Journal of Ambient Intelligence and Smart Environments 00 (20xx) 1–12
DOI 10.3233/AIS-170432
IOS Press

The intelligent industry of the future: A survey on emerging trends, research challenges and opportunities in Industry 4.0

Davy Preuveneers [a,*] and Elisabeth Ilie-Zudor [b]
[a] *imec-DistriNet, Department of Computer Science, KU Leuven, Leuven, Belgium*
[b] *MTA SZTAKI, Hungarian Academy of Sciences, Budapest, Hungary*

Abstract. Strongly rooted in the Internet of Things and Cyber-Physical Systems-enabled manufacturing, disruptive paradigms like the Factory of the Future and Industry 4.0 envision knowledge-intensive industrial intelligent environments where smart personalized products are created through smart processes and procedures. The 4th industrial revolution will be based on Cyber-Physical Systems that will monitor, analyze and automate business processes, transforming production and logistic processes into smart factory environments where big data capabilities, cloud services and smart predictive decision support tools are used to increase productivity and efficiency. This survey provides insights into the latest developments in these domains, and identifies relevant research challenges and opportunities to shape the future of intelligent manufacturing environments.

Keywords: Factory of the future, smart manufacturing, trends, challenges, survey

1. Introduction

With Intelligent Environments [5], we typically envision algorithms and software embedded in everyday objects that collectively aim to make our surroundings smart and support us with our daily activities by accommodating us to the given situation at hand. Indeed, technological breakthroughs in miniaturization and wireless communication have enabled sensors, mobile devices and applications to communicate with one another and be continuously in ours and each others' interaction range. Sophisticated context-aware applications and services have been built on top of these wireless sensors and actuators [34] to monitor their users' presence and adapt autonomously to an always evolving context, while remaining sensitive to changing needs and preferences. As a result, the hardware and software trends of the last decade have enabled various vertical domains – ranging from smart homes [7,51], offices and work places [1,3], smart cities [13] to applications for assisted living [45] and enhanced healthcare management [16], etc. – to add value to their offerings for intelligent environments. These technological advances and innovations are further accelerated by new emerging trends, such as the Internet of Things (IoT) [4,18,49] and Cyber-Physical Systems (CPS) [28,46]. These computing paradigms envision a future in 2020 with an estimated 50 billion devices around the globe connected to the Internet. Information and intelligent services will be invisibly embedded in every environment around us, and large amounts of data will circulate in order to create smart and proactive environments that will significantly enhance both the work and leisure experiences of people.

A similar digital transformation is taking place in the 4th Generation Industrial Revolution (Industry 4.0) [29,30]. A brief history of the industrial revolutions will help us understand how the industry has evolved over the past few centuries and will advance into next generation intelligent environments. Mechanical production with water power and the steam engine gave

*Corresponding author. E-mail: davy.preuveneers@cs.kuleuven.be.

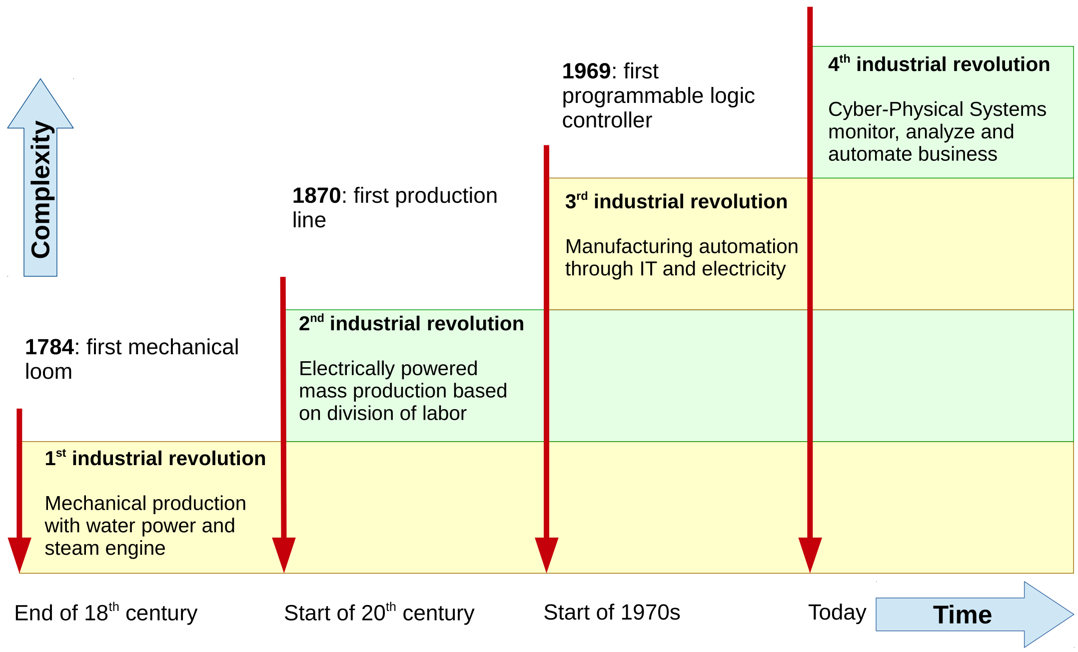

Fig. 1. The four industrial revolutions leading to the smart Factory of the Future and Cyber-Physical Production Systems.

rise to the 1st industrial revolution in the 18th century (see Fig. 1). Later on, electrically powered mass production based on division of labor characterized the 2nd revolution at the start of the 20th century, whereas the 3rd was marked with the introduction of the first programmable logical controller only a few decades ago that enabled IT-based manufacturing automation. The 4th industrial revolution will build upon the emerging Internet of Things and Cyber-Physical Systems paradigms to monitor, analyze and automate business processes at large. These technological revolutions will transform production and logistic processes into smart factory environments that will increase productivity and efficiency.

Indeed, Industry 4.0 and the related Factory of the Future (FoF) [11,24] paradigm envision a future of creating smart products through smart processes and procedures, strongly rooted in the Internet of Things and Services and Cyber-Physical Systems-enabled manufacturing [36], with applications in the area of energy, logistics, sustainable mobility, etc. The widespread adoption of Cyber-Physical Systems and Big Data analytics technologies by manufacturing companies will lead to the 4th Industrial Revolution where Cyber-Physical Production Systems (CPPS) [35] are blurring the boundaries between the real world and the virtual world. Smart products will plan, control and optimize their own production process with minimal human intervention. The digital transformation will enhance the transparency of the production process, even across the organizational boundaries of the manufacturing enterprise. As such, similar to the classical intelligent environments (i.e. the smart homes, smart offices and smart cities), there is a trend of transforming production and logistic processes into smart factory environments where big data capabilities and smart predictive decision support tools are used to increase productivity and efficiency [21].

This survey reviews relevant system- and user-oriented research tracks of intelligent environments, and discusses non-trivial challenges specifically related to the design, the implementation and the evaluation of smart industry applications:

1. Transparent networked production with industrial wireless networks.
2. Enhanced knowledge management with context-aware industrial systems.
3. Data-driven planning and optimization with Big Data analytics in the cloud.
4. Creating insights with machine learning and data mining for Industry 4.0 applications.
5. Human computer interaction aspects for different types of stakeholders.
6. Security and privacy threats as well as compliance regulations for personalized manufacturing.

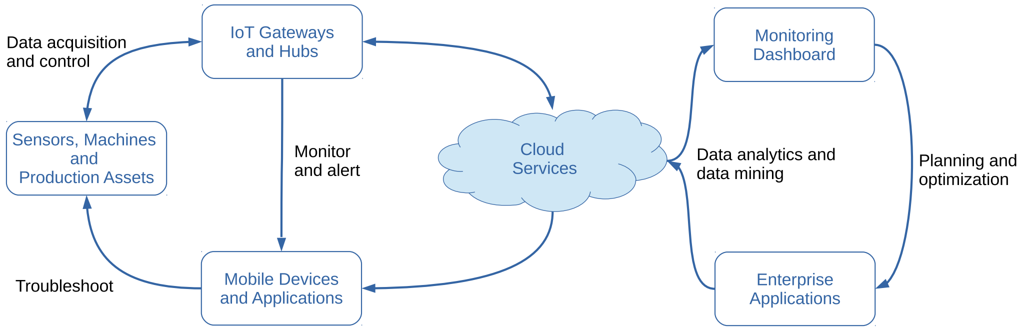

Fig. 2. Intelligent industrial IoT networks linking sensors, mobile devices and cloud services.

The survey highlights related work and contributions on recent developments and experiments with such applications in simulated smart environments as well as successful deployments in the real world.

Section 2 highlights ongoing research in wireless sensor networks that provide the foundation for the Industrial Internet of Things (IIoT). The application of context-awareness in this area is the subject of Section 3. Section 4 discusses the importance of enabling technologies of cloud computing and big data, whereas Section 5 highlights how machine learning and data mining can help to make factories smarter. The role of the user within such an ecosystem is further explored in Section 6, while security and privacy concerns are discussed in Section 7. In each of these sections, we will discuss how the techniques and best practices have been applied in the domain of Industry 4.0 and the Factory of the Future. We end this survey with some critical reflections and concluding thoughts in Section 8.

2. End-to-end production transparency with industrial wireless networks

Industrial companies are shifting from traditional wired infrastructures towards wireless sensor networks (see in Fig. 2) to continuously monitor the performance of their plants, as the former are often too complex to expand and too rigid to quickly adapt to evolving production market dynamics. Wireless sensor technology offers clear advantages to monitor production assets and the corresponding networked manufacturing or logistics business processes (a typical orchestration of such processes is depicted in Business Process Model and Notation (BPMN) in Fig. 3) in order to gain real-time insights in how to boost productivity, optimize resource efficiency, reduce interruptions, or minimize down time. The intrinsic value of wireless sensor networks is that they are much more flexible and cost-effective to install for temporary and incremental collection of additional data points. This enables a swifter end-to-end integration into existing industrial production networks that may consist of IoT networks, mobile applications and cloud services.

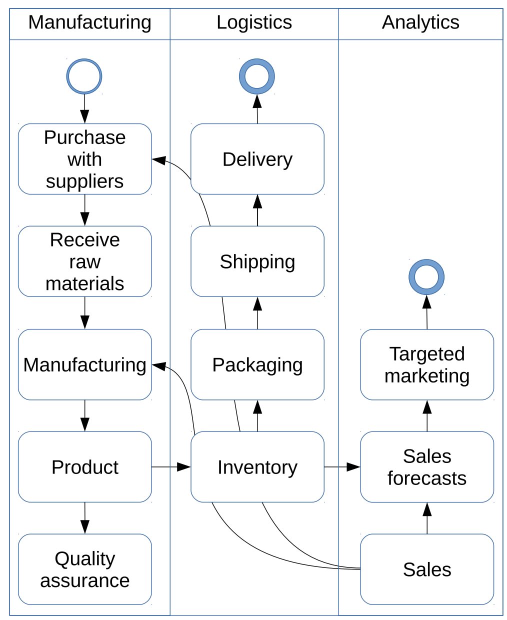

Fig. 3. Collaborative networked production systems and services in a Business Process Model and Notation (BPMN) diagram.

Li et al. [31] review how wireless sensor networks (WSNs) have played a pivotal role to build industrial wireless networks (IWNs) for Industry 4.0 applications. While WSNs and IWNs share many similarities and features, the authors argue that the latter impose new constraints and requirements for realizing efficient industrial intelligent environments. First of all, when monitoring and controlling industry or production systems in real-time, having a low network *latency* is a key concern, which is often realized at the expense of a higher energy consumption. This is in contrast to the traditional wireless sensor networks as found in the smart home and office environments where a higher latency is usually not a concern, but where maximizing the battery life-time is usually the goal for increased user convenience. Second, in production and manufacturing environments, there are many more *mobile* components that need to be monitored, such as mobile devices, robots, automated guided vehicles (AGVs), which results in wireless networks with many more mobile sensor nodes, compared to the more stationary networks in more classic intelligent environments. Third, the industrial *environment* in which the sensors are deployed may also be more challenging, due to interference of other obstacles, dust, vibration, higher temperatures and humidity, etc. These continuously changing circumstances may influence the reliability and efficiency of communication in production networks. Last but not least, due to the many tasks of sensor nodes in an industrial wireless network, they come with a higher *capacity* for data storage and processing compared to their consumer-oriented equivalents.

Similar research on the wireless challenges in Industry 4.0 was conducted by Varghese et al. [52], raising deterministic low network latencies, increased battery longevity, scalable connectivity, reliable machine-to-machine communication, high data rates, and seamless connectivity as important requirements. In particular, they investigate to what extent the 5G communication standard can address these requirements. They conclude that a single wireless standard, such as WiFi, will not be able to address all the requirements in the Industry 4.0 era, and that a combination of various technologies will be necessary to realize an efficient industrial wireless network.

Xu et al. [57] conducted an extensive literature review on the growing interest in using IoT technologies in various industries, highlighting comparable important challenges and opportunities. They offer an in-depth review of the applicability of service-oriented architecture (SOA) and other enabling technologies for IoT, and how such IoT systems are being adopted in different industries. The vertical domains that they cover, include the healthcare service industry, the food supply chain, mine safety, transportation, logistics and firefighting. Important complementary research challenges and future trends that the authors highlight include standardization (e.g. communication and identification), security and privacy. From a technical perspective, they consider the scalability and heterogeneity of IoT networks as non-trivial challenges, as well as a commonly accepted service description language for IoT services to ensure compatibility and interoperability, including integration with legacy systems.

Additional insights, trends and research challenges in wireless communication, industrial protocols, process automation, monitoring and control applications and industrial distributed environments are offered in other surveying articles [10,15,19,20,47].

3. Information management in context-aware industrial systems

Context-aware behavior is instrumental in industrial production environments to build smart manufacturing systems and applications on top of industrial wireless networks. Such systems mainly focus on tracking and tracing, zero-defect manufacturing and proactive maintenance. As confirmed in the final report of the Industrie 4.0 Working Group [23] on "*Recommendations for implementing the strategic initiative INDUSTRIE 4.0*", smart products will be uniquely identifiable and may be located at all times. Furthermore, it will be possible in the future to incorporate individual customer-specific features into the design. As Fig. 4 depicts, typical end-to-end Industry 4.0 integration scenarios involve many people with different roles and information needs. Effective and reliable data collection is key to implement context-adaptive decision support systems that continuously monitor and control manufacturing and production processes with humans in the loop. Context-awareness also helps to create a holistic view of assets, people and inventory, and can reduce human errors of production line engineers and operators by reducing their cognitive load.

With billions of sensors connected to the Internet, context-awareness is an important research area within the IoT. Perera et al. [40] surveyed a broad range of techniques, methods, models, functionalities, systems, applications, and middleware solutions related to context awareness and IoT. Their analysis includes a historic overview of how the area of context-aware computing has evolved over the last two decades. Additionally, the authors review an extensive list of 50 academic and industrial project initiatives. While not focusing on industrial IoT applications, the challenges that the authors highlight are of high importance to this domain. First of all, they proclaim the automated configuration of sensors as a necessity due to the

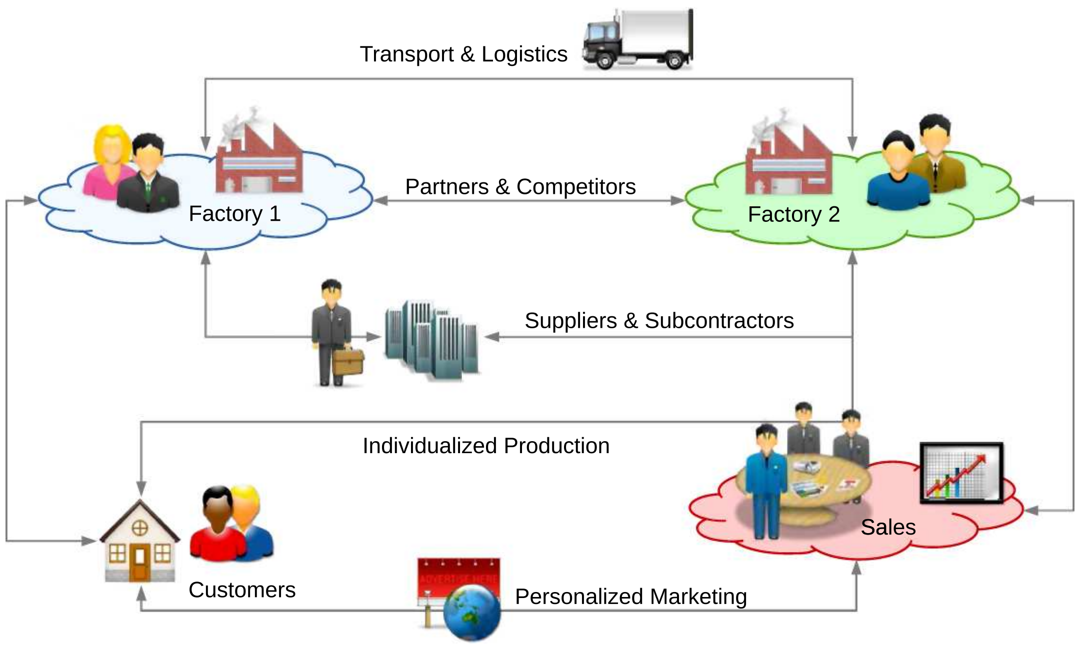

Fig. 4. Multiple stakeholders in Industry 4.0 related business processes.

sheer scale of industrial wireless networks. Other well-known challenges being mentioned, include the discovery, modeling, distribution, and sharing of context information, as well as the ability to reason upon context information and select sensors in a sensing-as-a-service model. Last but not least, the authors also mention security, privacy and trust as major considerations that have been there since the beginning of context-aware computing, concerns that will be here to stay in the foreseeable future.

Dhuieba et al. [12] highlight the importance of adequate knowledge management in manufacturing applications. With digital factories integrating a variety of IT-based systems – from product lifecycle management (PLM) systems, manufacturing execution systems (MES), enterprise resource planning (ERP) systems to manufacturing process management (MPM) systems, etc. – knowledge is omnipresent, a necessity to support different factory stakeholders with achieving their daily design, planning and optimization activities. The authors investigate how context-awareness can support knowledge reuse in multiple production contexts and factory environments while reducing information overload.

Lunardi et al. [32] present COBASEN, a middleware to simplify the discovery, search, selection, and interaction with devices in large Industrial IoT networks with devices having overlapping and sometimes redundant functionalities. The middleware is built around a context module and a scalable context-based search engine that leverages the semantic characteristics of devices to help users interact with them. Preliminary performance experiments show acceptable indexing and querying response time results. The authors also argue that COBASEN can be an essential tool to improve the development of Industrial IoT (IIoT) applications, by offering support not only for those people that deploy middleware, but also the ones that implement the IIoT applications and industrial processes.

Alexopoulos et al. [2] present a context-aware information distribution system to support users in industrial environments. Their context-aware manufacturing information system, called CA-MIS, is event-based and data driven. The problem that they address, focuses on the fact that contemporary information infrastructures often fail to successfully aggregate and manage data from factory-wide sensor networks as well as from various data sources, such as MES and ERP systems. Additionally, these systems often do not analyze the data and deliver it to different users in a context-based manner. Their proposed solution builds on top of NFC, RFID, RDF and HTML5 enabling technologies to provide the right information, to the right people at the right time on display devices, static or mobile, available at the shop-floor. It targets the development and deployment of services and applications to support decision making for users working at the manufacturing shop-floor.

4. Optimizing industry processes with Big Data and Cloud Computing

While the Internet of Things paradigm and recent advances in Machine-to-Machine (M2M) communication enable real-time monitoring of smart factories, the effective optimization of business processes and resource consumption often rely on fairly data intensive processes for which the computational resources available on-site are not sufficient.

In that sense are cloud computing and Big Data critical enabling technologies for the Industry 4.0 paradigm. It is not only the place where the bulk of industrial device data and decision critical information is ingested and analyzed, it offers the flexibility to scale on demand to diverse workloads to automate and optimize business processes (see Fig. 5). It enables data analytics with predictable performance, even with growing industrial wireless networks of interconnected things, resulting into a cost-efficient supply chain.

O'Donovan et al. [39] discuss the complexity that manufacturing facilities are faced with when having to manage exponentially increasing amounts of data, and analyze those datasets to extract meaning in order to make well-informed business critical decisions. Their

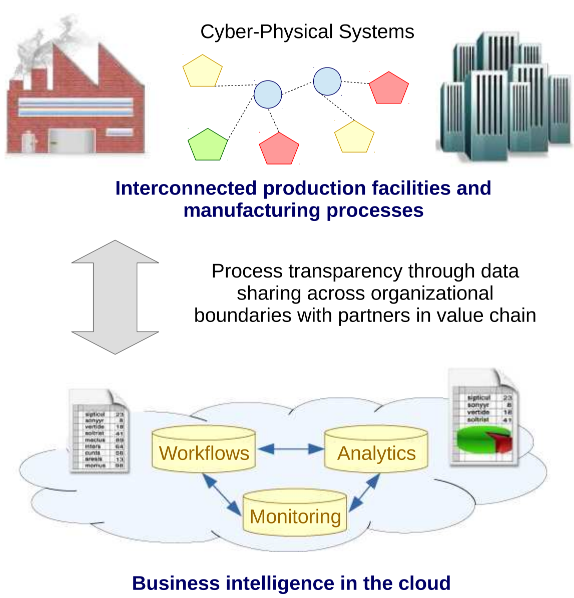

Fig. 5. Cloud-enabled networked production and manufacturing.

breadth-first review of big data technologies in manufacturing focuses on the systematic mapping of big data technologies in manufacturing. They investigate 5 fundamental research questions: (1) what are the popular publication fora for big data research in manufacturing, (2) what kind of formal or practical research is being carried out, (3) what kind of contributions – ranging from systems and tools to optimization methods – are being made in this area as results from these research efforts, (4) what kind of analytics are being used, and (5) which areas within manufacturing are being targeted the most.

Pisching et al. [43] investigate how the domains of both Internet of Things and Cyber-Physical Systems are converging within smart factories to the Internet of Services paradigm. The authors present a survey about service composition in a cloud-based manufacturing setting, and summarize advancements made in this area for Industry 4.0 as a collaborative and integrated manufacturing environment. These services could represent manufacturing processes, possibly offered by virtual enterprises. Customers could then request a particular virtual service, which is then composed out of existing cloud services to meet the customer's specific demand.

Wang et al. [54] present a framework that incorporates industrial wireless networks, cloud, and fixed or mobile terminals with smart artifacts such as machines, products, and conveyors. Their objective is the realization of a vertical integration to implement a flexible and reconfigurable smart factory. They also elaborate on the ability of such ecosystems to self-organize, assisted with feedback from big data analytics building blocks running in the cloud. Beyond these technical aspects, the authors also highlight important challenges that related to intelligent decision making and negotiation, high speed industrial wireless network protocols, special features of manufacturing for big data analytics, system modeling and analysis, cyber and property security, and modularization with flexible physical artifacts. The authors conclude that self-organization, coordination and big data based feedback are key to ensure that smart machines and products can communicate and negotiate with each other to reconfigure themselves for flexible production of multiple types of products.

Kehoe et al. [25] specifically survey over 150 works in the area of cloud robotics and automation, citing examples where the cloud can enhance automation by facilitating access to data sets, models, designs, simulation tools and other software. While moving robotics and automation algorithms into the cloud may mitigate the long delays when waiting for complex data analytics processes to return results, the authors also raise a range of security and privacy concerns related to cloud-connected robots and sensors that may collect sensitive information, such as corporate trade secrets, as well as other regulatory, accountability and legal issues of remotely connected systems.

5. Smarter manufacturing and production with machine learning and data mining

More and more software and intelligence are being integrated into industrial production and manufacturing systems to reduce the cost efficiency and improve the quality, efficiency and flexibility of production. The application of machine learning in manufacturing is hardly a novel theme. Already more than two decades ago, Monostori et al. [37] surveyed various machine learning techniques that seemed applicable for realizing manufacturing systems with intelligent behavior to handle the growing complexity of such dynamic systems in fast changing production environments full with uncertainties.

Pham et al. [42] discuss in their survey how machine learning is widely applied in different areas of manufacturing, highlighting example applications for optimization, control, and troubleshooting. The focus of their work is on supervised classification, covering algorithms such as decision tree induction, rule induction, instance-based learning, neural networks, genetic algorithms and Bayesian approaches. The key problems that they identified back in 2014 dealt with the necessity to scale up these machine learning algorithms for significantly larger data sets, and the necessity to learn multiple models in parallel.

Mekid et al. [33] discuss zero-defect workpieces and just-in-time production as important challenges of intelligent reconfigurable manufacturing systems. They address machine learning approaches for parameter optimization through self-learning as key enablers for process monitoring and control strategies in next generation intelligent manufacturing systems.

West et al. [55] investigate the problem of time-consuming rework and scrapage due to slight variations of the product state during production. They argue that traditional methods based on modeling of cause-effect relations can no longer handle the increasing complexity and high-dimensionality of modern manufacturing programmes. To address this concern, they research the applicability of combining clustering and supervised machine learning as a possible way to improve quality monitoring. While their approach is promising, the authors also highlight challenges emerging from the application of the proposed technique in industrial manufacturing environments. These relate to the complexity of collecting data and the integrity of that data, the creating of learning data for supervised learning methods, and possible risks of over-fitting.

A more recent by West et al. [56] re-explored the advantages, current challenges and contemporary examples of successful applications of machine learning in manufacturing. The same concerns remain, being a growing complexity, highly dynamic production environments, and high dimensionality data with chaotic structures. Their work resulted in a mapping of unsupervised machine learning, reinforcement learning, and supervised machine learning algorithms and matching applications. The authors conclude that supervised learning is a good fit for most manufacturing applications given that labeled data is often available for manufacturing applications. However, they also acknowledge that due to the growing availability of data and sensor technologies, unsupervised methods may gain importance in the future.

6. Human computer and machine interaction for problem solving and decision making

While automation and optimization of business processes are major challenges within Industry 4.0, it does not mean that human beings are taken out of the picture completely. The growing complexity of manufacturing and production means that adequate solutions must be provisioned to handle the growing amount of information. That is why the way humans interact with such systems for problem solving or decision making is a challenge which cannot be ignored.

Gorecky et al. [17] address intelligent user interfaces that offer technological assistance of workers by means of representing the cyber-physical world such that they can realize their full potential as strategic decision-makers and flexible problem solvers. They investigate to what extent the established interaction technologies and metaphors from the consumer goods market seem to be promising for the field of Industry 4.0. They analyze approaches for the acquisition, aggregation, visualization, and re-use of data and information within mobile context-aware interaction for the development of manufacturer-independent and multi-platform user interfaces.

Pfeiffer et al. [41] also investigate how to empower users to understand, monitor, and control automated processes within Industry 4.0. They propose a user-centered design (UCD) process with methods for usability and user experience engineering that should be fully integrated into the development process. Existing concepts within human computer interaction (HCI) and human machine interaction (HMI) should evolve not only to deal with more data and new machines, but also the account for the growing adoption of mobile devices for which existing traditional user interfaces are no longer adequate. Key challenges for an Industry 4.0 enabled user interface include a.o. the ability to handle large amounts of data with different levels of abstraction, offering explanation for automatic decision systems, the tension between standardized versus personalized user interfaces within collaborative production systems, and training.

Flatt et al. [14] employ context-awareness to assist with maintenance activities in smart factories. They present a tablet-based software solution that leverages augmented reality and indoor localization to place virtual sticky notes at production modules. The objective is that this system can exchange information about static and dynamic maintenance information and recurring maintenance tasks that show a worker how to execute particular maintenance steps. Next to textual information (e.g. plant process data or manuals), their solution also supports audio and video. Key advantages are the augmented reality subsystem does not require any configuration, as it learns its environment as it goes. Additional experiments show that the system can handle a large amount of sticky nodes without jeopardizing the stability of the tracking or require large amounts of storage space.

7. Growing concerns of security and privacy threats and new compliance regulations

Given the generation and aggregation of high volumes of volatile data and sensitive user information, it is clear that there are a multitude of security [22] and privacy challenges caused by sensors and smart devices continuously monitoring the environment. Embedded in the infrastructure and the products themselves, these sensors not only track business and manufacturing processes, but also customer behavior after the production phase, and sometimes in a way that is not visible to them. Indeed, the attack surface for security and privacy threats grows, as depicted in Fig. 6. That is why a Defense-in-Depth strategy for all production processes to protect both physical access and digital access on every network layer (as shown in Fig. 7) is paramount.

Cyber-security remains a clear challenge for the roll-out of the smart factories of the future. Many of the systems, technologies and protocols that exist today and that will become constituents of Industry 4.0 were never designed with networked production and

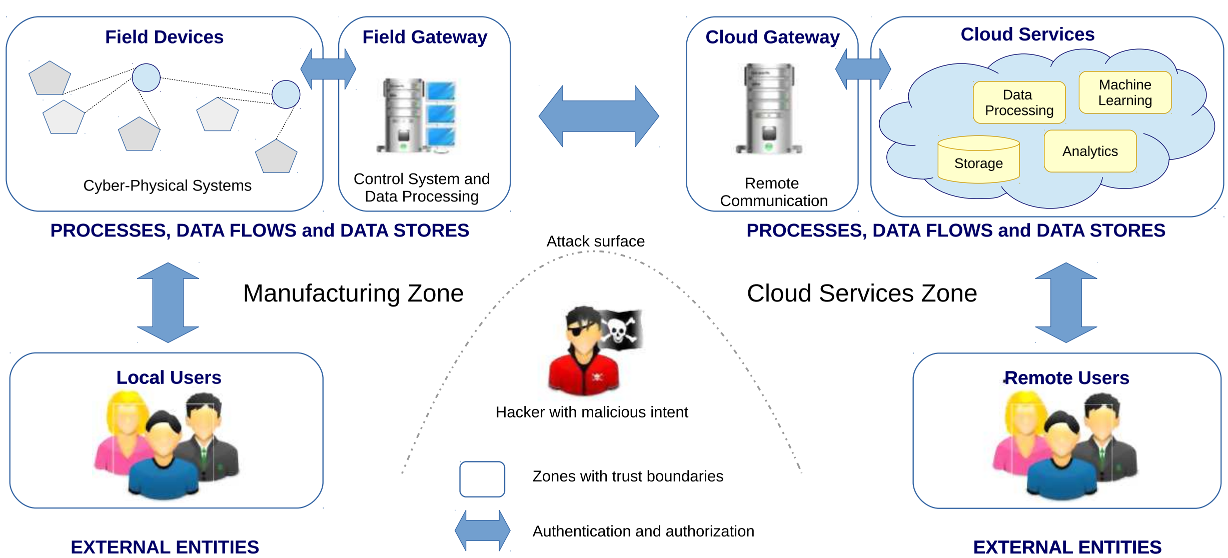

Fig. 6. Growing incentives for a hacker to attack distributed Industry 4.0 applications.

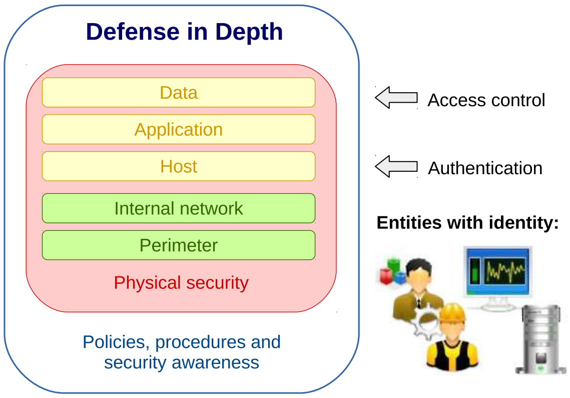

Fig. 7. Security best practices for networked applications.

large scale connectivity in mind. This can be witnessed from recent successful attacks on SCADA systems by dangerous malware like Stuxnet, Duqu, Flame, and Gauss [6,27]. In [38], Nicholson et al. survey ongoing research and present an overview of risks, threats and mitigation strategies in the area of SCADA security.

Sadeghi et al. [48] discuss various security and privacy challenges in the industrial Internet of Things, and offer an outlook on possible solutions towards a holistic security framework for Industrial IoT systems. They argue that contemporary security solutions are inadequate due to scalability issues to handle large networks of heterogeneous devices and cyber-physical systems, as well as concerns of constrained resources and the necessity to not jeopardize the fulfillment of real-time requirements.

Preuveneers et al. [44] present a framework that builds on top of Big Data enabling technologies to address various security and privacy challenges in the IoT. Their solution is inherently an attribute-based access control solution built on top of the Apache Spark Streaming framework to enforce access control policies on incoming and intermediate data streams. Their solution also incorporates data protection safeguards to protect the disclosure of sensitive data and quasi-identifiers using a.o. k-anonimity [50] and l-diversity privacy strategies.

With personalized manufacturing and product individualization being important objectives of Industry 4.0, it is no surprise that new regulations and directives will be put in place to protect the privacy of individuals. The seven core principles of Privacy by Design (PbD) [8,26], as proposed by Cavoukian in the 90's in response to the growing impact of ICT and large-scale networked data systems, appear more often these days in discussions on data protection and data security in the era of Big Data [9]. The general principles can be summarized as follows:

1. *Proactive not Reactive; Preventative not Remedial*
   The goal is to employ proactive rather than reactive measures in order to anticipate and prevent privacy-invasive events from occurring.
2. *Privacy as the Default Setting*
   Personal information must be automatically protected in any software system. Even if the individual does not undertake any action, his or her privacy is preserved.
3. *Privacy Embedded into Design*
   Privacy must be embedded into the design and architecture of any software system and business process from the start, and should never be an afterthought.
4. *Full Functionality – Positive-Sum, Not Zero-Sum*
   The functionality of a software system should only be extended if at the same time the system's privacy awareness is improved.
5. *End-to-End Security – Full Lifecycle Protection*
   Strong security measures are essential to protect personal information. Security and privacy measures go hand in hand during the entire lifecycle of the data involved.
6. *Visibility and Transparency – Keep it Open*
   All stakeholders are assured that all business practices and technologies are operating according to the stated promises, subject to independent verification.
7. *Respect for User Privacy – Keep it User-Centric*
   Keep the interests of the individual uppermost by offering strong privacy defaults, appropriate notice, empowering individuals with user-friendly options.

To address these concerns, the EU General Data Protection Regulation (GDPR) [53][1] – put forward by the European Commission back in January 2012 – was finally agreed upon in February 2016. The GDPR aims to harmonize the current data protection laws in place across the EU member states and directly applies to all EU member states after a period of two years without a need for implementing legislation at the national level. As such, the GDPR will significantly affect businesses in all industry sectors, including those outside the EU that process data of EU citizens as a service to support the effective operation of smart factories.

[1] http://www.eugdpr.org/more-resources.html.

8. Summary and reflection on the state of the art

This survey on emerging trends and research challenges on the industry of the future covered a wide variety of topics relevant for the design of intelligent environments. By no means did we aim to explore in-depth the state of the art on each of these topics. Our goal was to give a cross-disciplinary flavor of how ongoing research is shaping the future of intelligent manufacturing environments, while identifying important opportunities for further research. To get more details and insights on a particular topic, we highly encourage the audience to read the comprehensive surveys we referred to.

However, reflecting back on the surveyed works, we can conclude that making Industry 4.0 applications smart requires a holistic approach that further complicates the development process. We identified the following opportunities for further research on industrial-level intelligent environments to smoothen the transition from a proof-of-concept in the lab into tangible deployments in the real world:

- *Guaranteeing predictable system behavior*: Industry 4.0 applications do not operate in isolation, but often rely on and interact with services and components from third parties, which make them harder to test. With an increased focus on networked production, failures are bound to happen. Given that the competitiveness of a company resolves around cost efficiency, mitigating unknown risks due to external influences early in the design phase is key. Applying a design for failure methodology for distributed intelligent manufacturing systems may improve the reliability and robustness against unforeseen circumstances to guarantee zero-defect manufacturing. However, the literature seems to be focused more on avoiding errors rather than having contingency plans in place to be prepared for failures.
- *Quality assurance for context-aware behavior*: Heavily built on top of industrial wireless sensor networks, context-awareness plays a key role in strategic decision making (for troubleshooting or process optimization). The scientific literature on context-aware computing includes several works on how to effectively deal with subpar context information quality. However, there is limited work in this area for smart factories, meaning that there are several opportunities to investigate the negative impact of improper decisions and how that may influence the cost of automation.
- *Risks with shifting the intelligence*: A strategic risk with the application of machine learning in industrial applications, is that several classification and clustering techniques work very well, but do not offer any insights into why a model comes to these conclusions in a way that is understandable for human beings. Rather than reducing the cognitive load from operators and engineers, these enabling technologies may actually hamper user convenience and usability.
- *Compliance regulations and legal implications*: Industry 4.0 is heavily data driven. Each of the above objectives leverages context information from systems, customers and other assets. With data minimization being imposed in future privacy regulations, the question emerges what kind of trade-offs exists between purposefully reducing the amount and/or quality of sensitive information being collected and the ability to meet the above goals. Even as researchers, we will no longer be exempt from new compliance obligations and regulations when controlling or processing sensitive information.

Last but not least, we highly recommend the subsequent research articles in this thematic issue. In their own way, they each advance the fields towards the realization of truly intelligent industrial environments.

Acknowledgements

This research is partially funded by the Research Fund KU Leuven and by the European Commission through the H2020 project EXCELL (http://excell-project.eu/) under grant No. 691829.

References

[1] R. Ahmad and D. Kim, A collaboration based context prediction in smart office, *Journal of Ambient Intelligence and Smart Environments* **7**(6) (2015), 805–815. doi:10.3233/AIS-150348.

[2] K. Alexopoulos, S. Makris, V. Xanthakis, K. Sipsas and G. Chryssolouris, A concept for context-aware computing in manufacturing: The white goods case, *Int. J. Comput. Integr. Manuf.* **29**(8) (2016), 839–849. doi:10.1080/0951192X.2015.1130257.

[3] S. Aly, M. Pelikan and I. Vrana, A generalized model for quantifying the impact of ambient intelligence on smart workplaces: Applications in manufacturing, *Journal of Ambient Intelligence and Smart Environments* **6**(6) (2014), 651–673.

[4] L. Atzori, A. Iera and G. Morabito, The Internet of Things: A survey, *Comput. Netw.* **54**(15) (2010), 2787–2805. doi:10.1016/j.comnet.2010.05.010.

[5] J.C. Augusto, V. Callaghan, D. Cook, A. Kameas and I. Satoh, Intelligent environments: A manifesto, *Human-Centric Computing and Information Sciences* **3**(1) (2013), 1–18. doi:10.1186/2192-1962-3-12.

[6] B. Bencsáth, G. Pék, L. Buttyán and M. Félegyházi, The cousins of Stuxnet: Duqu, Flame, and Gauss, *Future Internet* **4**(4) (2012), 971–1003. doi:10.3390/fi4040971.

[7] V. Botón-Fernández, A.L. Tello, M. Pérez-Romero and E. Romero-Cadaval, Mining sequential patterns to efficiently manage energy storage systems within smart home buildings, *Journal of Ambient Intelligence and Smart Environments* **8**(3) (2016), 287–300. doi:10.3233/AIS-160381.

[8] A. Cavoukian, Privacy by Design: The 7 Foundational Principles, 2009.

[9] A. Cavoukian and J. Jonas, Privacy by Design in the age of Big Data, 2012.

[10] D. Christin, P.S. Mogre and M. Hollick, Survey on wireless sensor network technologies for industrial automation: The security and quality of service perspectives, *Future Internet* **2**(2) (2010), 96–125. doi:10.3390/fi2020096.

[11] A.W. Colombo, S. Karnouskos and J.M. Mendes, Factory of the future: A service-oriented system of modular, dynamic reconfigurable and collaborative systems, in: *Artificial Intelligence Techniques for Networked Manufacturing Enterprises Management*, L. Benyoucef and B. Grabot, eds, Springer, 2010. ISBN 978-1-84996-118-9.

[12] M.A. Dhuieb, F. Laroche and A. Bernard, Context-awareness: A key enabler for ubiquitous access to manufacturing knowledge, *Procedia CIRP* **41** (2016), 484–489. doi:10.1016/j.procir.2015.12.027.

[13] G. Ermacora, S. Rosa and A. Toma, Fly4SmartCity: A cloud robotics service for smart city applications, *Journal of Ambient Intelligence and Smart Environments* **8**(3) (2016), 347–358. doi:10.3233/AIS-160374.

[14] H. Flatt, N. Koch, C. Röcker, A. Günter and J. Jasperneite, A context-aware assistance system for maintenance applications in smart factories based on augmented reality and indoor localization, in: *2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)*, 2015, pp. 1–4.

[15] P. Gaj, J. Jasperneite and M. Felser, Computer communication within industrial distributed environment – A survey, *IEEE Transactions on Industrial Informatics* **9**(1) (2013), 182–189. doi:10.1109/TII.2012.2209668.

[16] K. Ganapathy, V. Vaidehi and D. Poorani, Sensor based efficient decision making framework for remote healthcare, *Journal of Ambient Intelligence and Smart Environments* **7**(4) (2015), 461–481. doi:10.3233/AIS-150330.

[17] D. Gorecky, M. Schmitt, M. Loskyll and D. Zühlke, Human–machine-interaction in the industry 4.0 era, in: *2014 12th IEEE International Conference on Industrial Informatics (INDIN)*, 2014, pp. 289–294. doi:10.1109/INDIN.2014.6945523.

[18] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Gener. Comput. Syst.* **29**(7) (2013), 1645–1660. doi:10.1016/j.future.2013.01.010.

[19] V.C. Gungor and G.P. Hancke, *Industrial Wireless Sensor Networks: Applications, Protocols, and Standards*, 1st edn, CRC Press, Boca Raton, FL, USA, 2013.

[20] W. Ikram and N.F. Thornhill, Wireless communication in process automation: A survey of opportunities, requirements, concerns and challenges, in: *IET Conference Proceedings*, Institution of Engineering and Technology, 2010, pp. 471–476(5).

[21] E. Ilie-Zudor, A. Ekárt, Z. Kemeny, C. Buckingham, P. Welch and L. Monostori, Advanced predictive-analysis-based decision support for collaborative logistics networks, *Supply Chain Management: An International Journal* **20**(4) (2015), 369–388. doi:10.1108/SCM-10-2014-0323.

[22] E. Ilie-Zudor, Z. Kemény and D. Preuveneers, Efficiency and security of process transparency in production networks – A view of expectations, obstacles and potentials, *Procedia CIRP* **52** (2016), 84–89.

[23] H. Kagermann, W. Wahlster and J. Helbig, Recommendations for implementing the strategic initiative Industrie 4.0 – Securing the future of German manufacturing industry, Final report of the Industrie 4.0 Working Group, Forschungsunion im Stifterverband für die Deutsche Wirtschaft e. V., Berlin, 2013.

[24] S. Karnouskos, A.W. Colombo, T. Bangemann, K. Manninen, R. Camp, M. Tilly, P. Stluka, F. Jammes, J. Delsing and J. Eliasson, A SOA-based architecture for empowering future collaborative cloud-based industrial automation, in: *IECON 2012 – 38th Annual Conference on IEEE Industrial Electronics Society*, 2012, pp. 5766–5772. doi:10.1109/IECON.2012.6389042.

[25] B. Kehoe, S. Patil, P. Abbeel and K. Goldberg, A survey of research on cloud robotics and automation, *IEEE Transactions on Automation Science and Engineering* **12**(2) (2015), 398–409. doi:10.1109/TASE.2014.2376492.

[26] M. Langheinrich, Privacy by design – Principles of privacy-aware ubiquitous systems, in: *Proceedings of the 3rd International Conference on Ubiquitous Computing, UbiComp '01*, Springer-Verlag, London, UK, 2001, pp. 273–291.

[27] R. Langner, Stuxnet: Dissecting a cyberwarfare weapon, *IEEE Security and Privacy*, **9**(3) (2011), 49–51. doi:10.1109/MSP.2011.67.

[28] E.A. Lee, Cyber physical systems: Design challenges, in: *Proceedings of the 2008 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing, ISORC '08*, IEEE Computer Society, Washington, DC, USA, 2008, pp. 363–369. doi:10.1109/ISORC.2008.25.

[29] J. Lee, B. Bagheri and H.-A. Kao, A cyber-physical systems architecture for Industry 4.0-based manufacturing systems, *Manufacturing Letters* **3** (2015), 18–23. doi:10.1016/j.mfglet.2014.12.001.

[30] J. Lee, H.-A. Kao and S. Yang, Service innovation and smart analytics for Industry 4.0 and big data environment, *Procedia CIRP* **16** (2014), 3–8.

[31] X. Li, D. Li, J. Wan, A.V. Vasilakos, C.-F. Lai and S. Wang, A review of industrial wireless networks in the context of Industry 4.0, *Wirel. Netw.* **23**(1) (2017), 23–41. doi:10.1007/s11276-015-1133-7.

[32] W.T. Lunardi, E. de Matos, R. Tiburski, L.A. Amaral, S. Marczak and F. Hessel, Context-based search engine for industrial IoT: Discovery, search, selection, and usage of devices, in: *2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA)*, 2015, pp. 1–8.

[33] S. Mekid, P. Pruschek and J. Hernandez, Beyond intelligent manufacturing: A new generation of flexible intelligent NC machines, *Mechanism and Machine Theory* **44**(2) (2009), 466–476. doi:10.1016/j.mechmachtheory.2008.03.006.

[34] D. Merico, Tracking with high-density, large-scale wireless sensor networks, *Journal of Ambient Intelligence and Smart Environments* **2**(4) (2010), 441–442.

[35] L. Monostori, Cyber-physical production systems: Roots, expectations and R&D challenges, *Procedia CIRP* **17** (2014), 9–13.

[36] L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn and K. Ueda, Cyber-physical systems in manufacturing, *CIRP Annals – Manufacturing Technology* **65**(2) (2016), 621–641. doi:10.1016/j.cirp.2016.06.005.

[37] L. Monostori, A. Markus, H. Van Brussel and E. Westkampfer, Machine learning approaches to manufacturing, *CIRP Annals – Manufacturing Technology* **45**(2) (1996), 675–712.

[38] A. Nicholson, S. Webber, S. Dyer, T. Patel and H. Janicke, SCADA security in the light of cyber-warfare, *Comput. Secur.* **31**(4) (2012), 418–436. doi:10.1016/j.cose.2012.02.009.

[39] P. O'Donovan, K. Leahy, K. Bruton and D.T.J. O'Sullivan, Big data in manufacturing: A systematic mapping study, *Journal of Big Data* **2**(1) (2015), 20. doi:10.1186/s40537-015-0028-x.

[40] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, Context aware computing for the Internet of Things: A survey, *IEEE Communications Surveys Tutorials* **16**(1) (2014), 414–454. doi:10.1109/SURV.2013.042313.00197.

[41] T. Pfeiffer, J. Hellmers, E.M. Schön and J. Thomaschewski, Empowering user interfaces for Industrie 4.0, *Proceedings of the IEEE* **104**(5) (2016), 986–996. doi:10.1109/JPROC.2015.2508640.

[42] D.T. Pham and A.A. Afify, Machine-learning techniques and their applications in manufacturing, *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture* **219**(5) (2005), 395–412. doi:10.1243/095440505X32274.

[43] M.A. Pisching, F. Junqueira, D.J.S. Filho and P.E. Miyagi, Service composition in the cloud-based manufacturing focused on the Industry 4.0, in: *Technological Innovation for Cloud-Based Engineering Systems*, Springer International Publishing, Cham, Switzerland, 2015, pp. 65–72.

[44] D. Preuveneers and W. Joosen, Security and privacy controls for streaming data in extended intelligent environments, *Journal of Ambient Intelligence and Smart Environments* **8**(4) (2016), 467–483. doi:10.3233/AIS-160384.

[45] N.P. Pulido, J.A. López-Riquelme, J.F. Melero, M.Á.V. Rodríguez and A.J. Barrios-León, A service robot for monitoring elderly people in the context of ambient assisted living, *Journal of Ambient Intelligence and Smart Environments* **6**(6) (2014), 595–621.

[46] R.R. Rajkumar, I. Lee, L. Sha and J. Stankovic, Cyber-physical systems: The next computing revolution, in: *Proceedings of the 47th Design Automation Conference, DAC '10*, ACM, New York, NY, USA, 2010, pp. 731–736.

[47] A.A.K. S., K. Ovsthus and L.M. Kristensen, An industrial perspective on wireless sensor networks – A survey of requirements, protocols, and challenges, *IEEE Communications Surveys Tutorials*, **16**(3) (2014), 1391–1412. doi:10.1109/SURV.2014.012114.00058.

[48] A.R. Sadeghi, C. Wachsmann and M. Waidner, Security and privacy challenges in industrial Internet of Things, in: *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1–6.

[49] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelfflé (eds), *Vision and Challenges for Realising the Internet of Things*, Publications Office of the European Union, Luxembourg, 2010.

[50] L. Sweeney, *k*-anonymity: A model for protecting privacy, *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* **10**(5) (2002), 557–570. doi:10.1142/S0218488502001648.

[51] K.J. Turner, Flexible management of smart homes, *Journal of Ambient Intelligence and Smart Environments* **3**(2) (2011), 83–109.

[52] A. Varghese and D. Tandur, Wireless requirements and challenges in Industry 4.0, in: *2014 International Conference on Contemporary Computing and Informatics (IC3I)*, 2014, pp. 634–638. doi:10.1109/IC3I.2014.7019732.

[53] J.M. Victor, The EU general data protection regulation: Toward a property regime for protecting data privacy, *Yale Law Journal* **123**(2) (2013), 513–528.

[54] S. Wang, J. Wan, D. Li and C. Zhang, Implementing smart factory of Industrie 4.0: An outlook, *Int. J. Distrib. Sen. Netw.* **2016** (2016), 3159805. doi:10.1155/2016/3159805.

[55] T. Wuest, C. Irgens and K.-D. Thoben, An approach to monitoring quality in manufacturing using supervised machine learning on product state data, *Journal of Intelligent Manufacturing* **25**(5) (2014), 1167–1180. doi:10.1007/s10845-013-0761-y.

[56] T. Wuest, D. Weimer, C. Irgens and K.-D. Thoben, Machine learning in manufacturing: Advantages, challenges, and applications, *Production & Manufacturing Research* **4**(1) (2016), 23–45. doi:10.1080/21693277.2016.1192517.

[57] L.D. Xu, W. He and S. Li, Internet of Things in industries: A survey, *IEEE Transactions on Industrial Informatics* **10**(4) (2014), 2233–2243. doi:10.1109/TII.2014.2300753.