Computers in Industry 81 (2016) 128–137

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook

Radu F. Babiceanu[a,*], Remzi Seker[b]

[a] Associate Professor of Systems Engineering, Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA
[b] Professor of Computer Science, Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA

ARTICLE INFO

Article history:
Received 16 April 2015
Received in revised form 22 December 2015
Accepted 29 February 2016
Available online 8 March 2016

Keywords:
Sensor-based real-time monitoring
Big Data
Internet of things
Cloud computing
Manufacturing cyber-physical systems

ABSTRACT

The recent advances in sensor and communication technologies can provide the foundations for linking the physical manufacturing facility and machine world to the cyber world of Internet applications. The coupled manufacturing cyber-physical system is envisioned to handle the actual operations in the physical world while simultaneously monitor them in the cyber world with the help of advanced data processing and simulation models at both the manufacturing process and system operational levels. Moreover, a sensor-packed manufacturing system in which each process or piece of equipment makes available event and status information, coupled with market research for true advanced Big Data analytics, seem to be the right ingredients for event response selection and operation virtualization. As a drawback, the resulting manufacturing cyber-physical system will be vulnerable to the inevitable cyber-attacks, unfortunately, so common for the software and Internet-based systems. This reality makes cybersecurity penetration within the manufacturing domain a need that goes uncontested across researchers and practitioners. This work provides a review of the current status of virtualization and cloud-based services for manufacturing systems and of the use of Big Data analytics for planning and control of manufacturing operations. Building on already developed cloud business solutions, cloud manufacturing is expected to offer improved enterprise manufacturing and business decision support. Based on the current state-of-the-art cloud manufacturing solutions and Big Data applications, this work also proposes a framework for the development of predictive manufacturing cyber-physical systems that include capabilities for attaching to the Internet of Things, and capabilities for complex event processing and Big Data algorithmic analytics.

1. Introduction

The current manufacturing global operations asks for more and stringent requirements than ever before, such as strict deadlines, low inventories, uncertain demand, standardization of manufacturing processes, product diversity, and security aspects [1]. Enhancing the manufacturing environment for more visibility and better control of the production processes becomes essential. Advances in sensor and communication technologies can provide the foundations for linking the physical facility and machine world to the cyber world of Internet applications and the software world. The coupled Manufacturing Cyber-Physical System (M-CPS) is envisioned to handle the actual operations in the physical world while simultaneously monitor them in the cyber world with the help of advanced data processing and simulation models at both the manufacturing process and system operational levels [2]. Moreover, a sensor-packed manufacturing system in which each process or piece of equipment makes available event and status information, coupled with market research for true advanced Big Data analytics, seem to be the right ingredients for event response selection and operation virtualization, and thus moving manufacturing operations closer to the cloud manufacturing paradigm [3]. As a drawback, the resulting M-CPS will be vulnerable to the inevitable cyber-attacks, unfortunately, so common for the software and Internet-based systems. This reality makes cybersecurity penetration within the manufacturing

* Corresponding author.
E-mail addresses: babicear@erau.edu (R.F. Babiceanu), sekerr@erau.edu (R. Seker).

http://dx.doi.org/10.1016/j.compind.2016.02.004
0166-3615/

domain a need that goes uncontested across researchers and practitioners.

The globalization trend, exhibited by the world economy for a while now, comes with significant challenges for the manufacturing industries of both developed and under development countries. The new predictive manufacturing paradigm, which is referred to more and more in recent peer-reviewed publications and proposal solicitations for funding competitions, is transformative in name. But more so, this new paradigm will be transformative in its implementation [4]. While the tools seem to be already available, what is needed is their customization for the manufacturing domain, new integration architectures and control algorithms, and mostly the willingness of the manufacturing actors. Tools such as cyber-physical devices, Big Data, IT infrastructures are now ubiquitous available. Manufacturing domain needs to take a hard look at them and perform the necessary customized integration.

This work provides a comprehensive literature review of the current status of virtualization and cloud-based services for manufacturing systems and of the use of Big Data analytics for planning and control of manufacturing operations. In the enterprise context, cloud solutions usually consider the business layer and address the needed tighter interaction with the customer and the integration with suppliers, competition, and regulatory bodies [2]. Building on already developed cloud business solutions, cloud manufacturing is expected to offer improved enterprise manufacturing and business decision support. Based on the current state-of-the-art of cloud manufacturing solutions and Big Data manufacturing applications, this work also proposes a framework for the development of predictive M-CPS that include capabilities for attaching to the Internet of Things, and capabilities for complex event processing and Big Data algorithmic analytics [3]. The development challenges for the M-CPS as identified in the literature as well as uncovered by outlining and detailing the proposed framework are also discussed.

From this point forward the paper is structured as follows: Section 2 provides a review of the most important aspects of complex event processing, cloud computing and virtualization in manufacturing, Internet of Things, Big Data analytics, and cybersecurity within the manufacturing domain. Then, Section 3 presents modeling framework guidelines for the manufacturing cyber-physical system, detailing certain critical modeling aspects and instantiates the predictive manufacturing systems paradigm. Finally, the future outlook for manufacturing cyber-physical systems is sketched and needed research is outlined.

2. Manufacturing cyber-physical systems component technologies and processes review

The technologies and processes that make possible the creation of M-CPS are already in use in other domains, some of them also reaching a certain degree of maturity. However, the penetration of these technologies and/or processes into the manufacturing domain is slower compared to other domains. This is due to the nature of manufacturing operations, which need to deal with large pieces of hardware equipment, many of them being legacy systems, the high cost of manufacturing equipment, which makes it unlikely to be replaced before the end of its useful life, and the resistance of senior management to the introduction of new technologies in already well-adjusted processes and systems. Still, the march of technology is an unstoppable one-way direction road, and manufacturing domain cannot and will not go against the technology wave. Ubiquitous computing in general is a reality and the first steps towards ubiquitous manufacturing, defined as the use of IT available tools as part of the manufacturing domain, are already reported in the literature. Ferreira et al. [5] propose a manufacturing architecture where ubiquity and effectiveness are enabled by cloud platforms and layers of new services directed to communication between users. Kiirikki and Haag [6] apply the ubiquitous computing concepts to manufacturing assembly cells, Lee et al. [7] apply them to decision support systems, while Horvath and Vroom [8] study their application to computer-aided design (CAD). Nevertheless, there are remaining challenges that need to be addressed not only for ubiquitous manufacturing, but also in the area of general ubiquitous computing. Botta et al. [9] attempt to identify the most pressing ubiquitous computing challenges within the cloud computing-Internet of Things workspace, as follows: standardization, power and energy efficiency, Big Data, security and privacy, network integration, and network communications, and others related to management operations. Several of these identified challenges are also part of the proposed M-CPS model.

2.1. Complex event processing in the manufacturing domain

Manufacturing domain is driven by events, and many times those events are collected through sensors and/or executed by actuators. Any action, activity, or monitored parameter change, which influences the operational status of a manufacturing process or system, is viewed as an event. When simultaneous or a series of time-ordered simple events occur, the resulting set of events is viewed as a complex event. The objective of complex event processing is described by Luckham [10] as the identification of game-changing events, in the form of opportunities and/or threats, and the generation of a reasonable answer within certain timing constraints. As an example, Nagorny et al. [11] consider the deployment of sensor/actuator cyber-physical devices and implements their collected events in Petri Nets models that support reasoning-based control, monitoring, and management functionalities. The implemented virtualization transfers all the data processing in the cloud and makes it available for all registered users. Attempts to formalize the process and make it available in the cloud have also been made. For example, Prabhu [12] proposes that a cyber-physical device data collection event be modeled as a set (device ID, event ID, time), which is initialized and changed at any times when the sensors or actuators collect or receive data.

At the shop-floor level, traditionally, manufacturing operations are event-based operations controlled using programmable logic controllers (PLC) and computer numerical controlled (CNC) resources. The forward step to operations virtualization and cloud-shared manufacturing files needs also consider the shop-floor aspects for legacy reasons, as many manufacturers will still use the traditional technology for a while. Chaplin et al. [13] propose a solution for the integration of legacy PLC and CNC controllers into a decentralized, context-aware, data distribution service, which can be used as a model for linking legacy systems to IT-cloud based systems. Other literature models related to integration of legacy systems into Internet-based systems are reported by Bodenheim et al. [14] for PLC controllers and by Hentz et al. [15] for CNC controllers.

Besides the expected events that drive manufacturing operations, at unknown points during manufacturing cycles, unexpected detrimental simple events, or aggregation of events, may also occur. The capability of manufacturing operations to cope with complex events and respond in acceptable time is called resilience. A more formal definition of resilience is found in literature [16] and addresses the ability to prepare for, absorb, and recover from actual or potential adverse events. Francis and Bekera [17] conducted an ample study on resilience, which includes the following characteristics: system identification, resilience objective, vulnerability analysis, and stakeholder engagement. A resilient manufacturing system model designed to sustain

operations in face of disturbances is proposed by Gu et al. [19]. Furthermore, Zhang and van Luttervelt [18] propose the concept of resilient manufacturing systems, together with the guidelines for the design and management of such systems. The authors define manufacturing resilience as a function of failure recovery capability, where failures exist as one or more of the following types: (1) user's demand is not satisfied; (2) required resources are not available; (3) resources are, at least, partially damaged; (4) raw materials do not exhibit the required quality; and, (5) resources are detrimental to the environment where they operate, or to the environment in general. The guidelines proposed include the need for (1) design redundancy at large; (2) component multiple function management; (3) component learning and training management; and, (4) manufacturing system ontology modeling.

2.2. Cloud computing and virtualization in the manufacturing domain

Cloud computing has been around since late 2000 s and has arrived recently at a mature development, as many every day user applications and also large business processes are performed exclusively in the cloud. Cloud computing considers every type of needed resource/process as a service, which is also called Everything as a Service (XaaS), where everything is dubbed either as software (SaaS), hardware (HaaS), platform (PaaS), infrastructure (IaaS), or lower level component services such as Sensor as a Service (SenaaS) or Sensor Event as a Service (SEaaS) [20]. Compared to other industries, manufacturing is late at profiting from all the benefits that computing in the cloud has to offer. But steadily in the last years, cloud computing is emerging as one of the major enablers for the manufacturing industry [21].

Two definitions for cloud manufacturing raised the attention during the literature survey. First, Li et al. [22] define cloud manufacturing as a "computing and service-oriented manufacturing model developed from existing advanced manufacturing models and enterprise information technologies under the support of cloud computing, the Internet of Things, virtualization and service-oriented technologies, and advanced computing technologies." The second definition provides more in-depth information in terms of supported resources and processes, as Xu [23] views cloud manufacturing as a "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable manufacturing resources (e.g., manufacturing software tools, manufacturing equipment, and manufacturing capabilities) that can be rapidly provisioned and released with minimal management effort or service provider interaction." During cloud manufacturing operations, users register with the cloud according to their requirements and can request services ranging from product design, manufacturing, testing, management, and all other stages of a product life cycle [23].

Another work, by Wu et al. [24] proposes the use of cloud services for both the design and manufacturing activities and names the resulting combined process as cloud-based design and manufacturing (CBDM). The resulting CBDM model considers shared access to a collection of diversified and distributed manufacturing resources that form temporary, reconfigurable production lines and are expected to improve efficiency, reduce lifecycle costs, and provide optimal resource allocations. The above referenced CBDM system, and also any other cloud manufacturing system for that matter, are expected to meet specific computing in the cloud requirements such as [24]:

- Social media capabilities to support communication and information sharing.
- Cloud-based distributed file systems for ubiquitous access to data.
- Open-source programming framework to process and analyze Big Data.
- Sharing of capabilities for same software instance.
- Real-time data collection from cyber-physical devices and storage in the cloud.
- Remote monitoring and control capabilities.
- SaaS, HaaS, PaaS, and IaaS services.
- Intelligent search engine to answer queries.
- Instant quotes in response to submitted service specifications.

Yet another name given to cloud manufacturing is Cyber-Physical Production Systems (CPPS), which is mentioned to rely on computer science developments, information and communication technologies (ICT), and manufacturing science and technology (MST) roots such as: intelligent manufacturing systems (IMS), biological manufacturing systems (BMS), reconfigurable manufacturing systems (RMS), digital factories (DF), and holonic manufacturing systems (HMS) [25,26].

Virtualization in manufacturing is a needed process conducted to make simulation capabilities available in the cloud or deliver the needed copy of the actual physical manufacturing process application, and thus, transforming the manufacturing cyber-physical system into a collaborative project work over different virtual platforms and across several physical environments. More specifically, virtualization in manufacturing refers to identifying the logic behind the physical resource operation and translating it into the cyber space in order to improve agility, enhance flexibility and reduce cost [27]. Several implementation platforms are reported in the literature. For example, Nagorny et al. [10] describe an approach for developing and implementing a service-oriented architecture based on the use of multi-agent systems that implements the IEC 62264 Level 2 standard. More insights in the concepts and implementation of cloud manufacturing and manufacturing execution systems virtualization can be gained by reviewing the works of Wang et al. [28], Wu et al. [29], Helo et al. [30], Wang [31], and Wu et al. [24].

In an actual implementation, Morariu et al. [32] discuss the virtualization concepts applicable to manufacturing execution systems and propose a laboratory pilot implementation reporting its benefits and limitations. Though not a pure manufacturing application, the cyber-physical approach for planning and control of maintenance, repair, and overhaul operations of a fleet of complex transportation systems proposed by Trentesaux et al. [33] provides the foundations for an optimized modeling methodologies that can be adopted with minimal customization for manufacturing domains.

2.3. Internet of things adoption in the manufacturing domain

In the recent years, with the advances in sensor and communication technologies, there is a surge in the volume of literature in the areas of Internet of Things (IoT) and Cyber-Physical Systems (CPS) [34]. A simple IoT definition describes a system where objects in the physical world, and sensors within or attached to these items, are connected to the Internet via wireless and wired network connections [35]. In the near future, the IoT is expected to connect everything around us, from objects, devices, and mobile systems used every day by the regular individual to small and large industrial equipment [36–38]. Moreover, Prabhu [11] envisions that the ubiquitous IoT will transform our world. The emerging IoT technology enables human or automated decision-makers to communicate with the physical devices. Within the IoT framework every device can collect, send and receive data enabled by communication technologies over wireless and cloud cyber-infrastructure [39,40].

For the manufacturing domain, the IoT will connect physical devices such as sensors, actuators, RFID tags and readers, GPS units, and high-definition cameras. The current state-of-the-art of manufacturing cyber-physical devices implementation into IoT having different levels of cloud services is presented by Wang et al. [41] together with directions of future research and applications that highlight the latest advancement in the field. A series of benefits expected from the implementation of IoT platforms in manufacturing operations are listed next: visibility of the manufacturing operations and across the supply chain, improved efficiencies, workflow automation, optimized energy consumption, improved preventive maintenance, and real-time information exchange among manufacturing facilities and across supply chain. Borgia [42] names the cyber-physical devices "smart objects," and considers that ubiquitous computing, the Internet Protocol (IP), sensing technologies, communication technologies, and embedded devices are merged together in order to form a system where the real and digital worlds meet and are continuously in symbiotic interaction. Within the IoT framework, these cyber-physical networks of devices perform their sensing, collecting, sending and receiving of data and can be looked at as a bridge between the Internet and the physical objects (i.e., manufacturing resources, facilities, and equipment, as well as physical inventory of raw materials, work-in-process, and finished products). Actually, these cyber-physical networks of devices are also called the Physical Internet in some works. Significant insights related to the concepts and implementation of IoT in the manufacturing domain can be gained by reviewing the works of Gubia et al. [43], Gerben et al. [44], Atzori et al. [45], and Miorandi et al. [46]. Of particular interest for the manufacturing domain is the resource management for IoT and cloud-based systems. Pop and Bessis [47] provide a review of the resource management architectures, models, and algorithms for energy-efficient message delivery covering the fault-tolerant cloud environments.

Qiu et al. [48] consider that the emergence of IoT offers solutions to achieve real-time visibility and information sharing from all levels of manufacturing operations. Their proposed supply hub model includes three key components, the physical asset service system (to include both passive and active objects), the information infrastructure, and a decision support system, which are networked to the IT enterprise system. It can be argued that virtualization on the cloud is the next logical step for the proposed model. Shrouf and Miragliotta [49] discuss energy efficient production management practices based on solutions offered by IoT and the resulting benefits of the proposed IoT-based solution adoption.

Another manufacturing CPS system application model is presented by Grieco et al. [50]. Given the penetration of robotics application in everyday life as well as in industrial applications, the authors argue that IoT-aided robotics applications will become common in the near future manufacturing applications. Wang [51] addresses the need for offering software applications, such as shop-floor process planning, as SaaS in collaborating manufacturing networks formed by small and medium enterprises (SMEs).

2.4. Big data analytics for the manufacturing domain

Big Data is another recent area of research with applicability in countless domains, including manufacturing. Just as in the case of cloud computing and IoT, manufacturing applications of Big Data are lagging in penetration and diversity compared to other domains, such as information science, policy and decision making, marketing, healthcare, or business processes [52]. A very important aspect of Big Data research is data analysis, without which the other Big Data aspects such as collection, storage, and use would not have much value. This is a direct result of the fact that unstructured data makes up to 95% of the data labeled as "Big Data" [19]. Big Data processing requires tools and techniques that leverage the combination of four key computing resources: process capability, memory, storage, and network, such as Hadoop Distributed File System (HDFS), MapReduce, YARN, HBase, HiveQL, NoSQL, and others [53].

Literature characterizes Big Data as large data sets having at least three distinct agreed dimensions, regardless the source of information or reference used [54]. Called the Big Data three "V's", these three main dimensions are agreed across the literature as follows:

- Volume: data is generated in large amounts.
- Variety: data is generated in different formats.
- Velocity: data is generated almost continuously.

Appropriate and efficient analytical methods are needed to process the large amounts of unstructured heterogeneous data collected continuously in formats such as text, audio, video, log file, or others. Due to the specificity and also ubiquity of Big Data in many domains, more recent works [55–59] attempt to assign other dimensions to the collected data labeled as Big Data, such as:

- Value: data generated should exhibit useful purposes; ensures data collected brings added-value to the intended process, and also addresses aspects such as broader use of information.
- Veracity: data generated exhibits consistency and trustworthiness; ensures statistical reliability of data and trusted and authentic origin, protected from unauthorized access and modification.
- Vision: data generated should come from a purposeful process; addresses the likelihood of data generation process.
- Volatility: data generated may have a limited useful life; addresses the lifecycle concept of data and ensures new data replenishes the outdated data.
- Verification: data generated should conform to a set of specifications; ensures engineering measurements are correct.
- Validation: data generated should conform to its vision; ensures transparency of assumptions and connections behind the process.
- Variability: data generated has a level of uncertainty or impreciseness; addresses aspects such as data inconsistency, incompleteness, ambiguities, latency, deception and approximations.

Adding the above "V" dimensions in the effort to analyze Big Data does not result in limitations of Big Data processing for manufacturing domains. The added six dimensions essentially provide a better characterization, from the engineering viewpoint, of the data collected from manufacturing applications and their related processes. Also, the process comprehension offered by Big Data analysis comes from more than just the first three "V" dimensions. It is the engineering aspects that give value to Big Data analytics for manufacturing domain [60].

Big Data projects implementation for manufacturing domain includes similar cycles as for the more general Big Data projects, namely: stating the business problem, data research, cross functional team formation, project roadmap, data collection and examination, data modeling and analysis, data visualization, insight generation, integration with IT systems, and training professionals [61]. Manufacturing Big Data projects could use insights that are already available coming from related domains, such as supply chain, logistics, and business environments. Loebbecke and Picot [62] argue that Big Data analytics will reshape business models and influence employment for knowledge-based workers in the same way as automation

influenced manufacturing workers decades ago. A personalized information recommendation system for opportunity finding in Big Data context is proposed by Xu et al. [63], which includes Big Data filtering and aggregation models. Also, unstructured Twitter data was analyzed by Chae [64] through descriptive analytics, content analytics, text mining, network analytics, visualization, and metrics techniques to make sense out of 22,399 hashtag #supplychain tweets. Finally, Big Data analytics is reported to enable timely and accurate insights for better manufacturing decisions, using machine learning, predictive analytics, HDFS, and MapReduce tools [65].

Dutta and Bose [61] present the Big Data implementation project at Ramco Cements Limited Company from India together with a framework that provides a holistic roadmap in conceptualizing, planning and successfully implementing Big Data projects. The presented results outline a series of lessons learned from the implementation project, labeled as essential for the success of manufacturing Big Data projects: flawless understanding of the business problem, detailed step-by-step project map, adoption of innovative visualization techniques, active involvement of management, and, last but not the least in importance, data driven decision making capabilities.

2.5. Cybersecurity for the manufacturing domain

Cybersecurity is a rapidly growing field in computer science which is devoted to safeguard the privacy, confidentiality, and integrity of digital data stored and/or transmitted in any format over internal networks and/or over the Internet. With daily attacks becoming more and more sophisticated, cybersecurity protection through firewalls, intrusion detection systems, and other systems, are becoming of utmost importance for individuals, businesses, and government alike [66]. Botta et al. [8] identify the challenges related to security and privacy of cloud and IoT systems, such as: session riding, SQL injection, cross site scripting, virtual machine escape, authorization roles and policies for sensitive data, compromised gateways, malware injection, etc. Besides the cyber-attacks characteristic for Internet-based systems, the cyber-physical devices, part of the M-CPS, represent a potential access point for an intruder into the network of devices, which ultimately can perpetuate to the entire system [67]. For example, Song et al. [68] argue that the existing synchronization scheme for wireless sensor networks, which made up a great number of cyber-physical devices to be deployed in M-CPS, were not initially designed for cybersecurity protection, which makes them an easy target for attackers. Weber [69] studies the attack-resilience, data authentication, access control, and client privacy in the context of IoT security and privacy challenges. Generally, the cyber-physical devices could be subjected to the following types of attacks [70]:

- Attacks on sensors and actuators.
- Attacks on the wireless communication and over the local network.
- Attacks on the maintenance mechanisms and physical interfaces.

To address the threat of attacks and limit the magnitude of unwanted consequences, adequate cybersecurity responses need to be implemented, such that the cyber-physical devices layer is attack-resilient and secure. More specifically, cybersecurity attacks directed to the cyber-physical devices can be categorized as follows [71]:

- Data integrity attacks, which are executed by corrupting the signals (measurements) of sensors or of the values of control signals. As a result of processing corrupted input values, the control unit would likely provide wrong solutions for the monitored process. Also, by using corrupted control signals, the control unit may direct the actuator to incorrectly action on the monitored process.
- Replay attacks, easily executed on an unsecured network through retransmission of legitimate control or measurement packets several times. These type of attacks are a variation of data integrity attacks and have the same negative consequences.
- Denial of service attacks, which result into unacceptable delays in the operation of the monitored process, or, many times, total unresponsiveness. Besides the obvious negative effect on applications having required real-time operational scenarios, any delays induced in the operational flow would be detrimental for the overall system efficiency.
- Timing attacks, which result only in delays of communication flow between the control unit and sensor/actuator cyber-physical device. These type of attacks are a variation of denial of service attacks and have the same consequences, albeit less dramatic, when no real-time requirements are imposed.
- De-synchronization attacks, which are directed towards the processes that require rigorous synchronization. Similar to timing attacks, these type of attacks are a variation of denial of service attacks and carry the same consequences.

At the M-CPS level, the resulting effects of these types of attacks could range from timing delays to failed cyber-devices, and to purposefully propagating incorrect data forward into other processes, which ultimately result in failed processes and significant losses. Related to cybersecurity and cloud manufacturing, the literature review witnessed the birth of a new discipline. Boyson [72] proposed the cyber supply chain risk management (CSCRM) as a new discipline designed to address the challenges of the rapid globalization and outsourced diffusion of hardware and software systems. CSCRM presents itself as an integrative discipline borrowing elements of cybersecurity, supply chain management, and enterprise risk management into a powerful concept to monitor and exert control of end-to-end processes of organizations and their supply chain collaborators. Wells et al. [73] provide specific insights in the needed cybersecurity processes for manufacturing domains and identify the significant threats of maintaining the conformity of products to their original design intent and also of maintaining the safety of equipment, employees, and consumers. Particular to manufacturing domain, the identified cybersecurity threats make the production process vulnerable to attacks over the entire product design and development cycle and anywhere in the manufacturing supply chain. Manufacturing files are not any more vulnerable only at, for example, the tool path level when errors are introduced, deliberately or not, in the computer-aided manufacturing (CAM) files, but also at any file sharing process over the networked organizations that work on collaborative projects. Having cybersecurity countermeasures in place ensure the confidentiality, availability, and integrity of data and IT systems by preventing or mitigating asset losses from attacks. Rees et al. [74] present decision support solutions for cybersecurity risk planning that can be easily adapted to the manufacturing domain. The trend towards Big Data and its required tools and techniques, presented in a previous section (MapReduce, HDFS, etc.), can be implemented securely by creating dynamic Big Data-driven application systems (DBDDAS) common in many systems, such as disaster management and traffic management, including manufacturing applications [75]. Characteristics of secure MapReduce and HDFS systems providing a specified level of privacy are also presented by Fabiano et al. [76].

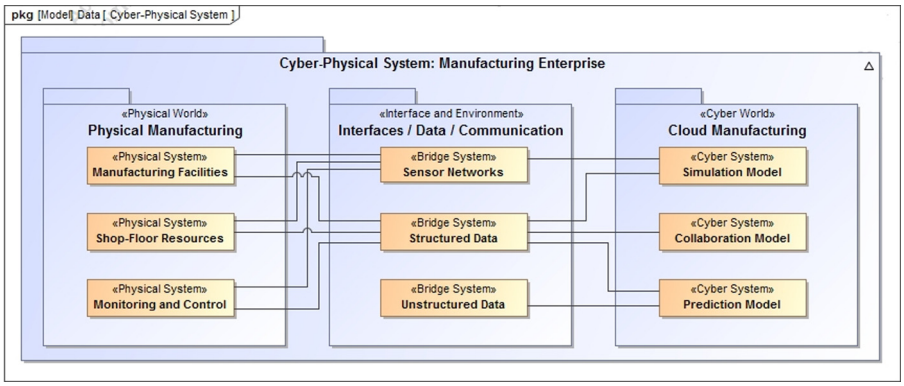

Fig. 1. The proposed manufacturing cyber-physical system.

3. Modeling guidelines for predictive manufacturing cyber-physical systems

3.1. Manufacturing cyber-physical system model

Previous work [2,3] provided a first glance at the M-CPS model, which includes both the physical world, where the traditional manufacturing system is located, and the cyber world, where the Internet connectivity resides and computing in the cloud is performed. In between the two worlds, there is a layer of cyber-physical devices, such as sensors and actuators, local area networks, and also application and cybersecurity software, that complete the cyber-physical system model depicted in Fig. 1 [2].

The layer of cyber-physical devices, when properly deployed and with the needed redundancy, are able to provide status control through the sensors and provide adjustments to any stages of the manufacturing operations through the actuators. For example, Fig. 2 depicts the change of the process conditions for the manufacturing of an engine component as a result of a complex event occurring: deformation of the engine component due to the resultant effect of the cutting and clamping device forces exhibited during the manufacturing process. Traditionally the finite element analysis (FEA) process is conducted offline as a result of the outcome of the quality control process. However, a sensor-packed manufacturing system would be able to acknowledge the occurrence of the complex event and signal the potential problem within the cyber world. The FEA would be, in this case, conducted online in the cyber world and would show precisely the occurrence of the complex event described above. Fig. 3 depicts the simulation performed offline for the profiles of the engine component and the cutting tool while in rotational move during the manufacturing process. The M-CPS cyber world would made possible the online simulation and, therefore, the needed adjustment decisions can be made and sent in real-time to the actuators located in the physical world.

All the data exchange operations of the proposed M-CPS model are scaled to certain levels of cloud mode environments to be supported by the model: private cloud, community cloud, and

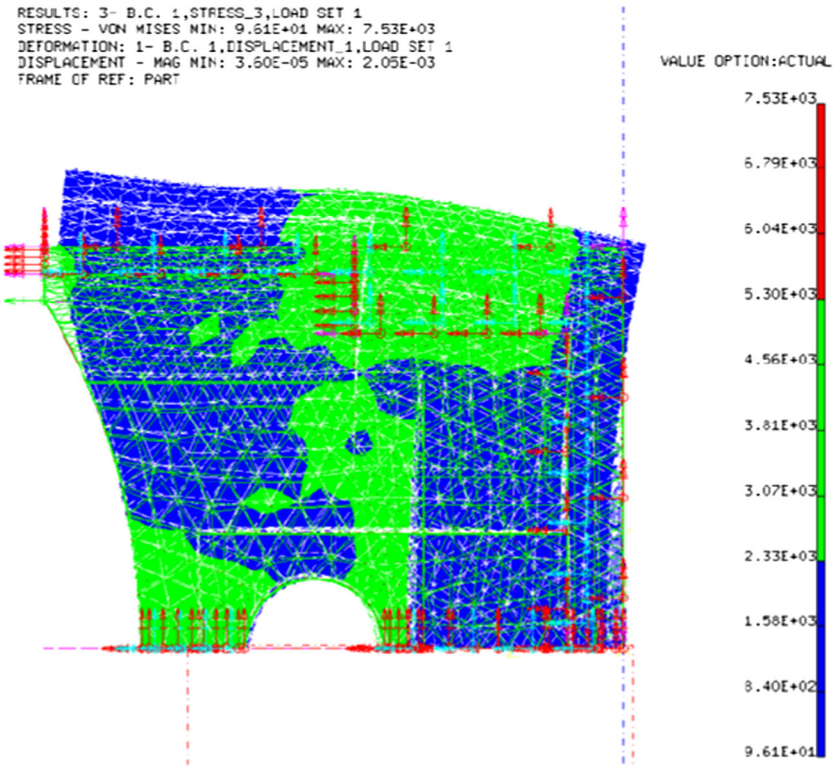

Fig. 2. Manufacturing process monitoring and complex event occurrence: Finite element analysis.

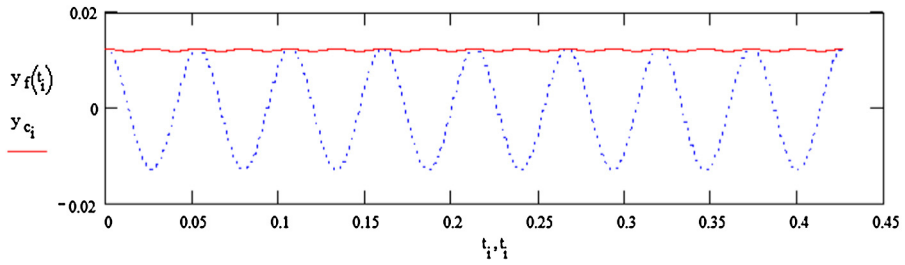

Fig. 3. Manufacturing process monitoring and complex event occurrence: Simulated profiles of the workpiece and cutting tool path.

public cloud. This scaled model enables authorized resource access only and enhances security and privacy of the shared data.

3.2. Big data generated and types

Structured and unstructured data were reported in previous articles to be generated and collected in the proposed M-CPS [2,3]. These data are illustrated in Fig. 4 below [2], where traditional structured manufacturing time-based and process data, cyber-physical device generated data, and unstructured external marketing, social networking, and customer support data are present. New Big Data processing tools must enable real-time data analysis, which is likely to result in significant improvements in real-time problem solving and reduced cost avoidance [35]. Related to Big Data, the cybersecurity data covering areas such as information security, network security, and cloud security, as well as the indirect cybersecurity aspects such as partnership security, through information sharing and collaboration, are outlined in the literature [2].

Krumeich et al. [77] propose seven requirements for Big Data processing which are adapted in this work to the predictive manufacturing domain, and presented in the below list.

- Provide scalable means for spreading out sensors throughout production/manufacturing processes and to store data in descriptive process and context models.
- Provide means for detecting and filtering of complex production/manufacturing events within streams of deployed sensor data.
- Provide means for real-time data storage capabilities to correlate and analyze Big Data collections and streams in terms of the identified "V" dimensions.
- Provide means for deriving and continuously adjusting the complex event-based prediction models.
- Provide means for creating alerts as responses to predicted deviations from planned production/manufacturing process objectives based on calculated analytics.
- Provide means for deriving recommendations and automatic decisions for the mitigation of production/manufacturing actions.
- Provide means for enacting proactive process adaptations on the basis of computed recommendations and decisions.

3.3. Complex event processing for operational prediction

Resilient systems in the case of complex event processing are intrinsically related to notions such as risk and vulnerability. Several of the modeling and simulation approaches identified in the literature are listed here: identification of frequent and significant failure patterns, quantification of interdependency related indicators, empirically risk analyses, multi-agent systems approaches, system dynamics approaches, economic theory approaches, and network science approaches [78]. Two types of measure of resilience were identified [79]:

- Equilibrium resilience: this measure is proportional with the inverse of the time necessary for the system to return to its equilibrium state, where equilibrium state implies that external perturbation deviating system from equilibrium state decays and the system returns to the vicinity of the state.
- General resilience: this measure is proportional with the inverse of the time necessary for the system to reach its original state, which not necessarily is its equilibrium state.

The aim of complex event processing for the M-CPS system is to assess the vulnerabilities of the manufacturing domain and provide an associated risk measure [80]. The objective of the proposed model is to assess the resiliency of the M-CPS in face of disruptions and failure from any cause. One of the metrics that can further improve the resiliency measure is the inclusion of behavior prediction modeling as an added stage of the overall resiliency modeling framework.

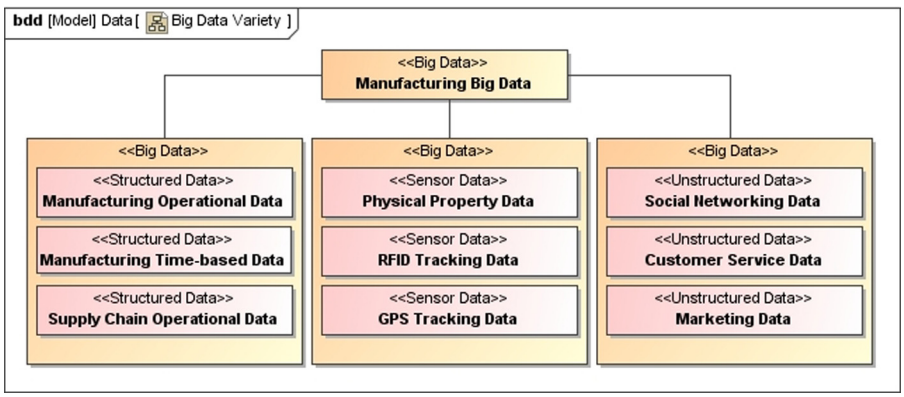

Fig. 4. Big Data generated by the manufacturing cyber-physical system.

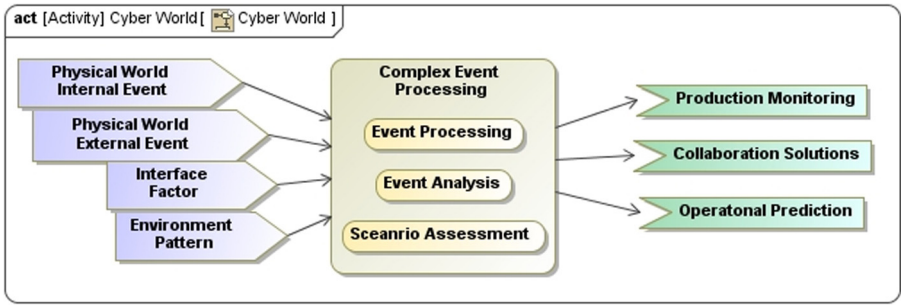

Fig. 5. Complex event processing in the manufacturing cyber-physical system.

As depicted above in Section 3.1, even simple complex event processing can be enhanced to more resilient operational solutions. Real-time accurate complex event processing is expected to be the basis for predictive operational solutions as illustrated in Fig. 5 below [2]. Using the guidance of the "V" dimensions, adequate algorithmic approaches are needed to realize the objective of prediction in manufacturing operations, or in any other processing domain for that matter. The predictive M-CPS capabilities are directed at the prediction of the location and timing occurrence of the next undesired events, as well as the prediction of the location and timing occurrence of the next opportunity events. In both cases, the prediction is to be made in the cyber world, but with direct online communication with the cyber-physical devices. By monitoring and triggering real-time changes of operations in the physical world, the M-CPS could actually achieve the desired predictive capabilities and appropriately adjust operational flow. Another example of prediction of manufacturing event occurrence is presented in [3], where survival analysis is used to estimate the amount of time until the next resource failure occurs.

4. Manufacturing cyber-physical systems: future outlook

This research outlines the advancements made in recent years in regard to the manufacturing-based customization of technologies and domains such as: IoT, Big Data, virtualization, cloud-based services, and cybersecurity. While there is significant more basic and applied research work needed for manufacturing to catch-up with other the more technology savvy domains, the gap is clearly shrinking, and it is expected that virtual/cloud/cyber manufacturing, or what this research calls M-CPS, will become a reality in real-world manufacturing settings, as well. To that objective, this research also proposes modeling guidelines for the development of M-CPS that include capabilities for attaching to the IoT, and capabilities for complex event processing and Big Data analytics for operational prediction.

Future work on the proposed predictive M-CPS will focus on developing Big Data algorithms appropriate for manufacturing operations and building simulation models, running as part of the cyber world. Algorithm processing on Big Data platforms need to take into account the problem of scheduling a set of jobs across a set of machines, such as in HDFS distributed file systems, and specifically analyze the system performance at very high loads [81]. Also, specific cyber-security aspects mandatory for actual cyber-physical systems deployments will be identified. General research directions are mentioned below:

- Develop cyber world models for all levels of the M-CPS. These models will provide insights for many of the traditional manufacturing operational issues, such as: process and production planning, resource allocation, facilities and layout design, manufacturing scheduling, inventory management, etc.
- Develop cyber world models for supply chain collaboration of the M-CPS. These models will provide visibility, tracking and tracing across the supply chain, and will address traditional logistics engineering issues, such as: forecasting, resource allocation, inventory management, transportation, etc.
- Develop cyber world models for security, data privacy and information sharing for the cyber-physical devices, manufacturing applications, and the supply chain, that will be tested using intrusion detection, penetration testing and cryptography tools.
- Develop bridging physical world—cyber world models for complex event occurring and processing in the M-CPS. These hardware/software models will provide insights in the aggregation of events that can change M-CPS status, and will address the appropriateness of "what-if" scenarios.
- Develop physical world models for data collection and generation based on powerful FPGA boards that can physically communicate with several real cyber-physical devices at the same time.

To develop the above cyber and physical world models, existing work in intelligent systems and context-aware environments for the IoT is likely to prove valuable. Cristea et al. [82] discuss the challenges, state-of-the-art, and future trends in context aware environments, both from the infrastructure and services points of view. Physical world components are envisioned to develop awareness of the context in which they operate and to cooperate with other IoT components.

References

[1] S. Mejjaouli, R.F. Babiceanu, Holonic condition monitoring and fault-recovery system for sustainable manufacturing enterprises, in: T. Borangiu, A. Thomas, D. Trentesaux (Eds.), Service Orientation in Holonic and Multi-agent Manufacturing, 544, Springer, Berlin, Germany, 2014, pp. 31–46.
[2] R.F. Babiceanu, R. Seker, Manufacturing cyber-physical systems enabled by complex event processing and Big Data environments: a framework for development, in: T. Borangiu, A. Thomas, D. Trentesaux (Eds.), Service Orientation in Holonic and Multi-agent Manufacturing, 594, Springer, Berlin, Germany, 2015, pp. 165–173.
[3] R.F. Babiceanu, R. Seker, Manufacturing operations, internet of things, and big data: towards predictive manufacturing systems, in: T. Borangiu, A. Thomas, D. Trentesaux (Eds.), Service Orientation in Holonic and Multi-agent Manufacturing, 594, Springer, Berlin, Germany, 2015, pp. 157–164.
[4] J. Lee, E. Lapira, B. Bagheri, H. Kao, Recent advances and trends in predictive manufacturing systems in big data environment, Manuf. Lett. 1 (2013) 38–41.
[5] L. Ferreira, G. Putnik, M. Cunha, Z. Putnik, H. Castro, C. Alves, V. Shah, M.L.R. Varela, Cloudlet architecture for dashboard in cloud and ubiquitous manufacturing, Procedia CIRP 12 (2013) 366–371.
[6] J. Kiirikki, M. Haag, Ubiquitous assembly cell concept and requirements, Procedia CIRP 12 (2013) 157–162.
[7] K.C. Lee, N. Chung, J. Byun, Understanding continued ubiquitous decision support system usage behavior, Telemat. Inform. 32 (2015) 921–929.
[8] I. Horvath, R.W. Vroom, Ubiquitous computer aided design: a broken promise or a sleepy beauty? Comput. Aided Des. 59 (2015) 161–175.

[9] A. Botta, W. de Donato, V. Persico, A. Pescape, Integration of cloud computing and internet of things: a survey, J. Future Gener. Comput. Syst. 56 (2016) 684–700.
[10] D. Luckham, The Power of Events: An Introduction to Complex Event Processing in Distributed Enterprise Systems, Addison-Wesley Professional, Boston, MA, 2002.
[11] K. Nagorny, A.W. Colomba, U. Schmidtmann, A service- and multi-agent-oriented manufacturing automation architecture: an IEC 62264 level 2 compliant implementation, Comput. Ind. 63 (2012) 813–823.
[12] N. Prabhu, Design and Construction of an RFID-Enabled Infrastructure: The Next Avatar of the Internet, Taylor & Francis, Boca Raton, FL, 2014.
[13] J.C. Chaplin, O.J. Bakker, L. de Silva, D. Sanderson, E. Kelley, B. Logan, S.M. Ratchev, Evolvable assembly systems: a distributed architecture for intelligent manufacturing, IFAC-Papers Online 48 (3) (2015) 2065–2070.
[14] R. Bodenheim, J. Butts, S. Dunlap, B. Mullins, Evaluation of the ability of Shodan search engine to identify internet-facing control devices, Int. J. Crit. Infrastruct. Prot. 7 (2) (2014) 114–123.
[15] J.B. Hentz, V.K. Nguyen, W. Maeder, D. Panarese, J.W. Gunnik, A. Gontarz, P. Stavropoulos, K. Hamilton, J.Y. Hascoet, An enabling digital foundation towards smart machining, Procedia CIRP 12 (2013) 240–245.
[16] S.S. Shah, R.F. Babiceanu, Resilience modeling and analysis of interdependent infrastructure systems, Systems and Information Engineering Design Symposium (2015) 154–158.
[17] R. Francis, B. Bekera, A metric and frameworks for resilience analysis of engineered and infrastructure systems, Reliab. Eng. Syst. Saf. 121 (2011) 90–103.
[18] W.J. Zhang, C.A. van Luttervelt, Toward a resilient manufacturing systems, CIRP Ann. Manuf. Technol. 60 (2011) 469–472.
[19] X. Gu, X. Jin, J. Ni, Y. Koren, Manufacturing system design for resilience, Procedia CIRP 36 (2015) 135–140.
[20] M. Mikusz, Towards an understanding of cyber-physical systems as industrial software-product-service systems, Procedia CIRP 16 (2014) 385–389.
[21] D. Moutzis, M. Doukas, Design and planning of manufacturing networks for mass customization and personalization: challenges and outlook, Procedia CIRP 19 (2014) 1–13.
[22] B.H. Li, L. Zhang, S.L. Wang, F. Tao, J.W. Cao, X.D. Jiang, X. Song, X.D. Chai, Cloud manufacturing: a new service-oriented networked manufacturing model, Comput. Integr. Manuf. Syst. 16 (1) (2010) 1–7.
[23] X. Xu, From cloud computing to cloud manufacturing, Rob. Comput. Integr. Manuf. 28 (2012) 75–86.
[24] D. Wu, D.W. Rosen, L. Wang, D. Schaefer, Cloud-based design and manufacturing: a new paradigm in digital manufacturing and design innovation, Comput. Aided Des. 59 (2015) 1–14.
[25] L. Monostori, Cyber-physical production systems: roots, expectations and R&D challenges, Procedia CIRP 17 (2014) 9–13.
[26] R.F. Babiceanu, F.F. Chen, Development and applications of holonic manufacturing systems: a survey, J. Intell. Manuf. 17 (1) (2006) 111–131.
[27] B. Golden, Virtualization for Dummies, Wiley Publishing, Inc., Hoboken, NJ, 2008.
[28] X.V. Wang, X.W. Xu, An interoperable solution for cloud manufacturing, Rob. Comput. Integr. Manuf. 29 (2013) 232–247.
[29] D. Wu, M.J. Greer, D.W. Rosen, D. Schaefer, Cloud manufacturing: strategic vision and state-of-the-art, J. Manuf. Syst. 32 (2013) 564–579.
[30] P. Help, M. Suorsa, Y. Hao, P. Anussornnitisarn, Toward a cloud-based manufacturing execution system for distributed manufacturing, Comput. Ind. 65 (2014) 646–656.
[31] L. Wang, Machine availability monitoring and machining process planning towards cloud manufacturing, CIRP J. Manuf. Sci. Technol. 6 (2013) 263–273.
[32] O. Morariu, T. Borangiu, S. Raileanu, vMES: virtualization aware manufacturing execution system, Comput. Ind. 67 (2015) 27–37.
[33] D. Trentesaux, T. Knothe, G. Branger, K. Fischer, Planning and control of maintenance, repair and overhaul operations of a fleet of complex transportation systems: a cyber-physical system approach, in: T. Borangiu, A. Thomas, D. Trentesaux (Eds.), Service Orientation in Holonic and Multi-agent Manufacturing, 594, Springer, Berlin, Germany, 2015, pp. 165–173.
[34] C. Sun, Application of RFID technology for logistics and internet of things, AASRI Procedia 1 (2012) 106–111.
[35] Lopez Research. Building smarter Manufacturing with the Internet of Things (IoT) Part 2 of The IoT Series. Lopez Research LLC. (2014), Web Link: http://www.cisco.com/web/solutions/trends/iot/iot_in_manufacturing_january.pdf.
[36] D. Bradley, D. Russell, I. Ferguson, J. Isaacs, A. MacLeod, R. White, The internet of things: the future or the end of mechatronics, Mechatronics 27 (2015) 57–74.
[37] I. Mashal, O. Alsaryrah, T.Y. Chung, C.Z. Yang, W.H. Kuo, D.P. Agrawal, Choices for interaction with things on internet and underlying issues, Ad Hoc Netw. 28 (2015) 68–90.
[38] D. Shin, A socio-technical framework for internet-of-things design: a human-centered design for the internet of things, Telemat. Inform. 31 (2014) 519–531.
[39] T.R. Cutler, The Internet of manufacturing things, Ind. Eng. 46 (8) (2014) 37–41.
[40] D. Chatziantoniou, K. Pramatari, Y. Sotiropoulos, Supporting real-time supply chain decisions based on RFID data streams, J. Syst. Softw. 84 (2011) 700–710.
[41] L. Wang, M. Torngren, M. Onori, Current status and advancement of cyber-physical systems in manufacturing, J. Manuf. Syst. 37 (2) (2015) 517–527.
[42] E. Borgia, The internet of things vision: key features, applications and open issues, Comput. Commun. 54 (2014) 1–31.
[43] J. Gubbia, R. Buyyab, S. Marusic, M. Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (2013) 1645–1660.
[44] G.G. Meyer, K. Framling, J. Holmstrom, Intelligent products: a survey, Comput. Ind. 60 (2009) 137–148.
[45] L. Atzori, A. Iera, G. Morabito, The internet of things: a survey, Comput. Netw. 54 (2010) 2787–2805.
[46] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (2012) 1497–1516.
[47] F. Pop, N. Bessis, Energy-efficient and fault-tolerant methods for message delivery in internet of things, The 11th Roedunet International Conference (RoEduNet). 2013 (2013) 1–6.
[48] X. Qiu, H. Luo, G. Xu, R. Zhong, G.Q. Huang, Physical assets and service sharing for IoT-enabled supply hub in industrial park (SHIP), Int. J. Prod. Econ. 159 (2015) 4–15.
[49] F. Shrouf, G. Miragliotta, Energy management based on internet of things: practices and framework for adoption in production management, J. Clean. Prod. 100 (2015) 235–246.
[50] L.A. Grieco, A. Rizzo, S. Colucci, S. Sicari, G. Piro, D. Di Paola, G. Boggia, IoT-aided robotics applications: technological implications, target domains and open issues, Comput. Commun. 54 (2014) 32–47.
[51] L. Wang, An overview of function block enabled adaptive process planning for machining, J. Manuf. Syst. 35 (2015) 10–25.
[52] C.L.P. Chen, C.Y. Zhang, Data-intensive applications, challenges, techniques and technologies: a survey on Big Data, Inf. Sci. 275 (2014) 314–347.
[53] D. Loshin, Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools, Techniques, NoSQL, and Graph, Morgan Kaufmann, Waltham, MA, 2013.
[54] V. Mayer-Schonberger, K. Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think, Houghton Miffin Harcourt Publishing Company, New York, 2013.
[55] J.J. Berman, Principles of Big Data: Preparing, Sharing, and Analyzing Complex Information, Elsevier, Waltham, MA, 2013.
[56] L. Zhang, A framework to model Big Data driven complex cyber physical control systems, Proceedings of the 20th International Conference on Automation & Computing (2014) 283–288.
[57] Y. Demchenko, P. Grosso, C. de Laat, P. Membrey, Addressing Big Data issues in scientific data infrastructure, Proceedings of the Int'l. Conf. on Collaboration Technologies and Systems (2013) 48–55.
[58] Z. Zheng, J. Zhu, M.R. Lyu, Service-generated big data and big data-as-a-service: an overview, Proceedings of the IEEE Int'l Congress on Big Data (2013) 403–410.
[59] Z. Ming, C. Lou, W. Gao, R. Han, Q. Yang, L. Wang, J. Zhan, BDGS: a scalable big data generator suite in big data benchmarking, Proceedings of the Workshop Series on Big Data Benchmarking (2013) 138–154.
[60] T.H. Davenport, Big Data at Work: Dispelling the Myth, Uncovering the Opportunities, Harvard Business School Publishing Company, Boston, MA: Harvard, 2014.
[61] D. Dutta, I. Bose, Managing a big data project: the case of ramco cements limited, Int. J. Prod. Econ. 165 (2015) 293–306.
[62] C. Loebbecke, A. Picot, Reflections on societal and business model transformation arising from digitization and big data analytics: a research agenda, J. Strat. Inf. Syst. 24 (2015) 149–157.
[63] W. Xu, J. Sun, J. Ma, W. Du, A personalized information recommendation system for R&D project opportunity finding in big data contexts, J. Netw. Comput. Appl. 59 (2016) 362–369.
[64] B. Chae, Insights from hashtag #supplychain and Twitter analytics: considering Twitter and Twitter data for supply chain practice and research, Int. J. Prod. Econ. 165 (2015) 247–259.
[65] S.J. Shin, J. Woo, S. Rachuri, Predictive analytics model for power consumption in manufacturing, Procedia CIRP 15 (2014) 153–158.
[66] P. Liu, M. Yu, Damage assessment and repair in attack resilient distributed database systems, Comput. Stand. Interfaces 33 (2011) 96–107.
[67] S. Backhaus, R. Bent, J. Bono, R. Lee, B. Tracey, D. Wolpert, D. Xie, Y. Yildiz, Cyber-physical security: a game theory model of humans interacting over control systems, IEEE Trans. Smart Grid 4 (4) (2013) 2320–2327.
[68] H. Song, S. Zhu, G. Cao, Attack-resilient time synchronization for wireless sensor networks, Ad Hoc Netw. 5 (2007) 112–125.
[69] R.H. Weber, Internet of things—new security and privacy challenges, Comput. Law Secur. Rev. 26 (2010) 23–30.
[70] N. Bezzo, J. Weimer, M. Pajic, O. Sokolsky, G.J. Pappas, I. Lee, Attack resilient state estimation for autonomous robotic systems, IEEE/RSJ International Conference on intelligent Robots and Systems (IROS 2014) (2014) 3692–3698.
[71] S. Sridhar, A. Hahn, M. Govindarasu, Cyber attack-resilient control for smart grid, IEEE Innovative Smart Grid Technol. (2012) 1–3.
[72] S. Boyson, Cyber supply chain risk management: revolutionizing the strategic control of critical IT systems, Technovation 34 (2014) 342–353.
[73] L.J. Wells, J.A. Camelio, C.B. Williams, J. White, Cyber-physical security challenges in manufacturing systems, Manuf. Lett. 2 (2014) 74–77.
[74] L.P. Rees, J.K. Deane, T.R. Rakes, W.H. Baker, Decision support for cybersecurity risk planning, Decis. Support Syst. 51 (2011) 493–505.
[75] C.C. Douglas, An open framework for dynamic big-data driven application systems (DBDDAS) development, Procedia Comput. Sci. 29 (2014) 1246–1255.
[76] E. Fabiano, M. Seo, X. Wu, C.C. Douglas, Open DBDDAS toolkit: secure MapReduce and Hadoop-like systems, Procedia Comput. Sci. 51 (2015) 1675–1684.

[77] K. Krumeich, D. Werth, P. Loos, J. Schimmelpfennig, S. Jacobi, Advanced planning and control of manufacturing processes in steel industry through Big Data analytics: case study and architecture proposal, IEEE Int. Conf. Big Data (2014) 16–24.
[78] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliab. Eng. Syst. Saf. 121 (2014) 43–60.
[79] P. Erdi, Complexity Explained, Springer, Berlin, 2010.
[80] K. Barker, Y. Haines, Assessing uncertainty in extreme events: applications to risk-based decision making in interdependent infrastructure sectors, Reliab. Eng. Syst. Saf. 94 (2009) 819–829.
[81] A. Sfrent, F. Pop, Asymptotic scheduling for many task computing in Big Data platforms, Inf. Sci. 20 (2015) 71–91.
[82] V. Cristea, C. Dobre, F. Pop, Context-aware environments for the Internet of Things, in: N. Bessis, F. Xhafa, D. Varvariogou, R. Hill, M. Li (Eds.), Internet of Things and inter-cooperative computational technologies for collective intelligence, 46, Springer, Berlin, Germany, 2013, pp. 25–49.

Dr. Babiceanu is an Associate Professor of Systems Engineering with the Department of Electrical, Computer, Software, and Systems Engineering at Embry-Riddle Aeronautical University. He received his Ph.D. degree in Industrial and Systems Engineering from Virginia Tech in 2005. Dr. Babiceanu's research provides a systems engineering approach to modeling, operation, and performance improvement of large-scale complex systems, such as manufacturing, supply chain, and transportation systems. His work addresses the requirements, architecture, integration, and evaluation of systems, considering their lifecycle effectiveness and sustainability characteristics using methodologies such as systems analysis, engineering optimization, discrete-event and continuous simulation, computational intelligence techniques, and multi-agent systems. Dr. Babiceanu published more than 50 technical publications in reputed journals and conference proceedings.

Dr. Seker is a Professor of Computer Science with the Department of Electrical, Computer, Software, and Systems Engineering at Embry-Riddle Aeronautical University. He received his Ph.D. degree in Computer Engineering from the University of Alabama at Birmingham in 2002. Dr. Seker's research interests have a strong foundation in the areas of safety and security critical systems and computer forensics. His research is motivated by the trend in rapid penetration of computer-based technologies into our society. Dr. Seker published more than 60 technical publications and actively serves on ACM and IEEE Computer Society Computing Curriculum Committee. He also served as a Department of Homeland Security Software Assurance Forum Working Group member.