CHALLENGES AND OPPORTUNITIES FOR IOT-ENABLED CYBERMANUFACTURING: SOME INITIAL FINDINGS FROM AN IOT-ENABLED MANUFACTURING TECHNOLOGY TESTBED

Devarshi Shah[1], Austin Hancock[2], Anthony Skjellum[2], Jin Wang[1*] and Peter He[1*]
[1]Department of Chemical Engineering
[2]Department of Computer Science and Software Engineering
Auburn University
Auburn, AL 36849

Abstract

Internet of Things (IoT) have gained tremendous momentum and importance in recent years. Initiated from services and consumer products industries, there is a growing interest in using IoT technologies in various industries. In manufacturing, advanced or smart manufacturing and cybermanufacturing are also drawing increasing attention. Because IoT devices such as IoT sensors are usually much cheaper and smaller than the traditional sensors, there is a potential for instrumenting manufacturing systems with massive number of sensors, then big data subsequently collected from IoT sensors can be utilized to advance manufacturing. This type of IoT applications has not drawn much attention from either academic researchers or industrial practitioners. One possible reason is that the benefits of such applications have not been recognized or tested. Therefore, we built an IoT-enabled manufacturing technology testbed (MTT) to explore the potential of IoT sensors. In this work, the characteristics of a type of IoT temperature sensor were studied and mathematical models were developed to capture these characteristics and to accurately reproduce the observed behaviors. Based on the initial findings from our MTT experiments, challenges and opportunities for IoT-enabled manufacturing are discussed.

Keywords

IoT, cybermanufacturing, manufacturing technology testbed.

Introduction

The concept of the Internet of Things (IoT) is not new as it was first coined in 1999 in the MIT Auto-ID Center, which has since gained tremendous momentum and importance. Recent advances in radio, network, mobile, and cloud technologies have supported the development of the first generation IoT services and products (Tarkoma and Ailisto, 2013).

Initiated from services and consumer products industries, there is a growing interest in using IoT technologies in various industries. Many countries have invested significantly on IoT initiatives based on the premise that IoT can be an effective way to improve traditional physical and information technology infrastructure, and will have a significant impact on productivity and innovation.

Despite the fact that the industrial IoT is still in its infancy, many applications are being developed and deployed in various industries including healthcare,

* To whom all correspondence should be addressed

inventory and supply chain management, transportation, workplace and home support, security, and surveillance, etc. (Xu et al., 2014).

For healthcare services, powered by IoT's ubiquitous identification, sensing, and communication capacities, all objects in the healthcare systems (people, equipment, medicine, etc.) can be tracked and monitored constantly (Alemdar and Ersoy, 2010). In addition, all the healthcare-related information (*e.g.*, logistics, diagnosis, therapy, recovery, medication, etc.) can be collected, managed, and shared efficiently (Xu et al., 2014).

For food supply chain , IoT technologies can address the traceability, visibility, and controllability challenges in the so-called farm-to-plate manner, from precise agriculture, to food production, processing, storage, distribution, and consuming (Xu et al., 2014).

To prevent or reduce accidents in the mining industry, IoT technologies were proposed to sense mine disaster signals in order to provide early warning, disaster forecasting, and safety improvement of underground production (Wei et al., 2011).

For inventory and supply chain management, IoT devices enable transportation and logistics companies to conduct real-time monitoring of the move of physical objects from an origin to a destination across the entire supply chain including manufacturing, shipping, distribution, etc. (Karakostas, 2013).

For transportation, IoT technologies can be used to enhance a vehicle's sensing, networking, communication, and data processing capabilities; to provide driving directions and to enable autopilot that can automatically detect pedestrians or other vehicles and take evasive steering to avoid collisions (Keller et al., 2011).

In manufacturing, advanced/smart manufacturing and cybermanufacturing are drawing increasing attention as well. The essence of these trends is the application of increasingly powerful and low-cost computation and networked information-based technologies in manufacturing enterprises. There is a general consensus that factories and plants connected to the Internet are more efficient, productive and smarter than their non-connected counterparts (Davis et al., 2012; Davis et al., 2015). One potential enabler for these advanced/smart or cyber-manufacturing is industrial IoT. Industrial IoT devices for manufacturing include sensors/actuators, computers with wireless networks, and, most importantly, systems that are small and easy to embed. They have contributed significantly to different aspects of manufacturing such as automation and tracking. However, there is one area that has been largely overlooked so far – because industrial IoT devices such as sensors are usually much cheaper and smaller than the traditional sensors, there is a potential of instrumenting systems with massive number of sensors. The big data collected from these IoT sensors can then be used to advance manufacturing. Currently this type of industrial IoT application has not drawn much attention from either academic researchers or industrial practitioners. One possible reason is that the benefits of such applications have not been recognized or tested. Therefore, in this work, we built an IoT-enabled manufacturing technology testbed (MTT) to explore the potential of industrial IoT sensors. Specifically, the MTT system is a continuous stirred tank reactor (CSTR) equipped with 28 IoT temperature sensors. In section II, the design and configuration of the MTT system is detailed. In section III, various experiments were conducted to test the functionality of the IoT-enabled MTT, as well as to getter better understanding of the IoT sensor behaviors; simulation results that accurately reproduce IoT sensor behavior are also reported. Finally, in section IV based on what we learned from the MTT system, the challenges and opportunities for IoT-enabled cybermanufacturing are discussed.

IoT-enabled Manufacturing Testbed (MTT) Setup

Simulation is a powerful, flexible tool often utilized by control engineers to understand complex dynamic systems and to test out new algorithms. However, the fidelity of the simulated system is limited by the understanding on the system, (i.e., the model that describes the system). Currently, industrial IoT is still in its infancy and there is insufficient understanding on the property, capacity and performance of IoT sensors to enable accurate simulation. Therefore, in this work, instead of relying on simulation to generate the big data delivered by IoT devices, we developed an IoT-enabled manufacturing technology testbed (MTT) to understand the properties and characteristics of IoT sensors, as well as to identify the challenges and opportunities presented by IoT-enabled manufacturing systems.

Currently, available IoT devices on the market are mainly for daily use consumer products such as cell phones and home security systems, and limited options are available for industrial applications. Based on the availability of IoT devices, their functionality, cost and potential industrial applications, we decided to use temperature sensors to develop the IoT-enabled MTT system, which is a continuous stirred tank reactor (CSTR) equipped with 28 IoT sensors (water proof DS18520 IoT temperature sensors), plus corresponding data acquisition, transmission and storage systems. As discussed earlier, these IoT sensors are small and easy to embed. Therefore, they offer the opportunities to instrument systems with mass number of sensors. With 28 sensors, the IoT-enabled MTT allows us to measure the temperature distribution within the reactor directly, without assuming ideal mixing.

In the final design of the IoT-enabled CSTR system, sensors are placed in three different levels: top, middle and bottom levels in the tank; in each level, sensors are distributed uniformly across the cross-sectional area of the tank. The selected design not only allows for the capture of non-ideal mixing within the tank, but also allows easy scale up. The corresponding sensor housing unit was designed and fabricated in house. The base of the sensor

housing unit (i.e., the tank lid) was fabricated using 3D printing, and 12 rods were inserted into the base and fixed with epoxy. IoT temperature sensors were then fixed to the rods at different heights. Figure 1 shows the setup of the IoT sensors within the CSTR made of transparent polycarbonate material.

For the data management system, the final architecture follows the publish/subscribe model enabled by the MQTT protocol, a lightweight messaging transport that allows for a small code footprint while utilizing minimal bandwidth. Both of these advantages are a key concern when dealing with small, embedded devices using high-latency or unreliable networks. As shown in Figure 2, a single MQTT server acts as a central broker for devices to subscribe and publish to. Publishers send data to the server, while subscribers wait for incoming data that matches their subscription topic. Raspberry Pi was used as local computer that houses different publishers (DataCollector program), a desktop computer in a remote central location houses the broker, the subscriber (DataLogger program) and Cassandra CQL database. The Raspberry Pi sends the data collected from different sensors to the broker via the Auburn University wireless network. Figure 3 shows the actual set up of the MTT system. Currently, wireless versions of IoT temperature sensors are not available, therefore, the sensors are connected with wired LANs to the Raspberry Pi. When a wireless version becomes available, they can directly communicate with Raspberry Pi devices through the wireless network.

The Apache Cassandra database allows for high availability and scalability without compromising performance, which is ideal when dealing with the volume of data produced in an IoT sensor enabled environment.

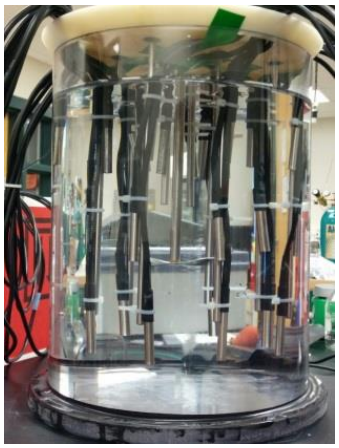


Figure 1. IoT sensors in the CSTR system

Furthermore, in the event of real time monitoring scenarios, Cassandra offers linear scalability as well as proven fault tolerance. Lastly, Cassandra offers support for replicating across multiple datacenters which allows for low latency for users which is once again ideal given the possible number of users in an IoT sensor enabled environment. With several rounds of modifications and improvements, the data management system has achieved a sampling frequency of about 0.8 seconds per sample per sensor, and the sampling speed is independent from how many sensors are plugged into the system (allowing for future scaling of the system). In addition, the most recent version of the system has optimized the functionality offered by the MQTT protocol library to drastically reduce rogue connectivity issues, significantly limiting loss of connection despite sub-optimal network conditions.

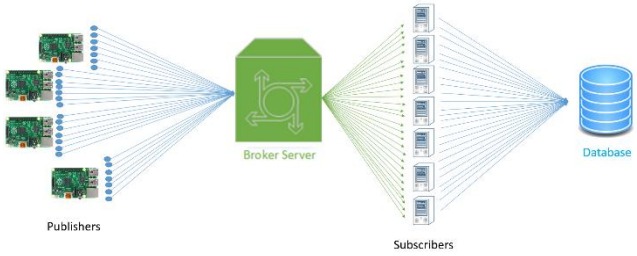


Figure 2. System architecture: publish /subscribe model enabled by MQTT protocol

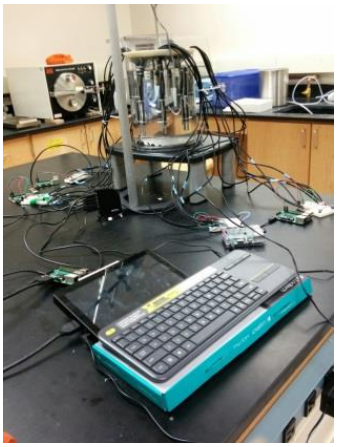


Figure 3. Actual setup of the MTT system

Designed Experiments and Findings

In order to test the functionality of the IoT-enabled MTT, as well as to gain better understanding of the behavior of the IoT sensors, steady state behavior and step response of the MTT were tested and analyzed. Additional experiments are designed and being conducted to investigate the mixing pattern and heat (mass) transfer within the CSTR.

Steady-state behavior

In order to study the behavior of IoT sensors, we first collected data over a period of time from the CSTR that is stabilized at room temperature. Figure 4 shows the data collected from two Raspberry Pi's (RPi's), and each RPi hosts seven sensors. In Figure 4, the bold red line

represents the reference temperature obtained using a mercury thermometer; while the other thin colored lines represent measurements obtained from different IoT sensors.

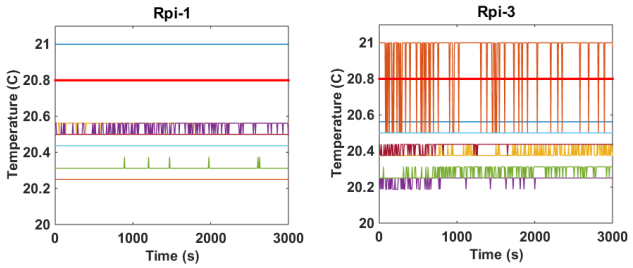


Figure 4. Steady-state behavior of IoT temperature sensors

Figure 4 shows that the IoT sensor responses are quite different from traditional mercury thermometers in the following aspects. First, many IoT sensors exhibit noisy behavior at steady state. Although some of the sensors show consistent readings, such behavior seems to be random, (*i.e.*, different sensors may show consistent readings during different test runs). Second, this noisy readings fall in fixed grids due to the bit resolution of the analog-to-digital (AD) conversion. In most of the cases, the IoT readings change in the multiples of 0.0625 ^{o}C; a couple of IoT sensors changes in the multiples of 0.5 ^{o}C, as the orange line shown in Rpi-3 in Figure 4. Third, the sensors all contain persistent bias over time.

Step response

In these experiments, the temperature in the reactor was initially at room temperature; after 5~10 minutes of sampling, the water temperature is suddenly changed to 38 ^{o}C (hot step) or 4.5 ^{o}C (cold step). Such step changes are achieved through moving the sensors and their housing unit together into a duplicated identical reactor with same amount of hot or cold water. Data collection continued even during the switch. After the switch, another 20~30 minutes of sample were collected. Figure 5 (a) and (b) show the step responses obtained through IoT sensors during hot and cold step changes, correspondingly. Figure 5 (c) shows the zoom-in of the transient response during the switch while Figure 5 (d) shows the zoom-in after the switch. The gradual decrease or increase of temperature after the step change in Figure 5 (a), (b) and (d) was due to the heat transfer between the reactor and ambient environment.

From Figure 5 we can see that: (1) the IoT sensors have slightly different time constants. The time constants estimated from their step response ranges from ~2.9 to ~5.3 second, with a mean of ~4.1 second. This behavior is similar to traditional sensors; (2) for gradual temperature changes, IoT sensors show "stiction" behavior, (*i.e.*, the temperature change, either increase or decrease, has to be over a certain threshold before the sensor readings change). The size of sensor reading increase is similar to their steady state behavior, either in the multiple of 0.0625 ^{o}C or multiple of 0.5 ^{o}C, again, due to the bit resolution of the analog-to-digital (AD) conversion.

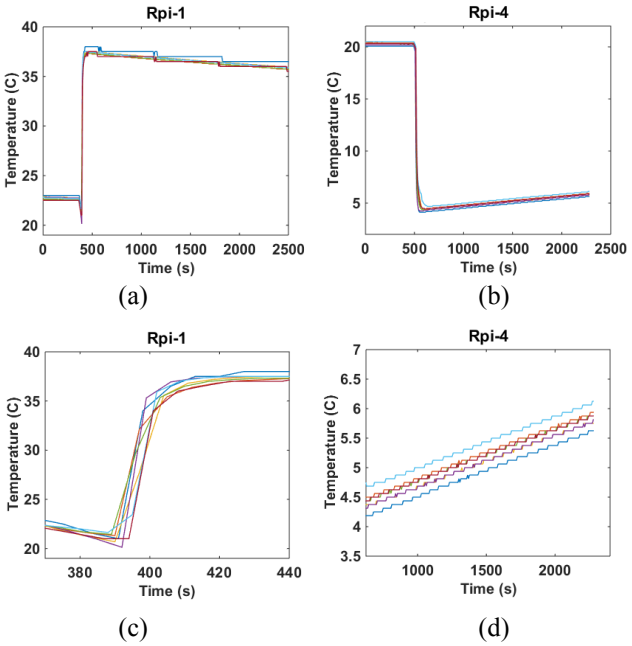


Figure 5. Step responses of the IoT sensors

Sampling interval

Besides different dynamic responses between IoT and traditional temperatures, another major differences is the sampling frequency or sampling interval. In our current configuration, the sampling frequency is mainly dictated by the IoT sensors. Whenever the IoT sensor sends a reading to Raspberry Pi, its corresponding publisher (DataCollector) will grab it and send it to the broker via the wireless network; and the corresponding subscriber (DataLogger) will receive it and store it into the Cassandra CQL database. Therefore, samples are not collected at fixed sampling intervals, instead, they are collected at various time intervals, and over the same period of time, different sensors will provide different number of readings. The sampling interval distribution for sensor #2 and sensor #8 are given in Figure 6. Over the same sampling period (5960 seconds), sensor #2 and #8 collected 7022 and 6982 samples respectively.

The main reason for such distribution is cause by the hardware (IoT sensor). The specification of the digital sensors usually provides information on how fast the sampling frequency could be. However, the software does play a significant role as well. For example, in our initial configuration, only one publisher listens to all the sensors,

which results in decreased sampling frequency when more sensors are added to the Raspberry Pi. After we switched to multi-agent setup, we were able to maintain the sampling frequency, no matter how many sensors are hosted by the same Raspberry Pi.

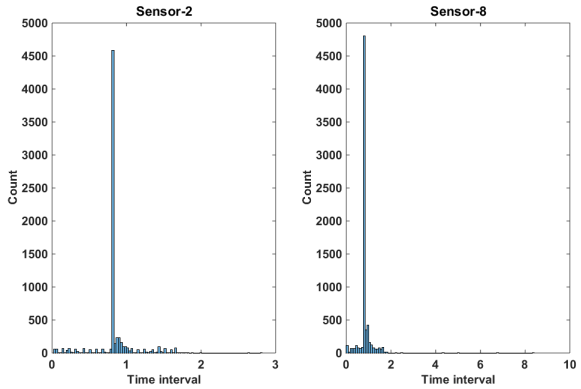
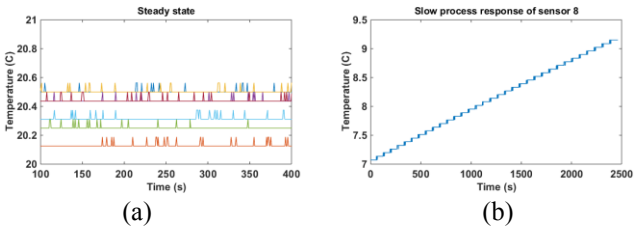


Figure 6. Sampling frequencies vary among IoT sensors. The time interval is in second.

Simulation results

One of the main goals of this work is to use the IoT-enabled MTT to study the dynamic behavior of the IoT sensors, and be able to generate simulation models to reproduce such behaviors.

Figure 7 presents some simulation results, where (a) shows the simulated steady state response of the 7 sensors on Raspberry Pi 1; (b) shows the simulated response by sensor #8 for a gradual temperature increase; (c) shows some simulated step responses, where the time constants obtained from experiments were used to predict sensor output for a given step change; (d) shows the distribution of sampling interval in one simulated case. Figure 7 shows that our simulation models can accurately reproduce the IoT sensor responses, and the sensor models can be integrated into existing simulators to generate realistic data that would be produced in IoT-enabled manufacturing processes. In this way, the data analytics algorithm development will not be limited by available IoT-sensors, and we can easily produce high fidelity big data that would be produced in cybermanufacturing and use that to test different big data analytics algorithms.



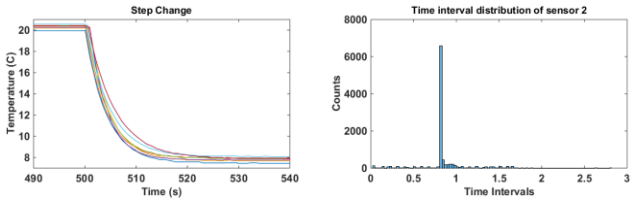


Figure 7. Behaviors of simulated IoT sensors mimic their true behaviors

Challenges and Opportunities

From the development and initial testing of the IoT-enabled MTT system, we identified the following challenges for IoT-enabled cybermanufacturing, in particular, how they translate to challenges to data analytics. Although most challenges are interrelated to each other, we categorized them into three areas: hardware, software and data analytics.

For hardware considerations, reliability is one of the biggest challenges. Reliabilities of the network (wired or wireless) connection provide the foundation of the smooth operation of a cybermanufacturing system. Reliability of the IoT devices is also a challenge, although it could be addressed partially by data analytics. Sensor accuracy presents another major challenge, as can be seen from the data we collected so far. Although each IoT temperature sensor has good precision, their accuracy is relative low. This could be a common feature of IoT sensors, because of the low cost and small size. Some well-established techniques such as filtering can help address some of the challenges. Another potential way would be to rely on big data generated by many sensors and data analytics to obtain accurate measurement of the system. The last but not least challenge in hardware is process safety. Traditional instruments usually have built-in safety considerations (such as air-to-open or air-to-close valves), but current IoT devices are lacking such process safety considerations.

For software considerations, wireless communication protocols and data management play a big role on the overall system performance, as demonstrated in this project. In addition, cybersecurity is another area that needs additional research. With all the information transmitted over the Internet, how to differentiate process operation faults from cyberattacks is one of the major challenges that need to be addressed. Potential solutions to address such challenges tie closely to data analytics.

For data analytics, four V's (4V's) are often used to characterize the essence of big data (Zikopoulos et al., 2012): Volume (the size/scale of the data), Variety (the form/format of the data), Velocity (the rate of the data being produced), and Veracity (the uncertainty/reliability of the data). Big Data analytics is arguably a major focus in the next round of smart manufacturing transformation, and could become a key basis of competitiveness,

productivity growth, and innovation (Qin, 2014). Here we discuss some challenges that data analytics face in addressing the 4 V's of Big Data.

For volume: The expected significantly and continuously increase in the number of variables is more difficult to handle than just large number of observations. Effective variable selection will help address these challenges to certain extent, but more likely drastically new approaches are needed to fundamentally address these challenges. We envision that some alternative process/data representations will emerge that utilize the complete set of variables rather than the filtered or pre-selected variables.

For Variety: Manufacturing operations generate different form of data, such as process data and product quality data, each could take different forms, monitor different parts of the system, measure different phases of the process, sample at different frequencies, etc. Existing data analytics usually deal one type of data at a time. New methods that can take a mixture of data types (such as images, texts, etc.) to build integrated models are desired.

For velocity: In the era of big data, there will be different modes of data analytics, such as streaming, batch, or mixed mode. It is expected that different modes of data analytics will be used for different purposes. In addition, we will probably see more development in different forms of incremental modeling or iterative modeling or both to address large volume of streaming data for real-time statistical analysis and online monitoring (Qin, 2014).

For veracity: In process industry, veracity means data quality or cleanness issues such as missing data, outliers, noises, delays and data asynchronism as shown in the IoT temperature measurements in this work. While traditional data analytics approaches emphasize the cleanness of the data to prevent potential misleading conclusions, it has been suggested that the next generation data analytics tools should consider data errors or messiness as unavoidable, and use massive data to develop solutions that are robust to the imperfections in the data (Qin, 2014).

Besides the 4V's associated with big data, the above mentioned challenges in the hardware and software all present challenges and opportunities to new algorithm development. It is worth noting that recently Wang and He (2010, 2011, 2016) proposed a statistics pattern analysis (SPA) based framework as a big data analytics tool for IoT-enabled manufacturing. In the SPA framework, various statistics of different variables, instead of variables themselves, are utilized to characterize process dynamics, which provides a general way to handle process nonlinearity and normality. In addition, SPA does not require data pre-processing for measurements collected at a variable frequency such as the IoT measurements in this work, therefore has advantages in address velocity. Because missing data, outliers, noises, delays and data asynchronism, as observed in this project, has no or much less impact on various statistics compared to variable themselves, SPA offers many advantages in address veracity issues as well. However, one major challenge SPA based data analytics has to address is how to select statistics patterns that effectively capture the process characteristics. This is non-trivial, particularly for complex nonlinear processes that have enormous variables measured through IoT sensors.

Future work will focus on how to make use of the data collected from IoT sensors for process monitoring and control.

Acknowledgments

Financial supports from National Science Foundation, NSF-CBET #1547124 (He), and NSF-CBET #1547163 (Wang, Skjellum, Shah and Hancock) are greatly appreciated.

References

Alemdar H, Ersoy C. 2010. Wireless sensor networks for healthcare: A survey. *Comput. Networks* **54**:2688–2710.

Davis J, Edgar T, Graybill R, Korambath P, Schott B, Swink D, Wang J, Wetzel J. 2015. Smart Manufacturing. *Annu. Rev. Chem. Biomol. Eng.* **6**:141–160.

Davis J, Edgar T, Porter J, Bernaden J, Sarli M. 2012. Smart manufacturing, manufacturing intelligence and demand-dynamic performance. *Comput. & Chem. Eng.* **47**:145–156.

He QP, Wang J. 2011. Statistics Pattern Analysis - A New Process Monitoring Framework and Its Application to Semiconductor Batch Processes. *AJ* **57**:107–121.

He QP, Wang J. 2016. Statistics pattern analysis as a Big Data analytics tool for smart manufacturing. *J. Process. Control.* **under review.**

Karakostas B. 2013. A DNS architecture for the internet of things: A case study in transport logistics. *Procedia Comput. Sci.* **19**:594–601.

Keller CG, Dang T, Fritz H, Joos A, Rabe C, Gavrila DM. 2011. Active pedestrian safety by automatic braking and evasive steering. *IEEE Trans. Intell. Transp. Syst.* **12**:1292–1304.

Qin SJ. 2014. Process data analytics in the era of big data. *AIChE J.* **60**:3092–3100.

Tarkoma S, Ailisto H. 2013. The internet of things program: the Finnish perspective. *IEEE Commun. Mag.* **51**:10–11.

Wang J, He QP. 2010. Multivariate process monitoring based on statistics pattern analysis. *IECR* **49**:7858–7869.

Wei Q, Zhu S, Du C. 2011. Study on key technologies of Internet of Things perceiving mine. *Procedia Eng.* **26**:2326–2333.

Xu L, He W, Li S. 2014. Internet of things in industries: A survey. *IEEE Trans. Ind. Informatics* **10**:2233–2243.

Zikopoulos P, Parasuraman K, Deutsch T, Giles J, Corrigan D. 2012. Harness the Power of Big Data The IBM Big Data Platform. McGraw Hill Professional.