Future Enterprise as an Intelligent Cyber-Physical System

Ioan Dumitrache *, Simona Iuliana Caramihai **,
Ioan Stefan Sacala*, Mihnea Alexandru Moisescu **, Dragos Constantin Popescu*

** Department of Automatic Control and Systems Engineering, University "Politehnica" of Bucharest, Romania (e-mail: ioan.dumitrache@acse.pub.ro, ioan.sacala@acse.pub.ro).*
*** Department of Automatics and Industrial Informatics, University "Politehnica" of Bucharest, Romania (e-mail: simona.caramihai@aii.pub.ro, mihnea.moisescu@upb.ro).*

Abstract: The appearance of new paradigms such as Cyber-Physical Systems paradigm has led to the appearance of the next industrial revolution. A Cyber- Physical System based Enterprise involves the usage of physical objects, knowledge structured based on workflows, control systems, human integration, systemic data representation and communication processes. The authors propose the concept of Intelligent Cyber Enterprise (ICE) in order to provide a generic architecture enabling the design of complex enterprise systems enhanced with social and technical capabilities. Components of the architecture have to be independent, facilitating the selection of context-oriented behaviors. In order to facilitate the design of ICE components, the authors have proposed a platform for modeling and evaluation.

Keywords: Cyber-Physical Systems, Intelligent Cyber Enterprise

1. INTRODUCTION

Adaptive Industrial Systems Architectures are becoming an important research topic in Cyber Physical Systems and Industry 4.0.

Decision processes in industrial systems are dependent of information processing transfer dealing with issues such as availability and heterogeneity. (Dumitrache et al., 2017)

Cyber-Physical Systems are becoming ubiquitous, pervading every aspect of an individual's daily life, including: Medical care and health, Energy, Transportation and Mobility, Manufacturing, Materials and many other sectors.

Highly connected systems of systems currently employed across numerous industrial and related fields generate vast amounts of data, thus offering new opportunities for the development and implementation of novel enterprise systems. Such systems cannot be modelled as separate subsystems, but as interconnected systems that address not only industrial systems but are tightly connected to economics and society.

Sensors, both physical and virtual (cyber world) are widely used in Cyber-Physical Systems (CPS) oriented enterprise systems. Data provided by these sensors can be analyzed and used both in enterprise level process monitoring systems.

In the following sections the authors analyses the CPS paradigm and propose the concept of Intelligent Cyber Enterprise (ICE). A generic architecture enabling the design of complex enterprise systems enhanced with social and technical capabilities is discussed. Components of the architecture have to be independent, facilitating the selection of context-oriented behaviors. In order to facilitate the design of ICE components, the authors have proposed a platform for modelling and evaluation.

2. COMPLEXITY IN RELATION TO CYBER-PHYSICAL SYSTEM

Cyber-Physical Systems (CPS), as defined by the National Science Foundation represent "engineered systems that are built from and depend upon the synergy of computational and physical components." (CPS, 2013)

Cyber-Physical Systems are concerned mostly with the study of complex systems, addressing both physical and virtual environment components, all sub-systems' interactions, as well as the involved processes and the information processing at both temporal and spatial scales.

CPS models must address the need for a distributed nature of systems, complex interconnections, robustness requirements, and security challenges. Also, CPS must provide capabilities such as adaptive reconfiguration and have the capacity to integrate the human factor in the engineering process.

This new discipline has permanently focused on the interoperability necessity, as defined according to the classical definition, as well as based on the newest interoperability trends in order for every system to be capable to sense and perceive the environment, connecting various sub-systems and, thus becoming a smart system. This approach plays a particularly important role in the future at both design level and implementation phase. Integrating big data analysis and cloud technologies is becoming a necessity because of emerging models for sensing systems. (Dumitrache et al, 2017)

Cyber-Physical Systems are open systems that have emerged at the intersection of physical, social and virtual worlds. To this matter, the next generation of systems will be capable to transform the concept of “smart” by integrating human-machine cooperation and communication (H2M and M2M).

Cyber-Physical Systems must be heterogeneous and widely distributed, at the same time being capable to support system flexibility and re-configurability. Nowadays, Cyber-Physical Systems have become ubiquitous, being more and more present in everyone’s daily life, in various domains, such as: Medical and healthcare, energy, transportation, mobility, manufacturing, etc.

The following conceptualization can facilitate the design of complex systems with the aid of Cyber-Physical Systems principles:

- Conceptual models of system components.
    - Modelling Complex Systems characterized by discrete behaviors of heterogeneous components
- Methodology based design.
    - Application of systemic theories including unification of principles, models, and methodologies
- Functional and control models
    - Compositionality of the components such as physical processes, distributed infrastructure, production systems, information systems and communication networks.
    - Modelling and prediction of system behavior in relation to incomplete or unpredictable information models
- Framework based system integration
    - large-scale integration of the physical and cyber ecosystem
- System architecture
    - adaptive systems, dynamic reconfiguration and systems of systems models
- Network Protocols
    - Modelling the interaction of systems through heterogenous networks
    - robust network control systems
    - network dynamics, cyber security
- Use of specialized languages and modelling tools

3. MODELLING THE COMPONENTS OF AN INTELLIGENT CYBER ENTERPRISE

2.1 Concept definition

The concept of the Intelligent Cyber Enterprise (ICE) must be seen as a complex system, part of a Cyber-Physical System, with social and technical capabilities. The representation of physical processes in the virtual environment is a very important aspect in today’s society in order to be capable of modelling and designing the behavior of a process and thus to be able to integrate hardware-in-the-loop and human-in-the-loop components. (Dumitrache et al, 2013)

Thus, the ICE must be modeled and implemented based on each system’s requirements.

An ICE involves the integration of physical infrastructure, data and data models, communication networks, workflow and process integration, control systems, human in the loop and knowledge integration. An ICE provides integration capabilities as well as interaction and cooperation functions as to facilitate emergent intelligent behavior and systemic adaptation.

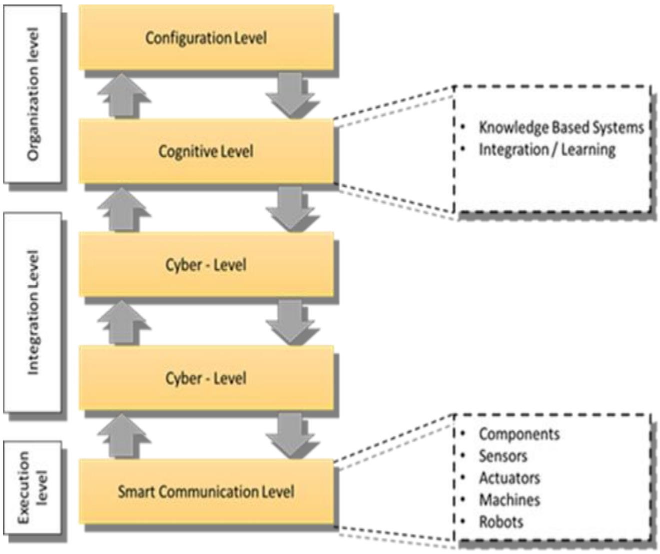


Fig. 1. CPS-based enterprise model.

Integration of intelligent functions in enterprise systems components has been a challenge. Emerging system implementations have already been proposed. The concept of intelligent asset has been defined in relation to physical objects that are able to sense, record and communicate information about themselves and/or their surroundings. The concept has been connected to enterprise model paradigms. (EMF 2016) The concept of intelligent product has been defined and characterized in relation to: monitoring their status and the environment, reaction, and adaptability to change, optimal performance and communication. (Venta, 2007) Another proposed approach involves a Cyber-Physical Toolset designed to optimize energy consumption based on prediction of power consumption in industrial processes (Pease et al., 2018).

The Intelligent Cyber Enterprise must be capable of solving any existing problem and to use the minimum amount of resources. In most situations, the problems that must be solved are addressing the operational level of a business. Seen from the CPS perspective, there is an urgent need to integrate the control loop component within the business process.

Control loops are used in real environments and they are based on specific control algorithms and rules, integrating heterogeneous information and heuristics. A layer abstraction model for the Intelligent Cyber Enterprise, based on the 5C architecture (Ahmadi et al, 2017) is represented in figure 1.

The Intelligent Cyber-Enterprise must be designed in such a way that all components of the architecture have to be independent and must be able to communicate with each other. The exchange, merger and linking of data and information and transfer of knowledge, must be corelated with context-oriented behavior modelling techniques.

One important characteristic that every Intelligent Cyber-Enterprise must rely on is the capability to connect different existing subsystems and implement clusterization techniques in accordance with predefined functions. Functionalities can be structured based on the required specifications, even if they are modified during the process implementation. For instance, manufacturing cells, seen as a component of a manufacturing system, must have the capability to fulfill specific functionalities and to develop various final products.

In conclusion, main functional and structural components of an Intelligent Cyber-Enterprise are focusing on the degree of required autonomy. Thus, based on the degree of intelligence and autonomy of each ICE, we can treat Cyber-Physical Systems ad Autonomous Systems.

2.2 Intelligent Cyber Enterprise Components

The development of an Intelligent Cyber-Enterprise generic architecture can be related to the following concepts:

Perception: data acquired from measurements used for sensing and perception. Thus, the role of perception is to understand the system's behavior;

Optimization: this concept has the main role to develop methods in order to improve the performance of each intelligent system;

Human-Machine collaboration: this characteristic addresses methods, behaviors and information models for increasing productivity and safety. This aspect is connected with the Cyber Worker model that is responsible for identifying the proper performance metrics and methods in order to create an adequate environment for the development of next-generation systems that are capable to integrate human behavior with processes.

Adaptability: this characteristic address system adaptability and reconfigurability capabilities based on data information and decision models

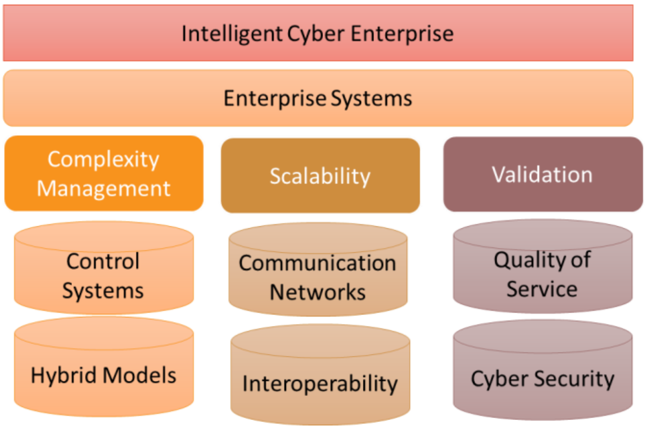


Fig. 2. ICE seen from a multidisciplinary perspective

Distributed vs centralized Intelligence: structural artificial intelligence and machine learning models and tools in order to improve the performance and autonomy of processes and applications.

Collaboration: this characteristic is responsible for developing specific models in order to facilitate coordination between various components of the system, in order to reduce the lack of advanced automation.

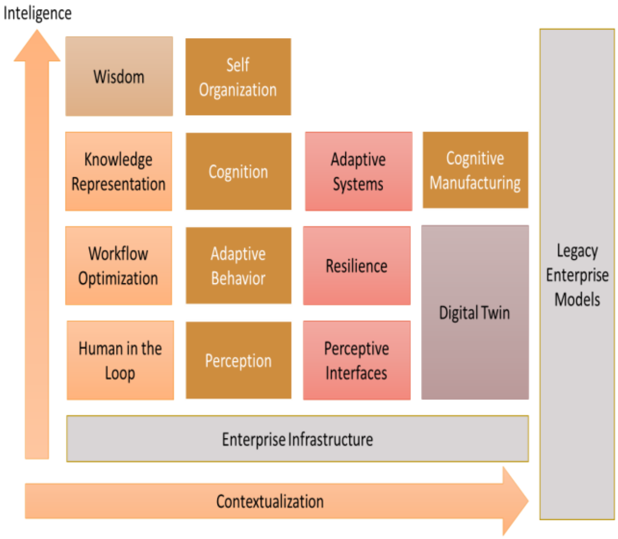


Fig. 3. Main components of a Intelligent Cyber Enterprise Architecture

Based on these characteristics, the Intelligent Cyber-Enterprise must be permanently focused on adopting new technologies in order to become agile and at the same time productive, being capable to collaborate and to interoperate with different smart manufacturing processes and applications, and thus, to be capable to evolve.

To this matter, Intelligent Cyber-Physical Systems (ICPS) represent the next generation of systems, capable to integrate distributed intelligence. Thus, CPS evolve from embedded systems (classic control, smart traffic, advanced control, etc) to complex systems that integrate human-interaction in the application processes (figure 2).

Next generation of systems must be capable to integrate faster applications, to be more precise and robust. As complex systems represent more than just a simple set of subsystems, we must take into account specific challenges and problems, with a direct impact on both industry and society:

- Self-organization capabilities and self-management of the infrastructure;

- Smart factory concept that relies on smart products and processes, based on specific architectures and business models, thus increasing the need of interoperability;

- Advanced integrated models and architectures that must include human-machine interaction, thus creating intelligent environments. This approach requires for a multidisciplinary perspective;

- High impact on all socio-technical layers.

The main key drivers for the development of Cyber-Physical Systems are:

- Capability to integrate smart embedded systems, mobile services and ubiquitous computing;

In conclusion, based on the required characteristics, by integrating bio-inspired methodologies, the next generation of Intelligent Cyber-Enterprise can be modelled as a Bio-Inspired System, and thus, can be treated as an Intelligent Cyber-Socio-Technical System (ICSTS).

- Transforming internet into a platform for business cooperation, resulting in an increased interaction between objects and services;

- Usage of semantic web and integrated services, thus being capable to create knowledge and complex networks;

- Integration of Quality of Services (QoS) and Quailty of Control (QoC) in order to create the proper environment for the evolution of the system.

Sensing enterprise represents a new paradigm that focuses on innovation by integrating Future technologies with sensing capacities. It represents the link between virtual enterprises and all interconnected networks. Also, a sensing enterprise, in order to become part of a smart system, must have the capacity to sense and perceive data from the environment, and thus, have the capability to adapt and to self configure. To this matter, a Product Service Systems Conceptual Framework is proposed in order to facilitate the development of interoperable product systems.

In this context, in order to model a CPS, we must identify all necessary mechanisms that support semantic addressing in order to reuse applications. On the other hand, a middleware layer must be used in order to implement the required sub-systems and their features necessary for control and heterogeneity. Information and knowledge processing must be tightly interconnected with physical processes, in order to better identify behavioral attributes of every process, based on specific procedures.

Integration of physical objects with the communication and control layer will allow the development of complex systems with high capabilities to process information and knowledge.

By embedding cyber capabilities into physical objects will allow the creation of complex scalable networks, capable to operate in real-time (figure 3).

2.2 Intelligent Cyber Enterprise and Future Internet paradigm

Based on these drivers, communication plays a very important role that must be taken into consideration as complex systems require for real-time communication in order to guarantee the bandwidth, throughputs and delays of the network. Thus, communication within every network must allow the formation of control loops. The location in the control loop of the systems and their components represent essential issues caused by the distributed nature of CPS.

Analyzing the characteristics of a Cyber-Physical System from a networking perspective, the following aspects must be highlighted:

- Network Complexity plays an important role within a CPS as it is related to the number of distributed nodes;

- Resource Constraints deal with the integration of embedded devices, as they have various restrictions related to energy efficiency, bandwidth, rate through, etc;

- Hybrid Traffic and Massive Data are directly dependent on the number of sensor and nodes that exist in a network and the amount of required and used data;

- Uncertainty is a component that results from the existing sensor measurement errors, computational model errors, software errors and number of changes that appear in a network;

- Structural and behavioral complexities are mostly related to modelling, analysis, design and implementation of CPS.

After the appearance of the Future Internet paradigm, systems have increased in complexity and thus, the necessity to cooperate has increased, as well as the complexity. Thus, we must put an emphasize on every system and the involved sub-systems in order to identify, implement and validate each required functionality. One possible solution can be based on the Model-based Cyber-Physical Systems.

Together with the development of internet-oriented paradigms, various computing based models have been proposed in order to optimize “smart” applications and to validate their functionalities in close correlation with the geographical distribution of the IoT devices and systems, to the detriment of outsourcing computations. Such architecture has been proposed and it includes an Edge / Fog / Cloud

Monitoring System and a Capillary Container Orchestrator, capable to manage multiple dynamic IoT environments. In such a system, the Edge node can be overloaded various times based on the increase in the workload.

Another crucial component of Future Internet Systems is related to security and trust. In order to address this aspect, next generation of systems must rely on various dispersed resources and services. A Trust Management architecture based on blockchain-based Smart Contract (SCs) can represent a reference point. Correlated with these concepts, new Enterprise models have emerged, integrating various paradigms, such as Factories of the Future (FoF) paradigm.

The Factories of the Future paradigm represents the future of enterprises and it relies mostly on collaboration and connectivity at different business levels, human-to-machine interaction, human in the loop and machine-to-machine interaction, in order to allow for the development of complex, interconnected networks of various stakeholders, such as suppliers, transporters and customers.

On the other hand, distributed manufacturing systems, being based on optimization models, represent an important component of the FoF. One existing model uses an optimization algorithm and is based on three heuristic methods. Material Flow Analysis is another important aspect of the FoF that relies on optimization algorithms in the production processes.

4. INTELLIGENT CYBER ENTERPRISE PLATFORM FOR KNOWLEDGE MODELING AND EVALUATION

In pursuance of materializing and validating the proposed Intelligent Cyber Enterprise architecture, flexible modelling and conception tools that can encompass a diverse knowledge representation, which is complete, precise and yet sparse and uncertain, are required. As a first step towards this goal, we have developed a flexible modelling software platform aimed at describing the structure and the behaviour of complex systems.

The backbone of the platform is an evolved version of the relational modelling formalism (Bubnicki, 2005), which is further developed to describe networks of models, crisp numerical information and statistical uncertainties. Each model is an abstraction of a specific real (hardware) or virtual (software) entity, for which the behaviour is described using a unified language, combining logical truth facts, numerical properties and probabilities. In such a way, multiple aspects of the emergent composition of a vast network of interacting entities can be analyzed throughout different contexts and scenarios. For instance, in a complex supply chain workflow, the outcome of a specific event (e.g. a transport truck has an accident or is a power break in one of the manufacturing plants) can be assessed in terms of different quality metrics (e.g. time delay, cost increase, profit dynamics etc.).

The proposed platform facilitates an intuitive understanding of the phenomena and allows for a formal representation and development of the appropriate tools in order to optimize, control, schedule and synchronize various concurrent workflows. In addition to the uncertainties, the proposed unified modelling language can also manage the heterogeneity of the complex systems. Seeking to optimally address all these modelling challenges, the theoretical formalism developed and the language defined are required to provide dedicated mechanisms for integrating all low-level and local views which, usually, belong to different actors of different backgrounds and objectives or which are focused towards entities having different natures (hardware systems, physical processes, software algorithms, control strategies, technological data, procedures, constraints etc.). All these aspects call for an approach addressing the following two objectives:

- integrating a unified domain-independent modelling language similar to human reasoning;
- integrating a formalism that provides specific tools for simultaneously approaching modelling at different granularity levels

Throughout the process of building a model, the following phases have to be performed:

1. The context has to be divided into multiple entities which act as atomic models inside the platform. Each model showcases a specific element: system, equipment, workflow, component, location, commercial entity etc. This task requires the user to perform the following actions: decomposition, identification and clustering matching.
2. The interface of each entity has to be defined subsequently. Each model will have input, internal and output parameters.
3. The external links between the models have to be identified and analyzed. This can be based on a set of correlation analyses and can be seen as an inter-relational capture of the entities involved. In real life, all these links can represent: inter-conditions, correlations, product, and component fluxes, information fluxes
4. In the structural inference analysis phase the input – output model correlation is defined. This is based directly on user knowledge and can be seen as an intra-relational capture of an entity.
5. The logical inference has to be defined in order to have a qualitative overview of the behavior. This is done using uncertain logical rules which combine all or part of the parameters contained.
6. The qualitative analysis can be further extended in order to achieve a quantitative overview by treating some of the parameters as numerical ones and, in this way, obtaining the means to define and propagate uncertain information through the network.

Fig. 4 and Fig. 5 an example of how the platform prototype can be used for supply chain modeling, scheduling and cost optimization. The case study implements a supply chain example in which the final assembly can be done in multiple factories using components from different suppliers for cars which have to be delivered to multiple clients.

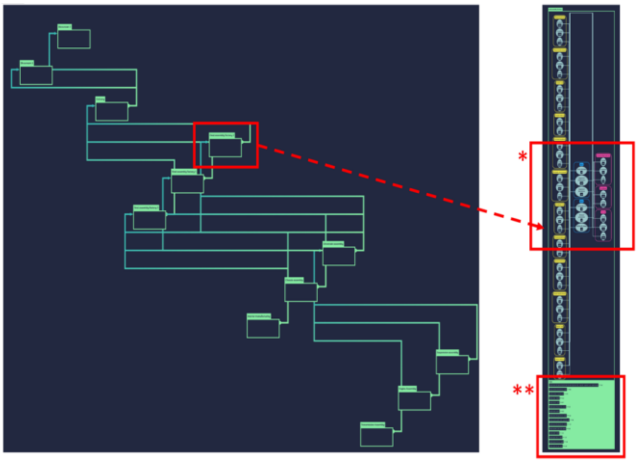
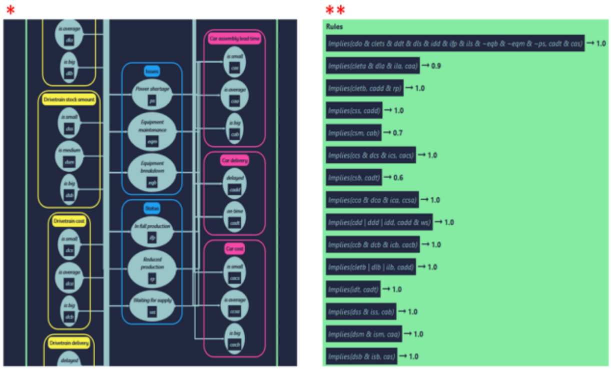


Fig. 4. Car manufacturing supply chain modelling



```
Rules
Implies(cdo & clets & ddt & dls & idd & ifp & ils & ~eqb & ~eqm & ~ps, cadt & cas) → 1.0
Implies(cleta & dla & ila, cao) → 0.9
Implies(cletb, cadd & rp) → 1.0
Implies(css, cadd) → 1.0
Implies(csm, cab) → 0.7
Implies(ccs & dcs & ics, cacs) → 1.0
Implies(csb, cadt) → 0.6
Implies(cca & dca & ica, ccsa) → 1.0
Implies(cdd | ddd | idd, cadd & ws) → 1.0
Implies(ccb & dcb & icb, cacb) → 1.0
Implies(cletb | dlb | ilb, cadd) → 1.0
Implies(idt, cadt) → 1.0
Implies(dss & iss, cab) → 1.0
Implies(dsm & ism, cao) → 1.0
Implies(dsb & isb, cas) → 1.0
```

Fig. 5. Model detail where input, internal and output parameters are displayed and behaviour rules are defined

6. CONCLUSIONS

A Generic Architecture for Future Enterprise Systems needs to address system characteristics such as availability, composability, compositionality and heterogeneity. In this context, the authors have analysed and proposed an architecture for Intelligent Cyber Enterprise. Capabilities related to the architecture include, but not limit to: semantic concepts for the description of system components, self – organization models, human – machine interactions and cognition.

Intelligent Cyber Enterprise can be implemented by integrating the most important results of the research in Cyber-Physical Systems, results integrated from a multidisciplinary perspective.

REFERENCES

Ahmadi, A., Cherifi, C., Cheutet, V. and Ouzrout, Y., 2017, December. A review of CPS 5 components architecture for manufacturing based on standards. In 2017 11th International Conference on Software, Knowledge, Information Management and Applications (SKIMA) (pp. 1-6). IEEE.

Bubnicki, Zdzislaw. Modern control theory. Berlin: Springer, 2005.

Cyber-Physical Systems, PROGRAM SOLICITATION NSF 13-502, National Science Foundation, 2013 https://www.nsf.gov/pubs/2013/nsf13502/nsf13502.htm

Dumitrache, Ioan, Simona Iuliana Caramihai, and Aurelian Stanescu. "From mass production to intelligent cyber-enterprise." In 2013 19th International Conference on Control Systems and Computer Science, pp. 399-404. IEEE, 2013.

Dumitrache, I. and Caramihai, S.I., 2014. Intelligent cyber-enterprise in the production context. IFAC Proceedings Volumes, 47(3), pp.821-826.

Dumitrache, Ioan, Simona Iuliana Caramihai, Ioan Stefan Sacala, and Mihnea Alexandru Moisescu. "A cyber physical systems approach for agricultural enterprise and sustainable agriculture." In 2017 21st International Conference on Control Systems and Computer Science (CSCS), pp. 477-484. IEEE, 2017.

EMF, 2016 "Intelligent Assets: Unlocking the Circular Economy Potential", Ellen MacArthur Foundation (EMF) Report

Lee, Jay, Behrad Bagheri, and Hung-An Kao. "A cyber-physical systems architecture for industry 4.0-based manufacturing systems." Manufacturing letters 3 (2015): 18-23.

Leitão, Paulo, Armando Walter Colombo, and Stamatis Karnouskos. "Industrial automation based on cyber-physical systems technologies: Prototype implementations and challenges." Computers in Industry 81 (2016): 11-25.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., Sauer, O., Schuh, G., Sihn, W. and Ueda, K., 2016. Cyber-physical systems in manufacturing. Cirp Annals, 65(2), pp.621-641.

Pease, S.G., Trueman, R., Davies, C., Grosberg, J., Yau, K.H., Kaur, N., Conway, P. and West, A., 2018. An intelligent real-time cyber-physical toolset for energy and process prediction and optimisation in the future industrial Internet of Things. Future Generation Computer Systems, 79, pp.815-829.

Venta O.¨, Intelligent products and systems, Technical Report, VTT, 2007

Vladareanu, V., Dumitrache, I., Vladareanu, L., Sacala, I. S., Tont, G., & Moisescu, M. A. (2015). Versatile intelligent portable robot control platform based on cyber physical systems principles. Studies in Informatics and Control, 24(4), 409-418.

Wang, L., Törngren, M. and Onori, M., 2015. Current status and advancement of cyber-physical systems in manufacturing. Journal of Manufacturing Systems, 37, pp.517-527.