Sensors & Transducers, Vol. 249, Issue 2, February 2021, pp. 54-64

Sensors & Transducers

Published by IFSA Publishing, S. L., 2021
http://www.sensorsportal.com

AI-assisted Distributed Applications at Edge for Industrial Field Autonomous Systems

[1,*] Yannick FOURASTIER, [2] Claude BARON, [3] Hakima CHAOUCHI, [4] Carsten THOMAS, [5] Thomas BOURGEAU, [6] Jean-Paul SMET, [7] Viktor YEHOROV and [8] Philippe ESTEBAN

[1] CodEUrope SAS, 244 Route de Seysses, 3100 Toulouse, France
[2] Université Toulouse, INSA, LAAS-CNRS, ISAE-Supaéro, 7 Av. Colonel Roche, 31200 France
[3] Institut Polytechnique de Paris, Telecom SudParis, 9, rue Charles Fourier, 91011, Evry, France
[4] HTW Berlin, Treskowalee 8, 10318, Berlin, Germany
[5] KB Digital, 1291 Commugny, Switzerland
[6] Nexedi GmbH, Technology Centre Munich, Agnes-Pockels-Bogen 1, 80992 München, Germany
[7] University of Odessa, Lab Mironaft, Kanatna St, 112-114, 65000 Odessa, Ukraine
[8] Université de Toulouse III, LAAS-CNRS, 7 Av. Colonel Roche, 31200 Toulouse, France
E-mail: yannick.fourastier@codeurope.eu

Received: 7 October 2020 /Accepted: 30 November 2020 /Published: 28 February 2021

Abstract: Complex industrial systems are increasingly software-defined, rapidly evolving into autonomous, self-adaptive processing at industrial fields. They are constituting worlds of things, wherein the internet of things is heavily developing with local semantic features. Also, artificial intelligence technologies are spreading fast in the industrial context, improving the operations efficiency. However, Edge computing systems involving artificial intelligence must also continuously ensure reliable and safe operations. This paper assesses the state of the art of cognitive technologies with their relevance for artificial intelligence implementation in industrial cyber-physical systems. It then introduces a state of research on artificial intelligence safety assurance practices. Implementation through three use cases at the software stack is illustrated with a virtual operating system that operates the data space in the industrial layout. More precisely, the industrial development is illustrated with a real case of swarm computing for advanced robotics powered with SlapOS[1]. Although still at an early stage, it shows experimentally how Edge operating systems are evolving fast as a kind of AI intensive software.

Keywords: Artificial intelligence, Cyber-physical system, Industrial edge, Swarm processing, Virtual operating system, Digital twin, Safety of intended functionality.

1. Introduction

Digitization is deploying fast in the industrial field. Complex industrial systems are increasingly software defined, as it also follows the digitization by softwarisation wave. They're rapidly evolving into autonomous and to some extent, self-adaptive processing relying on the artificial intelligence (AI)

[1] SlapOS is a general purpose overlay operating system for distributed POSIX infrastructures (Linux, xBSD, etc.) with a strong focus on service management. It is published as Free Software under fairly permissive licensing

algorithms developments and the fast and reliable distributed communication technologies offered. In the context of this paper, the "cognitive technologies" expression groups those technologies which gather intelligence from their data generation, and proceed them thanks to artificial intelligence techniques, in order to produce a learnt model that can autonomously outcome a result. From a similar approach, they may articulate some programmable mechanisms to self-adapt also to their context. These cognitive technologies are spreading fast at the so-called industrial edge; the processing connected nodes that controls the industrial Cyber Physical Systems (CPS). While enabling these systems with adaptive functioning, the deployed cognitive techniques are possibly self-evolving too in order to optimize the performance efficiency of such cyber-physical systems. When doing that, they also carry concerns, which can even turn into issues, regarding the safety assurance and also the performing stability. Our work addresses AI-assisted distributed applications at Edge for autonomous cyber-physical systems which are operating in the industrial field with dependable performance and critical safety. This paper is an extended version of our ASPAI' 2020 one [1].

This paper summarizes first the industrial related cognitive technologies; also called Industrial Internet of Things (IIoT). The industrial internet of things composes a virtual platform in the field. Such a world of industrial objects liaises semantically each with all, and also with distributed software codes and patterns. As a semantic web of things, it is sometimes named as WoT in the literature. It composes an industrial data space with methods, resulting with a software technology producing a digital twin. Standardized by the ISO, the industrial IoT as well as the digital twin, interact with the business orchestration, such as the Manufacturing Execution System (MES) in the production context, the signalling systems at railway, the urban traffic regulation at the smart city, or the building control and automation, etc. Such a digitized industrial platform brings more automatic decisions locally and actions; meaning as close as possible to the CPS. We study a software stack, namely SlapOS, able to virtually power safely the autonomous intelligent industrial system with Edge Computing. It is to build up a technology able to virtually power and control safely the autonomous industrial Cyber Physical Systems (ACPS) with distributed Edge embedded AI.

The Edge embedded AI indeed supports local decisions and actions which often influence safety critical operations at field level. This paper discusses the safety assurance practices for the design and development of dependable cyber-physical systems which are AI assisted.

The paper illustrates three actual implementations of industrial cases following our described vision. One aims at wind turbine health monitoring, the other is a virtualized control (virtual PLCs' interconnecting IoTs' at a production process), and the third is about guidance and navigation of a drone swarm.

2. Cognitive Technologies in the Industrial Field

Different sorts of algorithms support signal analysis, information characterization, memorizing and retrieving, processes automation, anomaly detection, operations predictions, and decision making. They can also emerge models from some perceived situation. This latter is factually a time series of input data, which produces the machine to learn to produce a model with some probability of correctness. What a supervisor will validate or not, then the machine will progress faster its learning.

In this section, cognitive technologies and their relevance for artificial intelligence implementation in the industrial field are succinctly introduced. Distinguishing from genetic algorithms (GA) and robotized process automation (RPA), we structure four families of techniques: machine learning (ML), deep neural networks (DNN), hybrid neural networks (HNN), and generative adversarial networks (GAN).

2.1. Automation Techniques: RPA

Robotized process automation (RPA) [2] mimics actions in sequences that are usually performed by a human operator. RPA uses structured data and kind of wired logic to function. Contrary to AI functions that use unstructured input data and develop its own logic to produce wished results. RPA in the industrial field, relates to the replacement of legacy hardwired automation by software executing on a generic processing platform.

2.2. Evolutionary Computing: Genetic Algorithms (GA)

In decision making processes, Genetic algorithms (GA) [3] develop heuristics and meta-heuristics from candidate solutions, to look for a best fit solution. GAs' functions on natural selection principles, with derivating secondary solutions from the candidates characteristics, mutated, altered, recombined or crossed. Proceeding iteratively, new generations of candidate solutions are produced. A fitness function evaluates the new set against the problem to solve. GA's are well fitting optimization problems, also to sort best decisions for specific situations as they are often in the industrial field, especially in complex process chains.

2.3. Machine Learning (ML)

Machine learning is essentially a form of applied statistics, at which complicated functions estimations are emphasized, while the importance of proving confidence intervals around these functions is decreased [4]. ML is driven from two main approaches, frequentist estimators and Bayesian inferences. Learning algorithms can be divided into supervised and unsupervised categories [5], in order to develop performant generalization abilities. These techniques are useful for pattern recognition applications, predictive models, and also model prediction with deep learning (signal processing, time series, speech recognition, objects, situations, etc.).

2.4. Artificial Neural Networks (ANN)

ANN are densely interconnected adaptive processing units (perceptrons) [6]. They enable fine-grain parallel computation of non-linear static or dynamic systems. ANN can be considered as parallel computational models. A major feature of such technique is its adaptive nature. Traditional programming is replaced with learning by example prior to solve problems. Artificial neural network results are linkable to applications at which there are little or incomplete data to solve a problem, but available training data. Also, ANNs' are relevant for function approximation, associative memory, non-linear system modeling, combination, optimization, information clustering, forecasting and prediction, and control.

2.5. Deep Neural Networks (DNN)

Multilayer perceptrons (MLP) implement feedforward neural networks. They aim to approximate a function with a mapping y=f(x;), and to record the resulting value for the best approximation [5]. With data flowing through the assessed function from x, through intermediate computations in charge of defining this function, and finally to output y, these learning models are feedforward. There aren't feedback connections, unless the implementation of recurrent neural networks with back propagation. While ones are efficient for image or complex analysis, the others power many natural language applications. Architecturing ML techniques with MLP, deep neural networks (DNN) have considerably simplified the modeling process that was a painful bottleneck to processing complex heterogeneous data. By incorporating both, feature engineering and conceptual learning, DNN directly processes raw data then generates the final, conclusive results [7]. Such techniques have better capability to generalize unseen combinations of features when solving large scale regression, classification problems, etc. Their applications can be answer selection, recommender system, predictions.

2.6. Hybrid Neural Networks (HNN)

ANNs' requires previously defined architecture for the neural net. Supervised, unsupervised or reinforcement learning are then usually achieved by adjusting the connection weights iteratively using a gradient descent-based optimization algorithm [8]. Design results difficult since the sensitivity to initial conditions of training and local character, leads to hybrid connectionist and symbolic computation at ANN and hidden layers behaviour weighting [6].

At hybrid neural networks (HNN), symbolic representations (probability distributions over the kinds of data encountered) provide explicit, fast initial coding, direct control, dynamic variable binding and knowledge abstraction, while the architecture (MLPs' net) provides robust learning, generalization to similar input, and fault-tolerant processing. HNN results with high adaptability and resistance to external noise, what's relevant for monitoring models, and the forecasting of computer networks states, which edge processing at industrial edge typically [9].

2.7. Adversarial Learning, Generative Nets (GAN)

GANs' develop beyond HNN to generate more efficient ANN models (architecture and embedded symbolic, which hyperparameters). A generative model somehow collaborates with a discriminative one, evaluating generated candidates. In control theory, adversarial learning based on neural nets can train robust controllers in a game theoretic sense, by alternating the iterations between a minimizer policy, the controller, and a maximizer one, the disturbance. Adversarial cognitive techniques are relevant to orchestrate the resilience in control systems.

2.8. Usages

Production systems automation is progressing since industry exists, as far as pure automation is considered one of the key factors for implementing cost effective production. In such a paradigm, the less the production system requires human energy, the more is presumably effective. The last fifty years of literature in industry engineering techniques have investigated that lead times and quality levels may exceed by far those of human workers. Such a machine-oriented assertion also leads to the artificial cognition principle in production systems and to function them software-defined. Fig. 1 summarizes the cognitive system architecture introduced by Bannat and *et al.*, with [10].

Such a cognitive cyber-physical architecture is concerned with its performance specifics which relates to processes timing, planning and coordination, including accordingly to discrete events. Hence, to some extent, the system components are often real time constrained. Additionally, they can have to deal with human safety and also environmental considerations. Therefore, they have to mitigate hazards accordingly.

With cognitive techniques integrated into the software defined industrial architecture, they are required to fulfil highly demanding requirements as other system components, in particular the safety ones. The Table 1 below proposes a summary of the AI techniques and the industrial safety. Although obviously depending on their allocation in the system and this latter's business specifics, the adherence of the AI techniques to real time constraints in the industrial system depends on their usage and purpose (what action in the CPS powering the industrial field).

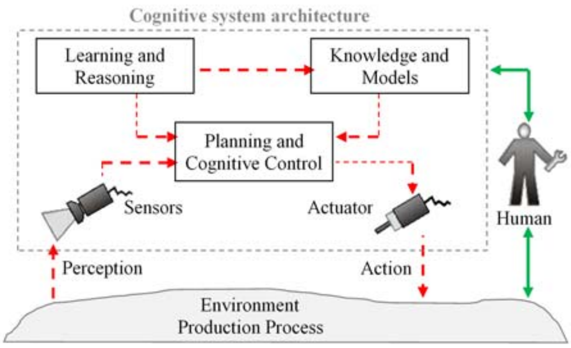

Fig. 1. Cognitive system architecture with closed perception-action loop [10].

3. Virtually Distributed Computing at Industrial Field

The concept of digital twins is at the limit of artificial intelligence technologies. A digital twin reproduces identically, but only digitally, the functioning of a real physical system. By extracting perceived behaviour from physical functioning, this technology produces a Model Order Reduction (MOR). It enables multiple numerical simulations to be carried out, in particular, in order to decide before any changes are made, which configuration variations to apply.

By working as close as possible to the physical system, distributed in the edge computing layer, the software does not necessarily need a computer to carry out numerical simulations, which are very costly in terms of computing time when all the layers are dissociated. In fact, it can give results in real time. This much shorter calculation time makes it possible to predict the behaviour of a system and control it in real time. Such an implementation between the digital twin and its real system constitutes "closed-loop digital twins". Reproducing the functioning of the real object, it also combines AI techniques to anticipate certain actions, and adjust certain behaviours of the digital twin. Visioning mechanisms allows human agents to interact or act remotely on real objects.

The ISO/IEC30141 [11] standardized the industrial internet of things into six domains as shown with Fig. 2: user, operations and management, application and services, access and communication, sensing and controlling, and physical entity.

Table 1. Cognitive techniques and industrial safety.

Cognitive techniques	Industrial Field action	Real Time adherence / safety
RPA	Automation of repetitive at data flows processing	Slack adherence
GA	Decision making Optimal solution computing	Slack adherence
ML	Predicting from time series or pattern sets, involved in machine self-deciding	Can be relevant
ANN	Problem solving Classification and sorting Function approximation Incomplete data sets linearizing	Can be relevant
DNN	Sorting Large scale regression Identification of combinations Pattern recognition Problems classification Generalization	Can be relevant depending on the architecture of the powered AI
HNN	Monitoring Forecasting	Can be tight adherence
GAN	Robust controllers training Control systems resilience	Tight adherence

Such a standardized IoT connects cyber-physical systems to remote processing and storage resources made available in the network. The main challenge being to ensure reliability, safety and security of these connected cyber-physical systems, bringing those processing and storage resources closer to these systems, is the way to go; it is named Edge computing or fog by opposition to the cloud, that is central.

Edge Computing moves the industrial internet of things as virtually distributed swarm computing, in near proximity to the field where CPS are orchestrated, while performing their tasks. In addition, AI algorithms perform better, they allow us to build cognitive techniques at the edge in order to better control, predict and automate decisions locally, thus requiring less human intervention. Fig. 3 illustrates possible placements of cognitive technologies closer to the industrial field. The industrial cloud is beyond the field digital fog where edge embedded cognitive algorithms are running. This cognitive capacity is increasing fast, following the 4.0 digitization pace.

This distributed Edge Computing offers both CPS control and data collection, storage and processing. It requires a highly reliable operating system and a CPS functioning safety, by design architecture. While data processing and storage capacities are increasing at such a fog ("digital cloud" at the edge), this one can also provide available resources opportunistically. Assisted with artificial intelligence techniques, the Edge virtual operating system organizes dynamically the sharing of resources to implement concretely a fog. It groups pseudo-available resources for functions or services to execute virtually at the cyber-physical system or close neighbourhood.

In order to build successfully this solution, and ensure reliable and safe behavior of the overall connected and cognitive based systems, it is necessary:

1. To connect the right physical objects to the network in line with the semantic web of IoTs'.

2. To build a correct representation of the physical objects using the virtual objects of that semantic web. Then these virtual objects bind to their physical platform.

3. To design and use efficient and well architectured distributed processing.

4. To build a robust, resilient, and secure, data persistence management.

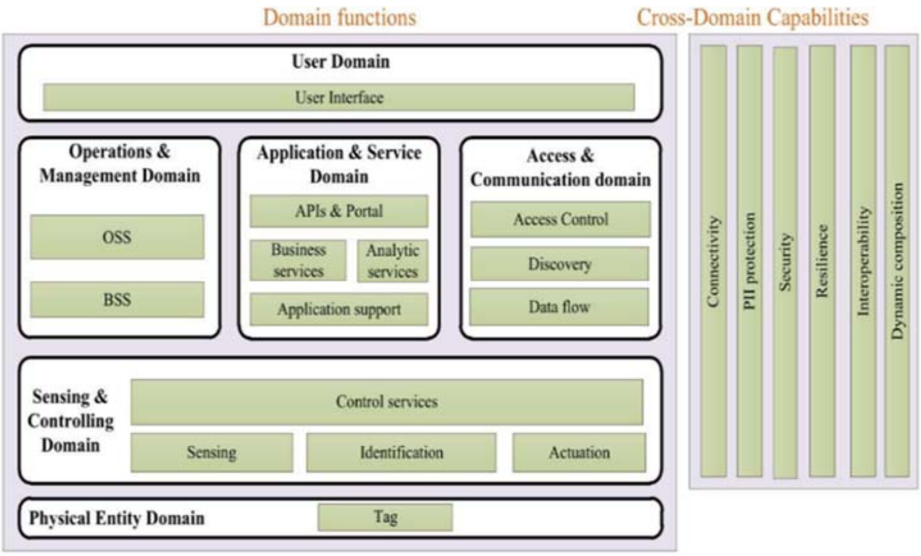

Fig. 2. ISO/IEC 30141 functional view [11].

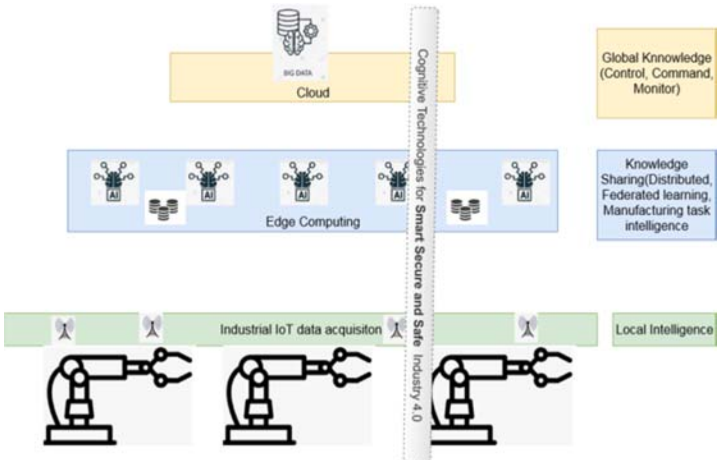

Fig. 3. IIoT and Cognitive technologies over the edge and the cloud in Future Smart Secure and Safe (3S) Industry 4.0 systems.

3.1. The World of Things with Multi-level Intelligence: the IoT 2.0

The internet of things connecting devices (sensors, actuators), enables software-defined command and control to interact with the physical world. That logical internetworking of things, forms the IoT 1.0, is quite the same as the general Internet has been in the late 90s'. With the technology heterogeneity challenging the machine-to-machine connectivity, the industrial internet of things (IIoT) has provided a software abstraction layer. That IIoT ended up by building a multilevel connectivity from the device, then to some gateway, up to the cloud to process the IoT device collected data.

With the fast growing of AI algorithms, IoT data analytics is getting us to a second phase named IoT 2.0. Building intelligent objects, able to interact autonomously with each other, and not anymore only connected objects, is a real challenge. IoT 2.0 is more about interfacing between machines and humans in a very intuitive fashion. It is about using AI intensively to understand people in the industrial field, to run autonomously processes with no human intervention. It is about getting these intelligent objects to become collaborators of humans (e.g. the cobots), multimodal with human interactions, including voice and gestures.

Combining connected things with virtual experiences, made possible by virtual reality (VR) and augmented (AR), has opened up new possibilities in the industrial cognitive system. With VR, the users are entirely removed from their real settings, and can interact with the digital twin through immersive experience. This software generated technology, re-creates the running scenario, and cancels the need to access the physical process. With AR, the user's current environment can be digitally overplayed with image, 3D model, sound, touch or haptic experience, and smell.

3.2. Distributed Physical and Virtual Objects Brings Semantic: Digital Twins

Digital twin is nothing but a virtual replica of an actual physical asset [13]. Back in the 1960s', NASA scientists created a replica of the physical asset on the ground and built a technology to match the processes and systems in space. Even though they were not directly connected with some data link, but the parameters manually propagated from one to the other, they were kind an ancestor of digital twins.

The ISO23247 [14] standardizes the digital twin reference architecture and technology. Its framework is layered on the IEC/ISO30141 one, as illustrated with Fig. 4, although the schema groups the six domains of IoT into four blocks at the digital twin framework. The six domains are organized in a way they can distribute in any Edge computing architecture, with cloud uplink or not, depending on the needs of computation.

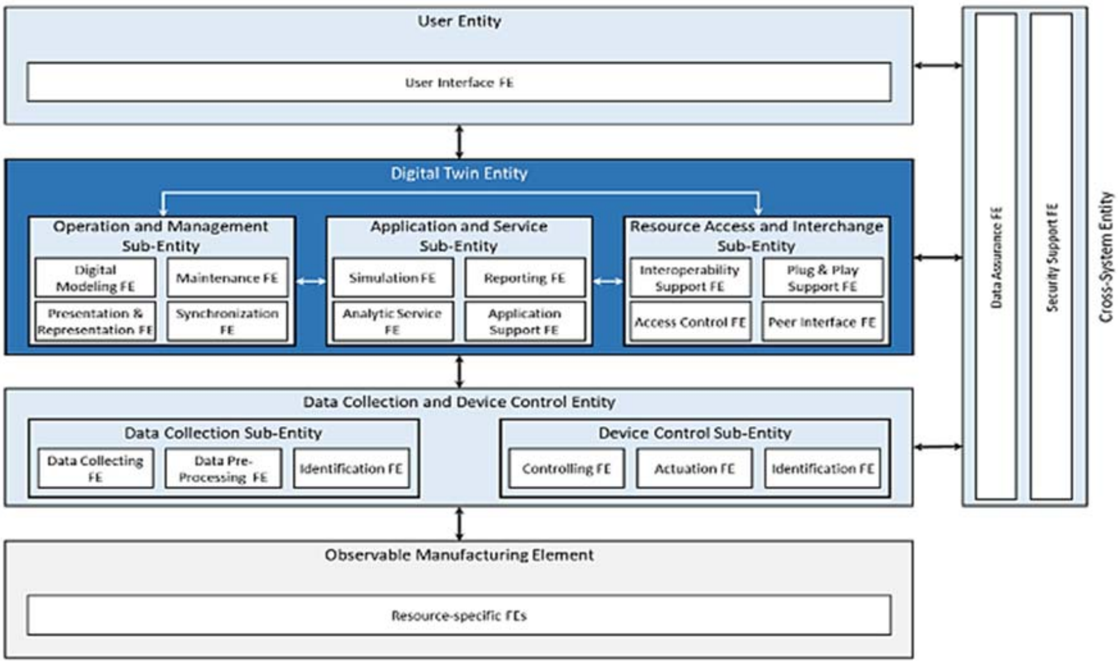

Fig. 4. Digital Twin framework ISO23247 [14].

3.3. Distributed Intelligent Processing

A major challenge of that standardized digital twin [14] is to really take advantage of the IoT technology in industrial decisions. IoT generates a myriad of data by the possibly huge amount of connected devices, including sensors and actuators, that are usually aggregated and stored at fog virtual platform, and up centrally to the cloud.

The interaction and the management of IoT devices has enabled new service opportunities including predictive maintenance, continuous monitoring of the parts that are more subjected to degradation and ageing, scheduling and remote running of maintenance interventions, product quality prediction and autonomous adjustment for correction or automatic tagging of non-quality.

Standardized digital twin (in fact most of previous IIoTs') exhibits several characteristics that can be sector specific (e.g. manufacturing, smart cities, smart buildings, etc.) in terms of communication bandwidth, real time adherence, latency improvements, robust connectivity, together with limited costs on large scale deployment scenarios. An integrated infrastructure is deployed to collect information from heterogeneous sensors, to process it in the cloudlets (herein kind of edge clouds), to transmit to the cloud only what complies with the digital twin policies and applied parameters to update the related in the form of a closed-loop system. Edge computing results to be a technology of distributed cloud that moves the processing functionality from centralized datacenters, to the edge of the network, in a virtualized field.

Generally speaking, such layout virtualization migrates core capabilities such as networking, computing, storage, and applications closer to the devices, and in particular to the IoT endpoints. There are already interesting examples in the related literature [14] about intelligent services close to manufacturing units, e.g., to meet key requirements such as agile connection, data analytics via edge nodes, highly responsive cloud services, personalized enforcement of privacy policy strategies.

In such a way, the distribution of the digital twins over cloudlets that architecture the industrial data space, composes hybrid twins which compose distributed intelligent processing with the industrial IoT, Edge nodes, and digital twin enabled services running at cloud as illustrated with Fig. 5.

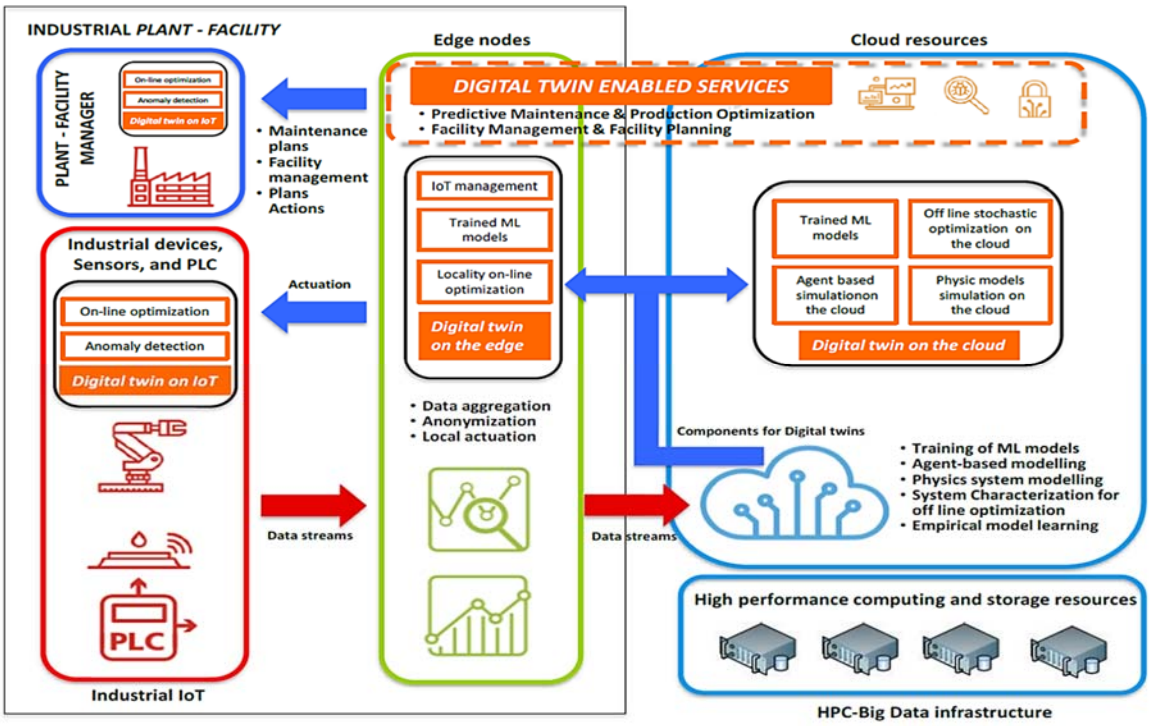

Fig. 5. Concept vision of IoTwins distributed hybrid twins [14].

With reducing the need of uploading data to the cloud, a kind of distributed intelligent processing architecture enables to proceed larger volumes of data, for example to proceed time series for AI treatment at the Edge. Nevertheless, it supposes reliable, secure and resilient data persistence mechanisms.

3.4. Data Persistence Management

From industrial technological realities such as the digital twins and its underlying industrial internet of things, robotics, additive manufacturing, sensors, or augmented reality capacities, to the development of innovative services within an ecosystem approach, the challenge is to well design the data system. This latter is to process the data, and also to store it, but virtually.

Data processing and management (DPM) needs to define the industrial data lifecycle and how to develop the business value. The defined DPM enables the architecture of data persistence management. ITU Technical Specification D2.1 has standardised a list of 23 capabilities to proceed from the data creation to its use and disposal [15]. From a data point of view, the listed capabilities might affect the state and structure of data, its location, the combination with other data, its transformation, use and disposal. TS-D2.1 also specifies processes to accumulate data for future processing and use. Duration of storage depends on the application, security, privacy and governance rules.

Data Collection and storage is one of the steps in the data lifecycle. Persistence is "the continuance of an effect after its cause is removed" [Datastax]. In the context of storing data in a computer system, this means that the data survives after the process with which it was created has ended. In other words, for a data store to be considered persistent, it must write to non-volatile storage, else a virtual storage that provides equivalence of non-volatility. The investigated EdgeDB [16] sounds a promising solution in front of other solutions we experimented to result in such non-volatility equivalence (namely BerkeleyDB, ObjectBox, Realm).

4. Safety Assurance for AI at Critical CPS

Embedded systems as they are designed for a fixed and known environment, lack events uncertainty which is faced by cyber physical systems. Building distributed AI based CPS framework, increases the need to build a strong safety approach that covers predicted but also unpredicted events. In the context of software defined physical systems, as typically are industry 4.0 facilities, the successful deployment of cyber-physical systems depends on the resilience functionality that should avoid as much as possible the safety risks. Additionally these CPS should have the correct behaviour recovery on a real time, using cognitive technologies at the edge.

Dependability of a system reflects the degree of trust into that system, because it demonstrates [17] (Fig. 6):

- Availability: The probability that the system will be up, running, and able to deliver the expected services.
- Reliability: The probability that the system will correctly deliver services as expected.
- Safety: A judgment of how likely it is that the system will not do what it should not do (typically to cause damage to people or its environment).
- Security: A judgment of how likely it is that the system can resist accidental or deliberate faults.
- Resilience: A judgment of how well a system can maintain the continuity of its critical services in the presence of disruptive events such as failure or fault injection.

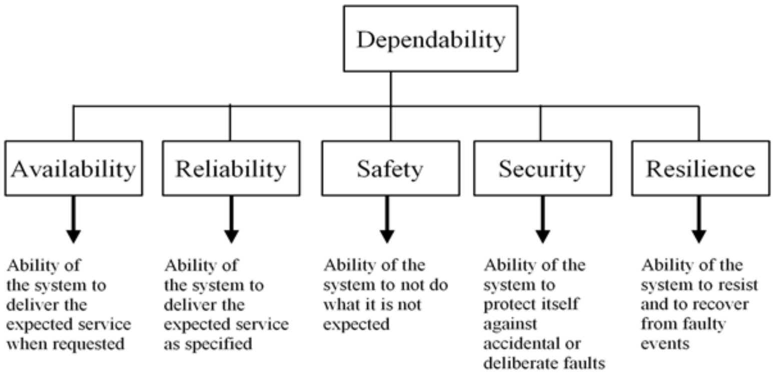

Fig. 6. Dependability attributes [17].

5. Cybersecurity at Virtual Swarm

With the virtualisation of the swarm processing into a virtual operating system, it raises cybersecurity issues. Actually, with the controllers which were previously hardwired and physically partitioned, even though the programmable logic, the cyber-physical system was relatively less exposed. But that’s only relatively: the accidentology has already shown since long ago, that cyber-attacks on industrial systems are common [24], [25]. With the virtualization of the whole process control, closely the execution, the cyber risk likelihood may increase with widening the access, standards protocols and multiplication of the objects in the industrial WoT.

Industrial safety remains a concrete reality at stake. Therefore, the distribution system which deploys the swarm processing has also to deploy simultaneously a security architecture, with security functions, mechanisms and their parameters. It could be a strategy of security in the uncertainty, but discussion of such an option is out of current scope. Industrial cyber-physical systems are presumably composed with known components. The IoTs’ on which the virtual system deploys shall natively embed a root of trust (as it is commonly the case with ARM-based microcontrollers). Then, the local micro-kernel can boot a safe image and procure a trusted local environment for further execution. Hosted local cybersecurity features are protected by the root of trust mechanisms. Hence the IoT is able to partition securely the device architecture, while interfacing with the deployed virtual operating system. Multiple trusted domains are then in execution on such an IoT platform. What means the IoT device can optimize the usage of its available resources accordingly with some policy (e.g. energy saving, safety critical operation, etc.) [26]. Nevertheless this cloudlet behavior, the primary function of the installation is to run a mission critical process, which shall comply with safety requirements. As explained by Hang and Wu [27], virtualization and isolation are mandatory. Hardware assisted virtualization and the virtual operating system layer (Open vSwitch in their example), build up such a cloudlet element, an edge computing / cloud networking system. Access control mechanisms, resource management, and cryptographic functions implement the cyber-secure environment that enable a proper functioning of the virtual swarm, with hardening against object requests or kind illegal codes.

Critical cyber and cyber-physical systems (CPS) are more and more using predictive AI models. These models help to expand, customize, and optimize the capabilities of the systems, but they are also vulnerable to a new and imminent class of attacks.

Although our current understanding of AI models is very limited, they are already identified to embed vulnerabilities. For instance, so-called “adversarial examples” can be generated algorithmically for defeating neural network models while appearing indistinguishable to human senses [18]. This can cause an autonomous vehicle to crash, illegal messages to bypass filters, while attacks may remain impossible to detect. A second type of vulnerability arises when the adversary provides malicious training samples that result in introducing biases into the cognition model. A third vulnerability is the potential violation of security monitors which provide the training data. More generally, the space of vulnerabilities and their impact on the overall control system are still to well-understand in order to overcome the safety risks that could result from security impacts.

6. Industrial Applications

In this section, we present three different industrial experimental use cases that empower AI-assisted distributed applications at the Edge. Each use case has been implemented thanks to SlapOS, an open source edge computing framework which provides, among others, autonomous intelligence, cognitive technologies and distributed swarm computing features.

Reproducing the IoTwins hybrid digital twin architecture previously described at section 3, the first case has demonstrated the use of GPUs at the edge to support real-time autonomic anomaly detection of the structural health of wind turbines with avoiding unnecessary service downtime, as well as extensive damage to the entire system. Based on models [28] calculated on a cloud-hosted data-lake using Keras deep learning, each edge node was equipped with a smart sensor. As wind turbines are generally deployed in low network coverage zones with limited uplink throughput, it was important to leverage IoT sensors in the wind turbines with powerful edge nodes handling most of the AI logic and reducing its network dependence. Thus, GPU based edge nodes directly connected to the wind turbines sensor were measuring continuous vibration to detect immediate icing, to optimize parallel processing, out-of-core processing, predictive algorithms, and to process data in parallel on each server (map reduce, batch processing, etc.) for higher reliability. It has shown higher effectiveness than older technologies deployed in the field with less network throughput.

The second case demonstrates Nexedi’s industrial control implementation based on virtualized PLCs' interconnected with IoTs at industrial layout and business orchestration in the cloud. In the context of food-processing industry, a fruit selection workflow has been proposed combining control of the production line (conveyors, valves, motors, etc.) with a software defined PLC, image recognition based on real time video capture and fault diagnosis process with ML toolkit at the edge.

Such an implementation virtualizes the production line with that software defined PLC powered by SlapOS that is an Edge operating system. Completed with part of the stack running at cloud, it builds up a digital twin which complies with the ISO23247 standard. The software defined PLC layer implements a distributed application, with an optical inspection and detection function, so the conveyor is “trained” to blow away any odd fruit the image recognition detects in the flow. For that purpose, the used ML toolkit was scikit, and openCV for image recognition. The management system interface in the cloud is then replicated as a software element at the edge being closer to the field sensors and actuators while providing an equivalent level of process control.

The third case studies a drone guidance implementation at a fleet, based on artificial intelligence deployed locally at IoT, with navigation at Edge and path planning in the cloud. A fleet of twenty drones were deployed, running autonomous software distributed at the swarm, to detect animals equipped with radio tag. Reporting services were to communicate position, map and sensed metrics in intermittent network conditions. The service provisioning handled the intermittent communication of the control station with the virtual drone system. It was to allocate to each drone a specific flight plan, whenever they were having connectivity access. The flight plan service was deployed at every drone to let the drone fly autonomously. Service operation can execute then, offline, totally autonomous, and independent from cloud interaction.

A mesh communication service was also deployed on all the drones. It was enabling drone to drone to datacenter communication, using a chain of transient links. With this approach, drones were able to deploy in any area with poor radio communication, yet achieving a defined flight plan to scan the area in a minimum amount of time.

7. Conclusions and Future Works

The emergence of Industry 4.0 has accelerated an increasing shift toward industrial fields functioning with software defined processing infrastructures embedding artificial intelligence techniques to perform the industrial operations, autonomous and efficient. Different AI techniques are supporting the operating functions which can deploy at the various domains of the ISO 30141 standardized industrial internet of things. Additionally the virtualization of the devices with software, the Edge Computing technologies have also introduced a next stage of virtualization of the whole physical layer into a software abstraction. Hence, elaborating upon that standard IoT architecture for industrial applications, the digital twin provides a cognitive system for such a virtualized world of industrial things, standardized with ISO23247.

Beyond just virtualizing the devices, the Edge computing technologies are coming with specific virtual operating systems which enable distributed computation accordingly the resources availability, and also data persistence. This latter emerges kind of a virtual storage in the fog that is a sort of cloudlet. It opens the possibility to cancel the need of uploading amounts of data to the cloud, but to compute locally the industrial processing. Only relevant data are then uploaded to the cloud. Hybrid digital twinning implements then a distribution of a new sort of industrial operating system software that deploys partly at cloud, and partly at fog. That way the AI-based cyber-physical system can function autonomously at the field.

Nevertheless, safety is a high concern for such industrial cyber physical systems. Running with potentially evolving configuration, the intelligent autonomous system requires specific attention for its design. The ISO26262 standard and complementary ISO/PAS 21448 "Safety of the intended functionality", provide an appropriate framework for the development of safe systems which run powered with AI. Tailored safety architecture and subsystems enable to conceive, autonomous intelligent CPS which can be eligible for the functioning of industrial applications and safety critical systems. Cybersecurity at the virtual swarm has to implement the prevention, alerting, and protection of the swarm components. The safety risks that could result from security impacts, are to overcome in order to ensure the safe performance of the AI-based CPS.

Experimental use cases at industrial environments or applications, have explored scenarios of execution with solutions. Although the validation of assumptions, these experiments also showed us limits and gaps, that lead currently to limitations of the technology. Future work on these technology aspects will have to develop software components we are missing for implementing correct Edge computing operating system. Appropriate Edge artificial intelligence can elaborate then on that basis, from a continuation of the industrial use cases.

Acknowledgment

We gratefully thank Dr Oleg Illiashenko and Department 503 of XAI, Ukraine National University of Aerospace in Kharkiv, for the collaboration and valuable recent results about methods and technologies for designing and implementing dependable systems based on the internet of things.

References

[1]. Y. Fourastier, C. Baron, H. Chaouchi, *et al.*, Industrial Field Autonomous Systems: AI-assisted Distributed Applications at Edge, in *Proceedings of the 2nd International Conference on Advances in Signal Processing and Artificial Intelligence (ASPAI'2020)*, Berlin, Germany, November 2020, pp. 201-203.

[2]. S. Madakam, R. M. Holmukhe, D. K. Jaiswal, The future digital work force: robotic process automation (RPA), *Journal of Information Systems and Technology Management – Jistem USP*, Vol. 16, 2019.

[3]. J. Shapiro, Genetic Algorithms in Machine Learning, *Machine Learning and Its Applications, Advanced Course on Artificial Intelligence (ACAI'1999)*, *Springer*, 1999, pp. 146-168.

[4]. T. Mitchell, Machine Learning, *McGraw Hill*, 1997.

[5]. I. Goodfellow, Y. Bengio, A. Courville, Deep Learning, *MIT Press*, 2016.

[6]. M. H. Hassoun, Fundamentals of Artificial Neural Networks, *MIT Press*, 1995.

[7]. P. A. Gutierrez, C. Hervas-Martinez, Hybrid Artificial Neural Networks: Models, Algorithms and Data, in *Cabestany J., Rojas I., Joya G. (eds.) Advances in Computational Intelligence IWANN 2011. Lecture Notes in Computer Science,* Vol. 6692. Springer, Berlin, Heidelberg, 2011.

[8]. H. Tian, S. C. Chen, M. L. Shyuy, S. H. Rubin, Automated Neural Network Construction with Similarity Sensitive Evolutionary Algorithms, in *Proceedings of the 20th IEEE Int. Conf. on Information Reuse and Integration for Data Science*, Los Angeles, CA, USA, July 30-August 1, 2019, pp. 283-290.

[9]. I. Saenko, F. Skorik, I. Kotenko, Application of Hybrid Neural Networks for Monitoring and Forecasting Computer Networks States, in Cheng L., Liu Q., Ronzhin A. (eds), Advances in Neural Networks – ISNN 2016, ISNN 2016, Lecture Notes in Computer Science, Vol. 9719, *Springer*, Cham. 2016.

[10]. A. Bannat, T. Bautze, *et al.*, Artificial Cognition in Production Systems, *IEEE Transactions on Automation Science and Engineering* Vol. 8, Issue 1, January 2011, pp. 148-174.

[11]. ISO/IEC 30141:2018, Internet of Things (loT) — Reference Architecture, ISO, 2018.

[12]. H. Hinduja, S. Kekkar, S. Chourasia, H. B. Chakrapani, Industry 4.0: digital twin and its industrial applications, *RIET-IJSET International Journal of Science Engineering and Technology,* Vol. 8, Issue 4, August 2020.

[13]. ISO/DIS 23247-1 Automation systems and integration — Digital Twin framework for manufacturing — Part 1: Overview and general principles, *ISO*, 2018.

[14]. P. Bellavista, A. Mora, Edge Cloud as an Enabler for Distributed AI in Industrial IoT Applications: the Experience of the IoTwins Project, in *Proceedings of the 1st Workshop on Artificial Intelligence and Internet of Things (AI&IOT'2019)*, CEUR Workshop, 2019, Rende, Italy, November 2019.

[15]. ITU-T Focus Group on Data Processing and Management to support IoT and Smart Cities & Communities, ITU-T, Technical Specification D2.1- Data processing and management framework for IoT and smart cities and communities, July 2019.

[16]. Y. Yang, Q. Cao, H. Jiang, EdgeDB: An Efficient Time-Series Database for Edge Computing, *IEEE Access*, Vol. 7, September 2019, pp. 142295-142307.

[17]. A. Avižienis, J.-C. Laprie, B. Randell, Fundamental Concepts of Dependability, LAAS Report no. 01-145, *LAAS-CNRS*, Toulouse, France, 1992.

[18]. Y. Fourastier, C. Baron, C. Thomas, *et al.*, Assurance levels for decision making in autonomous intelligent systems and their safety, in *Proceedings of the IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Kyiv, Ukraine, May 2020.

[19]. J. McDermid, K. Daffey, Safety of artificial intelligence and its role in autonomy: A Maritime Perspective, in *Proceedings of the Safety Critical Systems Symposium*, 2018.

[20]. McDermid, Y. Jia, I. Habli, Towards a Framework for Safety Assurance of Autonomous Systems, in *Proceedings of AISafety 2019*, Macao, China, 2019.

[21]. R. Salay, R. Queiroz, K. Czarnecki, An analysis of ISO 26262: Using machine learning safely in automotive software, *SAE Technical Paper, WCX World Congress Experience*, 2018.

[22]. ISO 26262 series - Road vehicles – Functional safety - Part 9: Automotive safety integrity level (ASIL) - Oriented and safety oriented analysis, *ISO*, December 2018.

[23]. ISO/PAS 21448:2019 - Road vehicles — Safety of the intended functionality, *ISO*, January 2019.

[24]. Y. Fourastier, L. Pietre-Cambacedes, *et al.*, Cybersécurité des installations industrielles, *Cépaduès*, 2015.

[25]. D. Kapp, L'industrie doit panser le numérique, Dossier Menaces sur l'industrie, *Face Au Risque*, Issue 562, Mai 2020.

[26]. S. Simanta, G. A. Lewis, E. Morris, K. Ha, M. Satyanarayanan, A reference architecture for mobile code offload in hostile environments, in *Proceedings of the Joint Workshop IEEE/IFIP Conference on Software Architecture*, August 2012, pp. 282–286.

[27]. D. Huang, H. Wu, Mobile Cloud Computing: Foundations and Service Models, Chap. 8, *Elsevier Morgan Kaufmann*, 2018.

[28]. O. Kramer, F. Gieseke, B. Satzger, Wind energy prediction and monitoring with neural computation, *Neurocomputing*, Vol. 109, 2013, pp. 84–93.