless actuators & sensors. The potential benefits of the convergence of 3C technologies for developing next-generation engineered systems are wide ranging and highly transformative via efficient computation, distributed sensing, high-level decision-making algorithms, control over wireless / wired communication networks formal verification technologies and multi-objective optimization; engineered cyber physical systems are in many societal critical domains such as construction, energy, transportation, and medical systems. Scientists and Engineers in this field have deep understanding of system and branches of mechatronics, biology, computer science and chemistry. Physical systems & Technical systems are developed and designed to be more & more reliable, efficient, smart, robust and secure.

With such high notions, the scope of CPS and integration of Cloud computing is about to bring the next big Industrial Revolution, Industry 4.0. The complete factory can be made into digital twin in the cyber space. 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, medical systems, Manufacturing and Traffic safety & control.

2 Industry 4.0

Industry 4.0, the next stage in the organization and control of the entire value stream along the lifecycle of a product. This cycle is based on increasingly individualized customer wishes and ranges from the idea, the order, development, production, and delivery to the end customer through to recycling and related services; which necessitates the consideration of many other issues that may occur in the upcoming new era, including standardization, safety and security, resource efficiency, new social infrastructure, work organization and work design, training, regulatory framework, etc. Technologies of nine aspects that power the transformation of the current industrial production to that of

Industry 4.0 have been identified, which more or less have something to do with CPS. Fundamental here is the availability of all relevant information in real-time through the networking of all instances involved in value creation as well as the ability to derive the best possible value stream from data at all times. Connecting people, objects and systems leads to the creation of dynamic, self-organized, cross-organizational, real-time optimized value networks, which can be optimized according to a range of criteria such as costs, availability and consumption of resources. Industry 4.0 is a collective term for technologies and concepts of value chain organization.

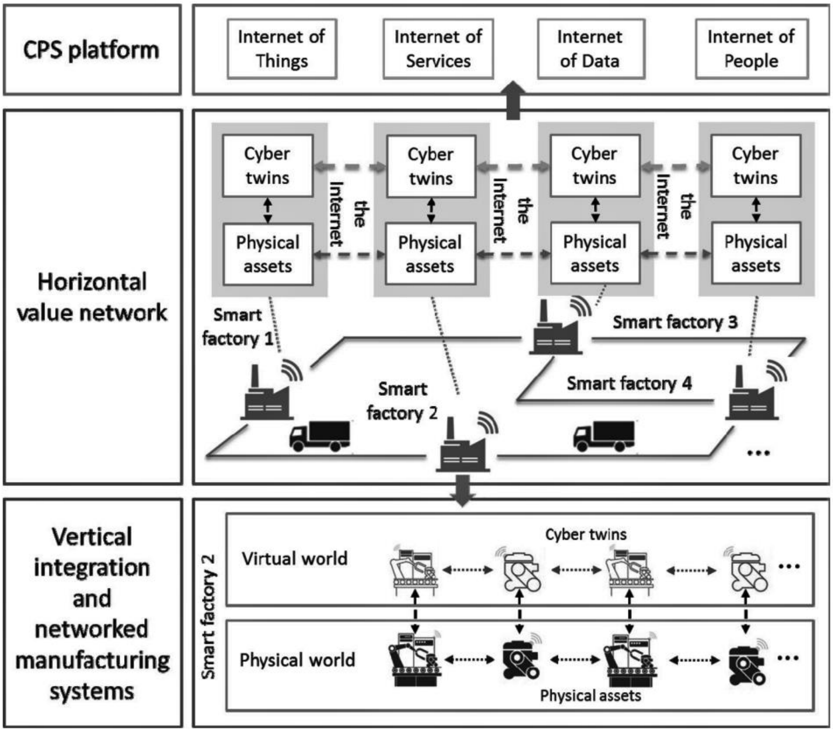


Figure 1: Industry 4.0 Principles

Within the modular structured smart factories of Industry 4.0, CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions. Over the IoT, CPS communicate and cooperate with each other and humans in Realtime. Via the IoS, both internal and cross organizational services are offered and utilized by participants of the value chain. In a smart factory, products and machines communicate with each other, cooperatively driving production. Smart products can refer to objects, devices, and machines that are equipped with sensors, controlled by software and connected to the Internet. Industry 4.0 will give rise to novel CPS platforms geared toward supporting collaborative industrial business processes and the associated business networks.

CPS provide a critical support to the vertical and horizontal system integration. The combination of CPS and the industrial IoT enables the creation of the IoT and IoS. Moreover, the widespread application of CPS means the generation of industrial big data, which requires cloud technology and big data analytics for storage and analysis. The virtual world of CPS consists of a great variety of models of the production facilities, for which simulation can play an important role. Augment reality technology is required for operators to interact with CPS. Additive manufacturing and robots are essential parts of the CPS-based manufacturing systems of Industry 4.0. Within a smart factory, all the physical production elements in the physical world have a cyber twin in the virtual world. The physical and virtual worlds as well as the physical assets and cyber twins in them are seamlessly connected to achieve the global optimization of production within a smart factory. Moreover, within a value network, multiple factories are horizontally integrated, i.e., the physical assets and the cyber twins are, respectively, integrated to enable optimized decision-making across the value network. The integration through the value network will give rise to CPS platforms, within which things, services, "data," and "people" are connected over the Internet.

3 Cloud Manufacturing

Cloud Manufacturing is a new networked manufacturing paradigm that organizes manufacturing resources over networks according to client's needs and requirements to provide a variety of on demand manufacturing services via networks & cloud manufacturing service platforms and a model for enabling convenient, ubiquitous, on-demand network access to a shared pool of configurable manufacturing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In the cloud manufacturing mode, providers can supply their requirements to the platform for requesting services ranging from product design, manufacturing, testing, management, and all other stages of a product life-cycle to their manufacturing resources, which will be transformed into services and then pooled into the cloud manufacturing platform which is an advanced manufacturing business model that focuses on issues that are directly related to manufacturing and pays less attention to issues like urban production and demographic change. A cloud manufacturing platform has a multilayer architecture, including resource layer, virtual resource layer, global service layer, application layer, and interface layer.

The implementation of different layers requires different technologies. IoT, virtualization, and servitization technologies are needed to sense manufacturing resources and transform physical resources into virtual resources in the virtual resource layer. The core technologies for global service layer are cloud computing, service-related technologies and semantic Web technology. In the interface, it is the human–machine interaction technology that plays an important role. The branch relies on Process and Digital Twin Modelling Solutions with modern developments of communication protocols and connection architectures, numerous initiatives have attempted to model physical machines, processes, and results with computational methods.

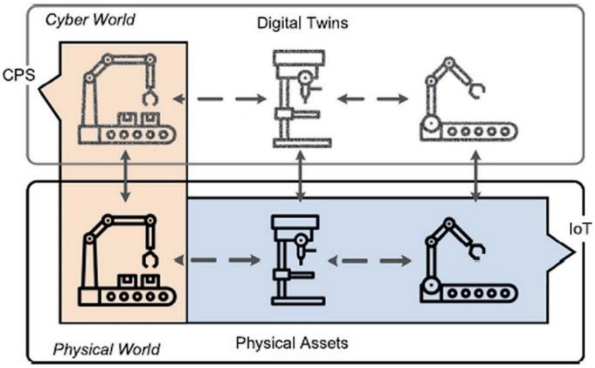


Figure 2: Digital Cloning via CPS implications

These Digital Twins of the physical world have been developed to different extents, each modelling and predicting different areas of the production process. Digital Twin initiatives have been implemented to address a wide variety of modelling scenarios. Simple solutions range from open-loop monitoring of process data while more complex implementations include AI-powered feedback to correct errors in a manufacturing process. The concept of self-control in a decentralized production system is based on the ability of several elements of the system to act and decide autonomously.

3.1 Simulated Production System

A simulation is used to acquire production data of a virtual factory. All of the factory's components like the machine tools, resources and the product workpieces are replicated into a cyberworld. Each machine has a machine type and each product has a product type, so there are different types of virtual products and machines. The work plan, i.e., mimicking the order of operations required to produce a final product in the physical ecosystem. Thus, the product type defines which operations need to be processed sequentially to finish the product, while the machine type defines the operation the machine is capable of the ability of machines of a certain type to perform an operation with specific requirements is encoded into the machine type.

This leads to different process times, even for operations with the same production technology. The required setup times for each operation are included in the resulting processing times. To finish the production of a product, all of its operations need to be processed in order, while each operation takes a certain time.

Many Digital Twin methods integrate models of physical systems with information and result from both computer simulations and CPS connected data. These two sources of information are combined to provide a more accurate method of predicting the system's behaviour and production results. The concept by summarizing the technology needed for a complete Digital Twin to predict microstructure development, residual stresses, and part defects in additive manufacturing. Through the integration of temperature and velocity fields from both numerical simulation and experimental measurements.

Digital Twin model for directed energy deposition in additive manufacturing provides a more accurate cooling rate and temperature gradient prediction than traditional conduction calculations. With more advanced capabilities to link and correlate manufacturing data from different sources, demonstrate a future application for Digital Twin modelling in partial and parallel disassembly sequence planning for products. Implementation of the near real-time analysis for product information, timing information, and upstream downstream events would provide beneficial flexibility and adaptability for assembly planning methods.

3.2 Security Mechanisms

The major security objectives are Confidentiality, Integrity, Availability and Accountability of the ecosystem. Security mechanisms are classified into the following four categories: asset-centric security, network centric security, data-centric security, and user-centric security.

The process of combining security mechanisms poses a complex challenge as it requires a proper combination of security mechanisms at every level further can be integrated into multiple independent layers while achieving multi-objective security. Designers need to be careful while combining security mechanisms, as it may lead to undesired redundancy, or security gaps that make the system vulnerable to attacks.

3.2.1 Assert-Centric Security

Asset-centric security revolves around the device or asset, which are classified into hardware security and software security.

Hardware Security focuses on establishing the validity of physical components. For traceability, liability reasons, counterfeit detection, typically through leveraging randomness that is extrinsic or intrinsic to the part which can be defended through Physical Marking/Watermarking and Crypto processors.

Software Security solutions are aimed at protecting software against attacks such as tampering or causing run-time misbehaviour through invalid inputs that the software erroneously treats as legitimate, later exploits the existing software bugs and vulnerabilities; introduced during the software development cycle which can be defended through Antivirus Software, Tamper-resistant software and Digital watermarking

3.2.2 Network-Centric Security

Aims at providing secure communication among different assets in the network, a major facet for cloud-based design and manufacturing. The security mechanisms are hit through HTTPS, Secure Multicasting, Virtual private networks, Blockchains, Onion routing and Intrusion detection systems.

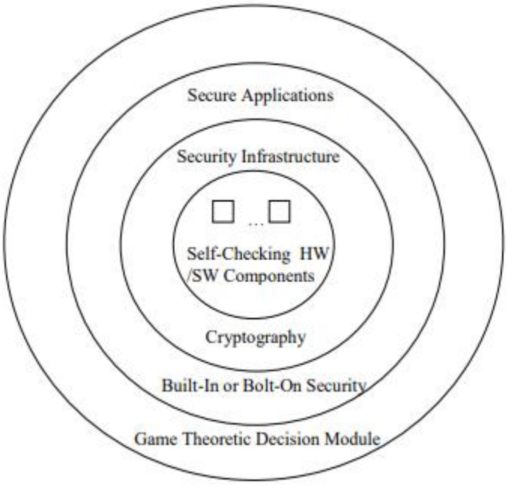

Secure Applications
Security Infrastructure
□ ... □
Self-Checking HW /SW Components
Cryptography
Built-In or Bolt-On Security
Game Theoretic Decision Module

Figure 3: Holistic System Design Approach

3.2.3 Data-Centric Security

Aims at protecting data throughout its lifetime starting from its creation, transmission, updating and storage which can be achieved through Steganography and Encryption model that bags up Symmetric Encryption, Asymmetric encryption, Secret sharing, Secure multiparty computation, Cryptographic hash functions and Digital certification techniques.

3.2.4 User-Centric Security

Advancements in sensor technologies and communication methods have made it possible to monitor product use in real time. Which can be achieved through Authorization, Authentication, Access control and Anonymity. such mechanisms help designers to come up with a security architecture that prevents an attack. A parallel branch, Forensic analysis includes damage estimation, identifying the method of attack and its source.

3.3 Data Collection

Virtual simulation approach is the most efficient way for data collection; the nodes, entities & products of the ecosystem records each & every measurement in every aspect. Since, the workflow of the system is pre-designed in order to mimics the physical world which adapts & synchronises itself with the help of actuators & sensors.

This process 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. Later, mould into advanced structural models.

Adopting Graph Database(NoSQL) approach for Industrial Data Analytics in varied industry-related applications, network operations, object tracking & asset and data management due to its scalability, versatility, efficiency and flexibility. GDBs perfectly improve the data management, include path finding with weighted and time-related path properties, mapping dependencies of various system components to capture potential weak points, and communications between various networked elements. Conversely, query languages are used to extract data, including comparing node properties, traversing the database and subgraph matching.

The data model will consider two types of system entities: dynamic and static. The class of static entities covers testbed setup profiles, which contain testbed components, network interfaces, 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 such as machine status reports, network traffic, and information flows in the testbed. These entities are dynamically added into the data set whose quantities and properties are determined by the measured data. GDBs provide the much-needed structure for storing the data and incorporating a dynamic data model.

4 Industrial Data Analytics

Industrial data analytics play an essential role in achieving the smart factory vision and improving decision-making in various industrial applications. Five main industrial data methodologies are generally studied including highly distributed data ingestion, management, repository, analytics and governance. Industrial analytical approach can avoid down-times, costly failures and tends to effective maintenance decisions.

The industrial data analytics are generally deployed for improving factory operations through improving machinery utilization and predicting production demands, improving product quality by analysing market demands and reducing defective products, and enhancing supply chain efficiency by analysing risk factors and making accurate logistic plans and schedules.

4.1 Visualization

Visualization Helps the us in building a mental map of the production systems considered an art of presenting data. A cognitive transition from one view to the others is a must, visualisation tends to mitigate a different perspective over the systems, latter influencing the decision-making process of the ecosystem through statistical comparison, interactions & workflows.

The overall goal is the optimization of the production process with respect to a diversity of parameters. Although the optimal solution is unknown to users, the presented tool can be used to iteratively improve factory settings. By that, users are enabled to approximate an optimal solution, thereby finding a sufficient solution to gain a certain confidence in their production process.

4.2 Game Theory Implementation

Game Theory is primarily a mathematical framework 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. Game theory depicts the game played between different players and the strategies of each player.

A game can be defined as interaction of different players according to a set of rules. Players may consist of individuals, machines, parties, companies or associations. The results of game theory depend upon behaviour of every other player present in the game and not only the current player.

Due to this reason, this approach is extremely scalable and versatile. The outcome of game theory also depends on the estimated payoff by each player before making decisions, which is a measure of the satisfaction obtained by each player by making that decision. Therefore, the players will perform actions and take decisions that would provide them the maximum payoff.

4.2.1 Game Types

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

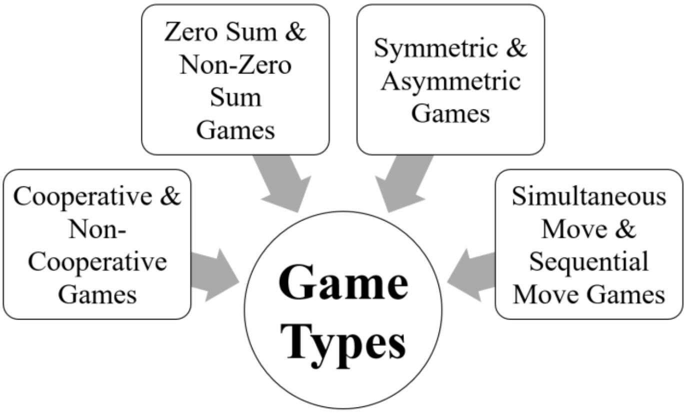
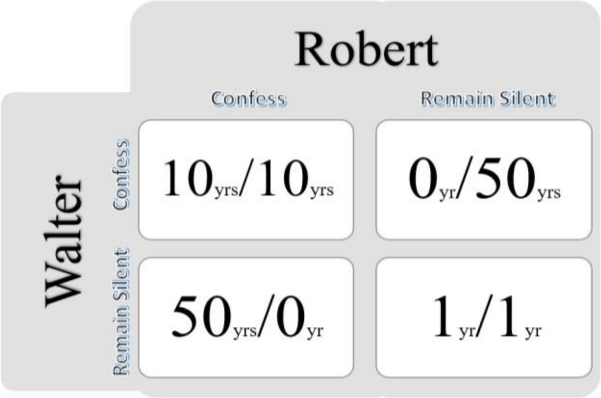

Zero Sum & Non-Zero Sum Games
Symmetric & Asymmetric Games
Cooperative & Non-Cooperative Games
Game Types
Simultaneous Move & Sequential Move Games

Figure 4: Game Theory Types

The prisoner's dilemma is one perfect example; how game analysed in game theory which shows why two completely rational individuals might not cooperate, even if it appears that it is in 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 charge.



		Robert	
		Confess	Remain Silent
Walter	Confess	$10_{\text{yrs}}/10_{\text{yrs}}$	$0_{\text{yr}}/50_{\text{yrs}}$
	Remain Silent	$50_{\text{yrs}}/0_{\text{yr}}$	$1_{\text{yr}}/1_{\text{yr}}$

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 the opportunity either to betray the other by testifying that the other committed the crime or to cooperate with the other by remaining silent. The options offered are:

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

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

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 the best option for both the parties. Individually 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 a partner offers a greater reward than cooperating with them, all purely rational self-interested prisoners will betray the other, meaning the only possible outcome for two purely 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 cooperative behaviour. The label "prisoner's dilemma" may be applied to situations not strictly matching the formal criteria of the classic or iterative games; for instance, those in which two entities could gain important benefits from cooperating or suffer from the failure to do so, but find it difficult or expensive but not necessarily impossible to coordinate their activities.

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

4.2 Machine Learning Approach

Machine learning is a branch of Artificial Intelligence; a system, rather than explicitly following the instructions fed to it. The system moulds itself to accomplish the set target through Supervised, Unsupervised and Reinforcement Training.

Supervised Learning leans on the regression & classification models trained through labelled data inputs which bags up Gradient Descent, Linear Regression, Naive Bayes, Support Vector Machine, Decision Tree and Random Forest techniques.

Unsupervised Learning leans on the association & clustering models trained through unlabelled data inputs which bags up K-means clustering, k-nearest neighbours, Hierarchal clustering, Artificial Neural Networks, Principal Component Analysis and Singular value decomposition techniques.

Reinforcement learning leans on exploitation & exploration models which adapts & interacts with the environment to take decisions in order to maximize reward in a given situation through undefined data inputs.

Engineering changes over the ecosystem might rely on the analytical & predictive report generated by the AI system completely enforced for industrial upgradation, ranging from decision making, production capabilities, scope for improvement, vulnerability check, power consumption to optimal workflow.

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.

5 Conclusion

With high notions of Smart physical & simulated factories, 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 via the collected dataset to give out an accurate predictive model to optimize the production & development of the system. Mixture of Game Theory & ML algorithms boils a robust defence system, securing the backdoors & vulnerable weak points of CPS. Such approach towards Industrialisation breaks the fabric of present production ecosystem to a more resilient & mature factories.

6 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 the human participants performed by any of the authors.

7 Reference

- **Article by DOI**

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.