Non-technical Challenges of Industry 4.0

Wojciech Cellary

Non-Technical Challenges of Industry 4.0

Wojciech Cellary

Poznan University of Economics and Business
Niepodleglosci 10, 61-875 Poznan, Poland
cellary@kti.ue.poznan.pl

Abstract. Cyber-physical systems, Industry 4.0, and Economy 4.0 are defined as current trends in industrial manufacturing and more broadly – in economy and society. Three non-technical challenges are distinguished: (1) a challenge to future employees requiring new educational methods; (2) a challenge to fixing errors in complex software and training datasets; and finally (3) a challenge to responsibility of complex software designers, developers and integrators. These challenges may be considered as directions of future research on Industry 4.0 and Economy 4.0. All these challenges have roots in technology, but they have far social consequences.

Keywords: Cyber-physical systems, Industry 4.0, Economy 4.0, artificial intelligence, human's role, fixing errors, responsibility

1 Introduction

Industry 4.0 is a concept that originates from the industrial community and is currently broadly discussed by both industrial and the scientific community. Industry 4.0 emerged in the aftermath of the rapid development of information technology and robotics that together has given birth to new kinds of integrated systems [9]. There are plenty of technical issues that must be solved to make such systems run efficiently, reliably and safely [11]. There are also some non-technical issues that must be solved to prepare societies to use such systems. In this paper, in Sections 2-4 we first define Cyber-physical systems, Industry 4.0, and Economy 4.0. Then, we describe three selected challenges that have roots in technology, but that have far social consequences. In Section 5, we describe a challenge to future employees who will need to cooperate with robots controlled by artificial intelligence. In Section 6, we deal with a challenge of fixing errors in complex software used in cyber-physical systems, especially ones that are driven by big data. In Section 7, we present a challenge to determination of responsibility for errors and their consequences that without a doubt will arise when cyber-physical systems will be massively deployed. Section 8 concludes this position paper stating that each of the above challenges requires new methods and approaches that are unknown as of now. Therefore, they may be considered as directions for future research.

2 Cyber-Physical Systems

To understand the concept of Industry 4.0, it is necessary to start with contemporary information technology (IT). IT is currently – more than ever – focusing on data flow. The internet of people and internet of things (IoT) are mass data sources. Depending on a network usage scenario, the 5th generation of wireless telecommunications – 5G – will provide high data rates across a wide coverage area, or low latency and high reliability for mission critical applications, or sporadic communication for up to one million IoT devices per square kilometer. Data storage clouds provide essentially infinite storage for the big (i.e., massive) combined data sets generated by these devices and systems. Machine learning, neural networks and other techniques of artificial intelligence permit us to efficiently process collected big data to acquire new knowledge. Feedback is provided again by the internet of people and the internet of things influencing peoples' behavior either directly or indirectly through their environments. A characteristic of contemporary IT is the fact that the above data technologies depend on one another. Only when all are applied together, do they constitute a system that provides value for people.

A consequence of the data flow system is the convergence of the physical world with the digital world forming the cyber-physical world [4], [5]. Up to now, the physical world coexisted with the digital world. For example, a physical bank branch coexisted with an e-banking website. Almost all the banking operations were possible in both the physical and the digital bank. Only a few operations requiring a physical signature were not available in the e-banking web. In the near future, we can imagine a bank "robot" working in the cyber-world. For example, it is possible to imagine that a customer arrives at a gas station, refuels her car, and goes out without any explicit payment operations requiring physical objects like a credit card or a mobile phone. The sum due is paid automatically by the bank robot. This is possible because the car and the face of the customer are recognized by the system of the gas company cooperating with the bank, and the sum due is automatically deduced from her account using a direct debit scheme.

3 Industry 4.0

One may expect that such cyber-physical systems will emerge in different areas. The most natural area is factories, where these systems are called *smart factories* [11], or in the broader sense – industry, called *Industry 4.0* [7], [8], [9], [10], [12], [13]. A factory is a good candidate for application of cyber-physical systems, because it is a closed environment precisely controlled by factory management. Therefore, cyber-physical systems may be deployed step by step in a controlled manner, mitigating the risk involved.

Industry 4.0 may be defined as the information-intensive transformation of manufacturing in a cyber-physical environment of:

- Data,
- People,
- Processes,

- Services,
- Systems, and
- IoT-enabled industrial assets

due to:

- Generation,
- Leverage, and
- Utilization of actionable information

to improve innovativeness, efficiency, productivity and customization [8]. In [2] collaborative networks are considered to be a core enabler of Industry 4.0

However, the above definition is not particularly revolutionary. Industry has always tried to improve its efficiency and productivity to reduce costs and increase profit, to modernize through innovations so as to get competitive advantage over competitors, and to better satisfy its customers with customization of its products. For a long time, these goals have been achieved by aligning the IT solutions responsible for generation, leverage, and utilization of information with business processes and services involving people. Thus, the revolutionary character of Industry 4.0 may be best expressed as follows:

> ***The goal of Industry 4.0 is to provide mutually cooperating cyber-physical systems with decision-making autonomy.***

It is the planned autonomy of cyber-physical systems that makes the difference between Industry 4.0 and former approaches. Former approaches required the human maker of operational decisions to take responsibility for the decision outcome. The autonomy of cyber-physical systems in Industry 4.0 is possible due to the intensive data flow mentioned above and the application of artificial intelligence techniques to process big data to extract knowledge leading to autonomous decisions.

4 Economy 4.0

The idea of Industry 4.0 may be extended to Economy 4.0 [6]. Economy 4.0 encompasses a full digital value chain from suppliers of materials and components required for production, through all the brokers and providers of necessary services, up to the final recipients of the entire production, i.e., end-customers, regardless of who they are:

- Entrepreneurs,
- Consumers,
- Owners of buildings,
- Owners of retail stores,
- Employees,
- Citizens,
- Passengers,
- Patients, etc.

Economy 4.0, on the one hand, encompasses Industry 4.0 with its cooperating smart factories, while simultaneously extending smart concepts to many other sectors such as: smart energy grid, smart mobility and transportation, smart buildings, smart healthcare, smart breeding, etc. The range of Economy 4.0 may be classified as follows:

- Technologies 4.0 applied within a smart factory;
- Technologies 4.0 applied for cooperation among factories (smart or not);
- Manufactured smart things deployed in smart end-user environments;
- Digital services provided to users of smart environments.

In Economy 4.0 logistics and supply chain management play a particular role. They may be seen as tools of integration: vertical – within a smart factory, and horizontal – between factories, and between factories and smart end-user environments [1].

Economy 4.0 constitutes a more challenging environment than Industry 4.0 for two main reasons. First, it is an open environment controlled by more or less vague rules obeyed or not by different independent objects. Second, people in this environment are not trained as smart factory employees about how to interact most effectively with autonomous cyber-physical systems. Both reasons increase the risk of malfunctioning, and inaccurate interpretations of the actions of cyber-physical systems.

5 Challenges to Future Employees

The main challenges to achieving Economy 4.0 are adding the proper level of autonomy and intelligence to systems. The goal here is not only to make the systems more intelligent, but also to make them more efficient, effective, communicating, agile and flexible, and thus well adapted to the global, inter-connected, real-time economy. A consequence of this challenge is the necessity to find a right balance between autonomous and self-organizing systems, and the planning role of humans (employees).

A future employee will have to demonstrate his/her knowledge level, and his/her ability to cooperate with machines, including robots, in real world scenarios containing fast-changing conditions, requirements, and goals. Adaptation of work methods to the requirements of Economy 4.0 requires an holistic, but agile management approach in real-time, within rapidly changing, distributed environments. This means moving from an approach based on centralized organization and planning to an approach based on ad-hoc planning and risk management.

We may then anticipate that the human's role will then be markedly transformed in Economy 4.0. The depth of the change can be illustrated by the following example showing two extremes. Currently, to provide transportation of goods, the trucks that are used are driven by truck drivers. A truck driver may be seen as an operator of systems of interconnected devices, both mechanical and electronic, that comprise the familiar vehicle called a truck. In the future, in Economy 4.0, autonomous trucks will replace human-driven trucks, so the truck driver's job will gradually disappear. A human will be required, however, to play the role of a manager of a fleet of autonomous trucks. In other words, a human will be a supervisor of autonomous systems of devices controlled by artificial intelligence. This job is much more challenging. Working in concert with artificial intelligence, an employee will need enhanced skills of thinking and reasoning to be able to supervise autonomous decisions made by the system controlled by artificial intelligence.

6 Challenge to Fixing Errors in Software

The ancient Romans said: "Errare humanum est" which means: "To err is human". This truth is particularly well known to programmers, who are constantly making, discovering, and fixing errors in software.

Information, being the basis of decisions may be:

- Retrieved from memory,
- Computed, or
- Assumed.

In case of erroneous data, it is possible to find the errors and correct them. In case of an erroneous program, it is possible to find wrong piece of code and correct it. But, in case of erroneous assumptions and specifications, the entire system may need to be rebuilt. Fixing errors in data or code is an operational IT activity. However, changing specifications and assumptions adopted before the system was developed is a strategic interdisciplinary activity, especially if a cyber-physical system is concerned. Re-designing the digital part of a cyber-physical system is a challenge, but re-designing the non-digital part of a cyber-physical system, e.g., mechanical one, is usually much harder. It is worth noting that specifications and assumptions may become erroneous during system exploitation due to changes in the environment the system is devoted to serve. In the case of the fast-evolving Economy 4.0, such situations may arise frequently. The problem of system reliability is even harder when we take into account the need to protect systems against cyberattacks that may be considered as a fast evolving part of (hostile) environment of cyber-physical systems.

Fixing errors in software is hard, but methods to do that have been elaborated within software engineering discipline. Fixing errors of artificial intelligence systems stemming from design specification errors or invalid assumptions will be an enormously complex challenge. If we are dealing with a neural network consisting of thousands of nodes and trained by peta-bytes of data, then finding out why it generates erroneous results may approach impossibility. Perhaps we will discover ways to allow other artificial intelligence methods to help us with that.

7 Challenge to Responsibility

An important aspect of human life is discovering who or what is responsible for any significant accident. Consequently, today, methods of determining who is responsible for an accident are well developed. In the case of Economy 4.0, however, the problems are much harder and methods for determining responsibility for errors and accidents are not yet set. Consider, for example, the above mentioned autonomous truck travelling without a human driver that is involved in a serious single vehicle accident without injuries to any person in the vicinity. There are several suspects who might be responsible for that accident. The first is the truck owner. However, the truck owner is a car rental company. If it maintained the truck properly as required by law, it would be difficult to say that it had responsibility for the accident. The second suspect is the person who rented the truck. However, the renter in this case is also a company whose warehouseman loaded some goods into the truck, carefully secured them, then entered the customer's address and clicked “go”. Again, very likely this renter had nothing to do with the accident.

If the truck’s mechanics were right, then the next suspect are computer systems, i.e., hardware, internet and software. In case of an autonomous truck, hardware is not only an on-board computer, but also a cloud in which programs, data, maps, etc. are stored. If the on-board computer has not been mechanically damaged, it can be checked if it worked correctly. However, the cloud cannot be easily checked. There are usually several million processors in each data center composing a cloud. Only advanced testing software may check if any of them is functioning incorrectly. It is also difficult to determine which particular processor was supporting the truck that had the accident. Moreover, each processor was allocated to serve the truck for a very short time-slot. Then, the service could be taken over by another processor, or even a different data center located in a different country.

The cause of the accident could also be a break in internet communication. The internet is a very complicated system consisting of gates, routers, cables, fiber optics, wireless communications, satellites, etc. Each data packet exchanged between the cloud and the truck can go a different way. Generally, the internet works very reliably due to error detection and repeating the transmission of incorrectly transmitted data packets, although not all packets reach their destination immediately. Occasionally, however, it fails. The impacts of such failures are often unnoticeable, but in an Industry 4.0 environment, this may change and internet failures may start resulting in actual damages.

The most suspect component for the autonomous truck accident described above is the software operating the autonomous vehicle. This does not mean, however, that assigning blame only requires us to find and charge a suspect programmer. Hundreds of programmers who do not even know each other are involved in creating such a complex software that is required to drive an autonomous truck. One team of programmers once wrote a program module solving a general problem and put it in a digital library. Another team of programmers used this module in their vehicle guidance program module. Yet another team of programmers assembled the whole software system to drive an autonomous truck from such modules developed independently. The system was thoroughly tested by independent testers. It is practically impossible to determine who is responsible for an error in a software system so large and complex that has been developed and validated by so many people.

As mentioned in Section 6, an even harder problem is finding a person responsible for errors generated by artificial intelligence. Neural networks recognize images by calculating probability based on millions of cases stored in the cloud, so the result depends not on a human, but on which cases have been recorded and used to train the neural network.

8 Conclusions

Current societies are more and more dependent on software systems controlling not only the digital world, but also the cyber-physical world [3]. With increasing deployments of autonomous cyber-physical systems, the risk of damages caused by decisions following from their malfunctioning or wrong interpretation of the situation around them increases. As we have indicated above, cyber-physical systems are controlled not only by very complex software, but also by the big data sets used to train systems of artificial intelligence. The complexity and size of programs and training data are so massive that they cannot be verified for correctness using traditional software engineering methods. On the other hand, society cannot allow the errors of such software to be dismissed as a “force majeure” (which traditionally refers to the forces of nature beyond human’s control such as tornados, hurricanes, eruption of volcanos, earthquakes, tsunamis, etc.). Humankind cannot lose control over his own products. Therefore, one of the greatest challenges of modern computer science and engineering is to develop new methods of identifying the causes and fixing errors in complex information systems including artificial intelligence. The goal should not be to find and to punish a guilty programmer, but to ensure the error cannot reoccur.

Industry 4.0 and Economy 4.0 will maximally challenge our educational systems. The demand for routine cognitive and physical work will decrease, because computers and robots will do such work more precisely, effectively and cheaply. However, computers and robots controlled by artificial intelligence do not understand what they manage, they only count the probability of realizing possible scenarios that have already arisen in the past, and choose the one that optimizes a given criterion, in particular, the criterion that minimizes costs of production or service provision. Thus, Industry 4.0 and Economy 4.0 will need people who think, reason and understand how to control artificial intelligence to prevent terrible mistakes that may happen if the past is mindlessly repeated. Understanding and creativity will remain the exclusive domain of humankind. Therefore, the educational system will be required to transform itself to provide Industry 4.0 and Economy 4.0 with graduates who have capabilities attuned to 4.0 systems thinking, reasoning and creativity. These are the people we will depend on to be capable to cooperate with computer systems and robots controlled by artificial intelligence in conditions of distribution, diversity and uncertainty.

Acknowledgments. Many thanks to Louis E. Freund, Ph.D., Professor Emeritus in the Department of Industrial & Systems Engineering at San Jose State University, San Jose, CA, USA. Dr. Freund is founder and former Director of the SJSU Graduate Program in Human Factors/Ergonomics. The author is grateful for his participation in many thorough discussions and for his comments that greatly improved the manuscript.

References

1. Azevedo, A.: Collaborative Transformation Systems – Path to Address the Challenges Around the Competitiveness of Mature Countries. In: Camarinha-Matos, L.M., Afsarmanesh, H., Rezgui, Y. (eds.) Collaborative Networks of Cognitive Systems. PRO-VE 2018. IFIP AICT, vol. 534, pp 21-32. Springer (2018)
2. Camarinha-Matos, L.M., Fornasiero, R., Afsarmanesh, H.: Collaborative Networks as a Core Enabler of Industry 4.0. In: Camarinha-Matos, L.M., Fornasiero, R., Afsarmanesh, H. (eds.) Collaboration in a Data-Rich World. PRO-VE 2017. IFIP AICT, vol. 506, pp 3-17. Springer (2017)
3. Cellary. W., Freund, L.E., Kwan S.K., Leitner C., Spohrer, J.: The Human-Side of Service Engineering: Advancing Technologies Impact on Service Innovation. In: Proc. 6th Naples Forum on Service, 2019 (to appear)
4. Cyber-Physical Systems: Enabling a Smart and Connected World, https://www.nsf.gov/news/special_reports/cyber-physical/
5. Cyber-Physical Systems, https://www.nist.gov/el/cyber-physical-systems
6. Economy 4.0 and its labour market and economic impacts, http://doku.iab.de/forschungsbericht/2016/fb1316_en.pdf
7. Industry 4.0: Definition, Design Principles, Challenges, and the Future of Employment, https://www.cleverism.com/industry-4-0/
8. Industry 4.0: Technologies Integrations, Security, People/Workers and Society, https://devisionx.com/fourth-industrial-revolution/
9. Industry 4.0: the Fourth Industrial Revolution – Guide to Industrie 4.0, https://www.i-scoop.eu/industry-4-0/
10. Plattform Industrie 4.0, https://www.plattform-i40.de/PI40/Navigation/EN/Home/home.html
11. Industry 4.0: Building the digital enterprise, https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf
12. Schweichhart, K.: Reference Architectural Model Industrie 4.0 (RAMI 4.0). An Introduction, https://ec.europa.eu/futurium/en/system/files/ged/a2-schweichhart-reference_architectural_model_industrie_4.0_rami_4.0.pdf
13. Stich, V., Gudergan, G., Zeller, V.: Need and Solution to Transform the Manufacturing Industry in the Age of Industry 4.0 – A Capability Maturity Index Approach. In: Camarinha-Matos, L.M., Afsarmanesh, H., Rezgui, Y. (eds.) Collaborative Networks of Cognitive Systems. PRO-VE 2018. IFIP AICT, vol. 534, pp 33-42. Springer (2018)