Measuring the Effect of Wireless Sensor Network Communications on Industrial Process Performance

Richard Candell, Kang Lee

National Institute of Standards and Technology, Gaithersburg MD, U.S.A
richard.candell@nist.gov

Abstract — Real-time sensor data is essential for making decisions in controlling industrial processes. Wireless sensor networks (WSN's) are becoming more common for industrial processes and condition monitoring. However, wireless communication is subject to interference and thus may affect critical industrial operations. A wireless testbed was developed to study how various wireless sensor network configurations and topologies affect the performance and safety of manufacturing plant operations. A continuous process chemical plant operation was adopted and run in simulation. The chemical process adopted is the Tennessee Eastman Challenge Process with the Lawrence Ricker decentralized controller. The simulated process with sensor output is interfaced to an IEEE 802.15.4-based wireless sensor network via a programmable logic controller (PLC). This integration of the simulated physical system with a real wireless network allows us to examine the effects of real-time wireless communications in a factory running different wireless activities on simulated plant processes. This paper describes the testbed and presents preliminary results of the study.

Keywords — wireless sensor network, wireless control, chemical process, cybersecurity, industrial security, process control, radio environment emulation, chemical process simulation, hardware-in-the-loop, HIL, IEEE 802.15.4, WirelessHART, ISA100.11a, Industrial IoT, SCADA

I. Motivation

The Industrial Internet of Things (IIoT) has introduced a variety of economic advantages to the manufacturing industry. These advantages are based on the increased ability to sense the physical systems and correlate the data to improved efficiencies in production. The IIoT promises manufacturers the ability to monitor and control their processes in real-time with increased operational efficiency and uptime, improved visibility into factory operations, and collaboration between humans and machines thus improving productivity and work experiences [1]. These economic advantages have spurred rapid production of wireless sensing devices for use in industrial environments [2]; however, most of these devices are designed for sensing and few offerings exist for wireless actuation. A prevailing opinion of wireless networks is that the presumed reliability issues of wireless communications make wireless control a non-starter for most manufacturers. In addition, wireless is often presumed to be less secure than that of the wired alternatives. Using a measurement science approach, our wireless testbed is designed to investigate the effectiveness and security of wireless technologies when applied to sensing and control. The results of our study will be used to inform a set of guidelines that will support manufacturers in the use of wireless sensing technologies in their industrial automation systems.

II. Wireless Technology for Process Control

Over the last two decades, many wireless technologies have emerged for use in office and home environment. These technologies include the ubiquitous Wi-Fi™ which is based on the IEEE 802.11 standards. The primary objective of the 802.11 standards was wireless connectivity between home and office computers and a router that enabled users to access internet resources while maximizing throughput within a finite channel bandwidth. This approach to wireless networking has been very successful for applications that can tolerate multiple access channel contention and indeterminate packet flight time. Cases do exist where IEEE 802.11 wireless networks are used for industrial application, and those applications typically focus on a shared communication medium for sensor instrumentation, push-to-talk voice, and video surveillance. Indeed, for applications that require packet arrival determinism and reliability, the IEEE 802.11 standards may be sufficient in some case and insufficient in others [3]. IEEE 802.11 technologies have been gradually applied for various industrial plant process applications that involve real-time transfer of data and voice, position location, and video streaming. An example of this is the application of the 802.11 layer 2 wireless technology based on peer-to-peer mobile ad-hoc network (MANET) at a cement factory located in Chicago, Illinois and in another cement factory in Hagerstown, Maryland [4].

In 2003, the IEEE 802.15.4 standard emerged to address the need for reliable wireless communications that may be used in industrial applications. The standard could fill an important role in the industrial internet of things (IIoT). The IEEE 802.15.4 standard of wireless communications provides a lightweight physical and link layer protocol for low power devices. Many higher-layer protocols now exist to make IEEE 802.15.4 easier to apply to industrial applications. These protocols include ISA 100.11a (IEC 62734) [5], WirelessHART (IEC 62591) [6], and ZigBee [7]. Each of these protocols are similar in that IEEE 802.15.4 is used at the lowest layers with differences appearing in their higher-layer approaches to network architecture routing[8], security[9], and application interfaces.

III. Chemical Reactor Process Description

A chemical reactor is an example of industrial system involving many measured and manipulated variables. One such available model of a chemical reactor process is the Tennessee Eastman (TE) process model defined in [10]. The TE process model is illustrated in Figure 1. This model was chosen for a number of reasons. First, the TE model is a well-known plant model used in control systems research and the dynamics of the plant process are well-understood [11]. Second, the process must be controlled;

otherwise, perturbations will drive the system into an unstable state. By being open-loop unstable, the TE process model represents a real-world scenario in which a communications reliability event could pose an appreciable risk to human safety, environmental safety, and economic viability. Third, the process is complex, highly non-linear, and has many degrees of freedom by which to control and perturb the dynamics of the process. And finally, numerous simulations of the TE process have been developed and reusable code is readily available. We chose to use the controller developed by Lawrence Ricker of the University of Washington [12]. The Ricker Simulink model was chosen for its multi-loop control architecture making distributed control architectures viable. The physical process is described by Downs and Vogel (D&V) in detail in [10], however, a synopsis is given in the following paragraphs.

D&V did not reveal the actual substances used in the process, but instead used generic identifiers for each. The process produces two products, G and H from four reactants A, C, D, and E. The process is defined as irreversible and exothermic, and the reaction rates of the four reactants are a function of the reactor temperature. The process is broken into five major operations, which include a reactor, a product condenser, a vapor-liquid separator, a product stripper, and a recycle compressor.

Gaseous reactants are combined in the reactor to form liquid products. The reactor temperature must be controlled and is cooled using cold water cooling bundles. The reaction is not 100 % efficient and some gaseous feed components remain. The output of the reactor is fed to a condenser where the products are further cooled into liquid form. The vapor-liquid separator then separates unreacted gases from the liquid products. The unreacted gases are sent back to the reactor by a centrifugal recycle compressor. Again, the separation process is not 100 % efficient, and the remaining reactants are removed in a stripping column by stripping the mixture with C in feed stream four (4). The products, G and H, are then sent downstream for further refining. Byproducts of the process are purged from the process through the purge valve of stream nine (9).

The process has six (6) different modes of operation, which control the G/H mass ratio and the production rate through stream eleven (11). Our primary use case for the system is the base case indicated as Mode 1. D&V provided heat and material balance data for the Mode 1 case. It is important to note that the process is designed to shut down if the reactor pressure exceeds 3000 kPa; however, as noted in [2] the reaction efficiency improves as reactor pressure increases. This indicates that reactor pressure must be driven as close to the maximum threshold without exceeding the shutoff limit. The reactor pressure therefore represents a vulnerability to system integrity [11] that could be induced through a security breach or a network reliability problem. It is conceivable that the network could be compromised by radio frequency (RF) interference or a change in the RF environment (e.g. the addition of a physical structure that adversely impacts electromagnetic propagation). Krotofil and Cardenas provide an excellent discussion of how security vulnerabilities affect the physical performance of the TE process [13]. These security vulnerability impacts are analogous to wireless communications impacts on process performance. Our research here measures the impact of wireless communications on the performance of the chemical reaction process.

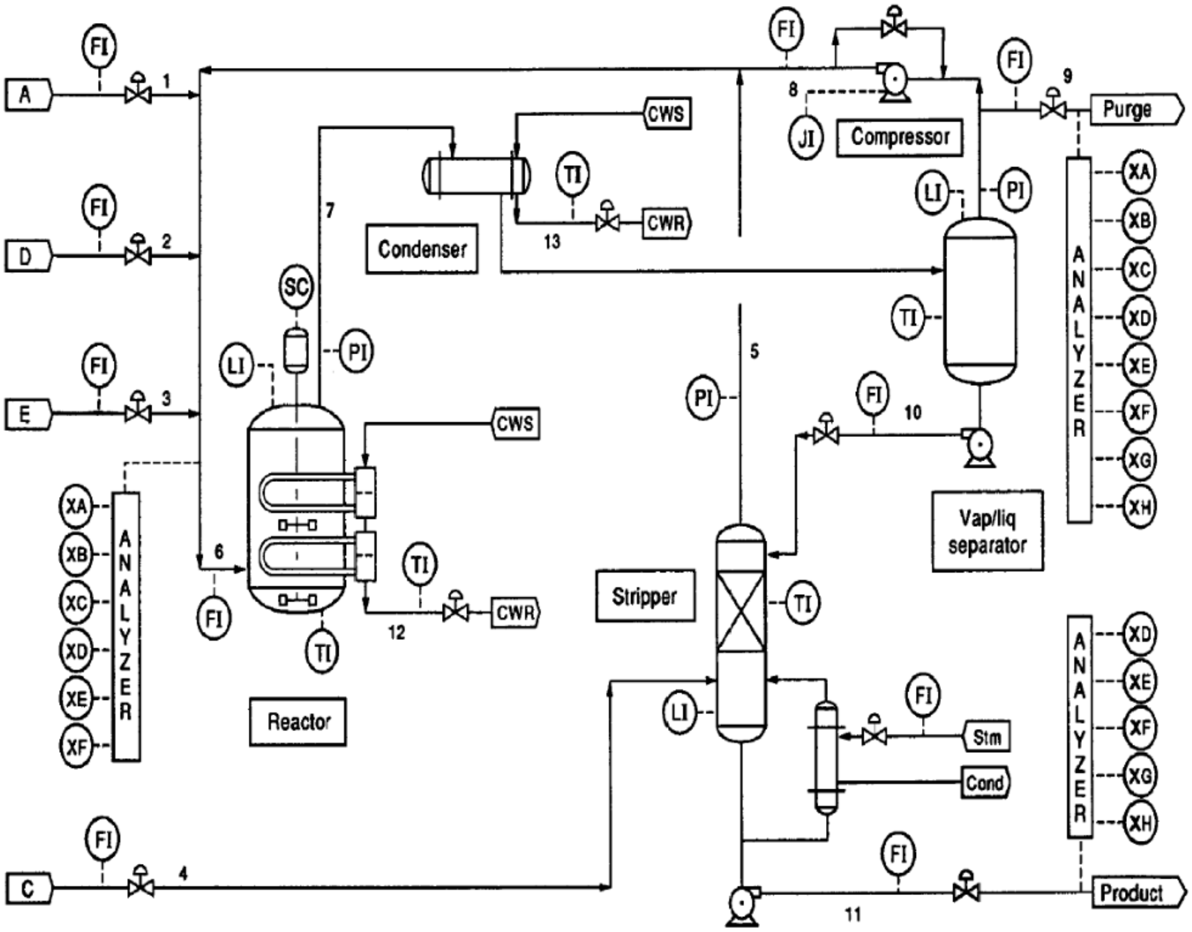

Figure 1. Tennessee Eastman Control Problem (reproduced from [10])

For an analog analysis of performance, a network connection is unnecessary, and instead a channel model may be inserted to simulate the effects of the communication links. The channel model will simulate packet error rates and delay variations of the communications links between sensors/actuators and the controller. Using this approach we will be able to predict in simulation the effect of wireless communication on the performance of the control system.

While a mathematical simulation is an important first step in the analysis of the performance of any system, it will be equally important to understand how a practical system behaves when instrumented with wireless sensing technology that will invariably insert transmission uncertainties. A hardware-in-the-loop (HIL) simulator was therefore constructed to demonstrate the impacts of wireless communication on the performance of the chemical reaction process.

IV. Testbed Implementation

The NIST Industrial Control Systems (ICS) Cybersecurity chemical process testbed presented at the 2014 ISA Process Control and Safety Symposium was adopted as the basis for the wireless testbed [11]. Indeed, the underlying chemical plant simulators are identical. They differ only in the cyber-physical interfaces that are employed for plant performance evaluation. The wireless testbed was constructed using a personal computer (PC)-based simulator, a programmable logic controller (PLC), an IEEE 802.15.4 wireless sensor network, and a Modbus/TCP server. A diagram of the testbed is shown in Figure 2.

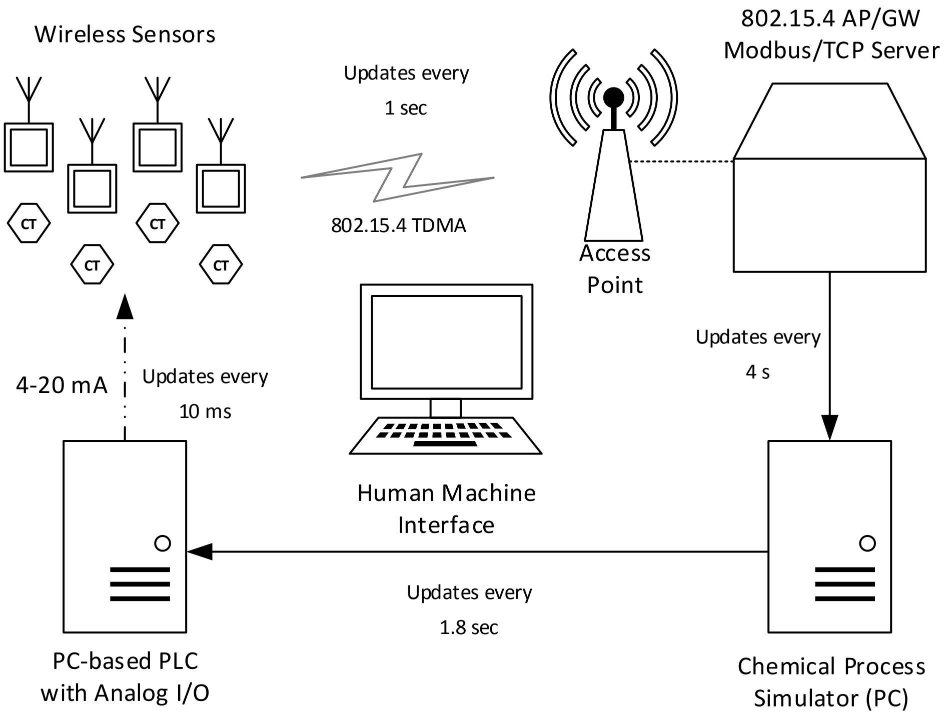

Figure 2. Chemical Process Testbed with Wireless Devices

The chemical plant process is modeled as a first-order system of differential equations as described in [10] and includes the decentralized controller described by Ricker in [12]. The plant and controller processes are herein referred to jointly as the "TE simulator." The TE simulator is incremented every 0.0005 hour (1.8 seconds). This integration time step was chosen to match the time increment chosen by Ricker for the design of his loop controllers. Modifying the time step may have unintended side effects on the stability of the plant, and therefore was left unchanged.

One of the original requirements for the implementation of the TE simulator as designed by Ricker was simulation speed. However, the TE simulator of our testbed is required to run in real-time, i.e., synchronous to the wall clock. To achieve this goal, a synchronization class (*TETimeSync*) was developed using the *boost::chrono* software module. The simulator is delayed after each increment to slow down the simulation clock enough to match the current wall clock time. If the simulator runs too slowly for real-time, *TETimeSync* detects the condition, and a warning is issued to the console.

A challenge of the testbed was to make the signals compatible with the wireless sensors on-hand. Our wireless sensors are capable of sensing various climatic conditions as well as capable of sensing a 4-20 mA current with varying uncertainty. A PC-based programmable logic controller was used to transfer the TE simulator's current sensor output to the wireless sensor network (WSN) node as shown in Figure 3. A Beckhoff Automation CX2020 PLC with 4-20 mA current output modules was used as the bridging technology. Measured variables (*xmeas*) from the plant process are communicated to the PLC using the Automation Device Specification (ADS) protocol as double precision floating point values. An IEC 61131-3 (Structured Text) program is then used to convert the doubles to signed integers, which are then loaded into the analog output modules. Each wireless node senses the current and transmits the value of the current over-the-air to the wireless gateway where values are stored in a Modbus/TCP server. A Modbus client on the CX2020 polls the Modbus/TCP server for updated current values during each PLC scan and provides the measured variable to the TE Simulator as a floating point value that the TE simulator can use to calculate manipulated values.

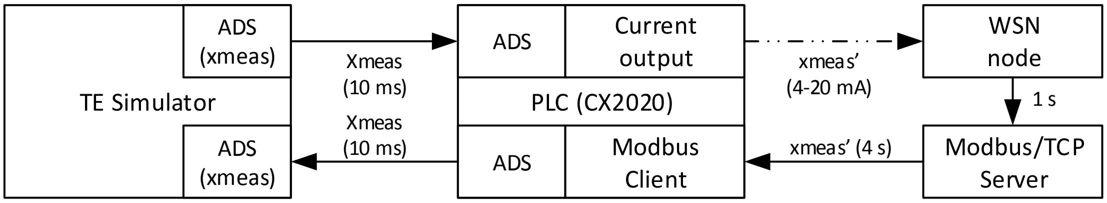

Figure 3. Data Flow of Measured Variables

a) Challenges

Some impact to the performance of the plant process as a result of the wireless network can be attributed to the increase in uncertainty due to sensor calibration errors, network delays, and sensor noises, and the loss of precision of the measured variables resulting from the format conversions. To isolate the effects of these factors from the wireless network, special care was taken to characterize and then minimize those factors.

Sensor Calibration

The first factor affecting plant performance was calibration error of the current sensor within each wireless node. Sensor testing showed an average of 1.4 mA offset for each sensor across all current input levels as show in Figure 4. In addition, the calibration offset drifted with time by +/- 0.1 mA. For the purpose of measurements, the average offset was corrected after the reading was pulled from the Modbus/TCP server.

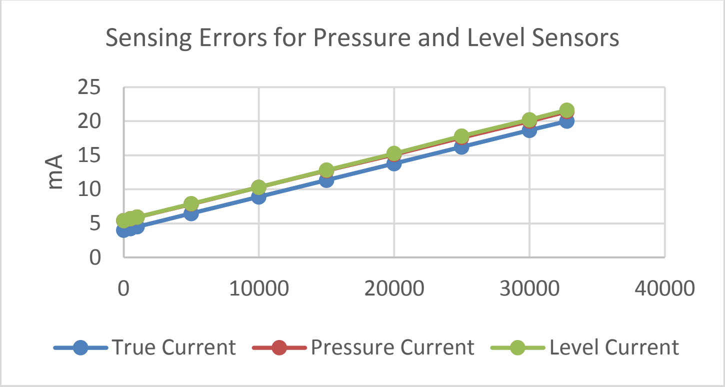

Figure 4. Current Sensing Errors

Real-time Time Correlation

Another challenge to integrating a PC-based simulation of the TE chemical process with wireless sensors was maintaining real-time correlation between the observable states of the simulated chemical process variables with the representative current outputs from the PLC. This problem was solved by configuring the PLC scan time to 10 ms, which is sufficiently faster than the integration time step of 1.8 s within the PLC. The PLC adjusts the current within 10 ms, which is much faster than the signal update rate from the TE simulator.

Configurability of the Wireless Sensor Network Components

Typical wireless sensor networks provide sufficient configurability by providing the operator with a fine-tuning capability of the acquisition rates, wireless sensor transmission rates, and automation server storage update rates. Our wireless sensor network did not provide a high degree of configurability in all cases. One area of concern in our system was the Modbus/TCP server update rate. Our system allowed for the transmission of sensor values from the various nodes every second; however, the gateway updates the Modbus database only every 4 seconds, thus dropping the intermediate readings. This is conformant with the required burst rate for WirelessHART sensor devices, and this is compatible with the requirements of the TE simulator.

Assuming an ideal RF communication channel, the Primary remain disturbance due to the network can be calculated based on known delay constants. The worst case per reading delay from signal acquisition to actuation was determined to be 5.02 s.

V. Test Scenarios

As indicated by Ricker, most control theory analyses focus on metrics of loop controllers with little attention given to areas of control that plant operators consider. In an attempt to address both technical factors and operational factors, scenarios were carefully chosen to match the set-points and disturbances addressed by Ricker in [12]. These process control scenarios are listed in Table 1. For each experimental scenario, a baseline scenario was run without the wireless sensor network to represent the ideal case, such as lossless, noise-free, latency-free conductors similar to that of classical copper wire control loops. Therefore, each scenario produced a baseline data set and an experiment data set.

Table 1. Experimental Scenarios for Wireless Sensing and Control Analysis

Scenario	Description
Reactor Level	The level set-point of the reactor is modified to 80.1% from 65 %
Reactor Pressure	Reactor pressure set-point adjusted downward to 2700 kPa from 2800 kPa.
Production Rate	Production rate set-point is modified to 25 from 22.89
Quality Factor	% mol. G set-point is modified to 35 % from 53.8 %
Stuck Reactor Cooling Valve	The valve controlling cool water flow to the reactor does not respond to commands.

VI. Results

The chemical process wireless testbed was exercised with the scenarios listed in Table 1. For each scenario, the measured variables as reported by the TE simulator were collected every 20 integration time steps of the simulator. Values were stored in a tabbed delimited file for offline processing. Metrics were then collected for each scenario to include statistical quantities, such as mean, median, quantiles, and outliers of each measured variable as well as the difference of the measured variable to its baseline. Deviations were measured as the percentage difference of the experimental case to the baseline case for each signal. In addition, plots of the time series for baseline and experimental cases were qualitatively compared attempting to explain the differences in statistical results.

Example statistical measures are listed in Table 2 and a graphical representation of the distribution of deviations from baseline is provided in Figure 5. This particular scenario shows the experimental deviation when the reactor pressure set-point was lowered from 2800 kPa to 2700 kPa. The figure shows that when changing the set-point using a wireless network versus a faster, and presumably more reliable, wired network, most measured variables tracked the baseline case closely. While the costs for operating the plant showed significant deviations with periods of higher costs of more than 100 %, closer examination of the time series (Figure 6) showed that deviations were due to a lag in the time series response.

By referring to Figure 6, we may also be able to explain this discrepancy by the longer settle times and larger overshoots of the key process variables for a small period of time between 3 and 4 hours. We have observed large deviations in inventories (i.e., tank levels) during this time, which could lead to larger hourly costs. Eventually, the experimental case settles to track the baseline case, and it is conceivable that optimization algorithms could be used to minimize these deviations. Calculation of the cost function is defined in “MultiLoop_mode1.mdl” in the *Tennessee Eastman Challenge Archive* [14].

Table 2. Statistical Summary of the % Difference from Baseline for the Reactor Pressure Change Scenario

Variable	*Min*	*Max*	*Mean*	*Std. Dev.*
Reactor.Pressure.kPa	-1.3	1.30	-0.02637	0.27
Reactor.Level.Pct	-5.5	22.90	-0.05048	1.76
Reactor.Temp.C	-0.3	0.05	0.00009	0.01
Sep.Level.Pct	-16.6	31.34	-0.06063	7.24
Stripper.Level.Pct	-20.9	78.42	2.13762	21.19
Sep.Underflow.m3.hr	-3.7	6.31	-0.36017	1.56
React.Cool.Temp.C	-0.1	1.12	0.00142	0.15
Product.G.mole.Pct	-1.1	0.53	0.00329	0.26
Hourly.Cost	-38.5	134.78	3.79610	20.08

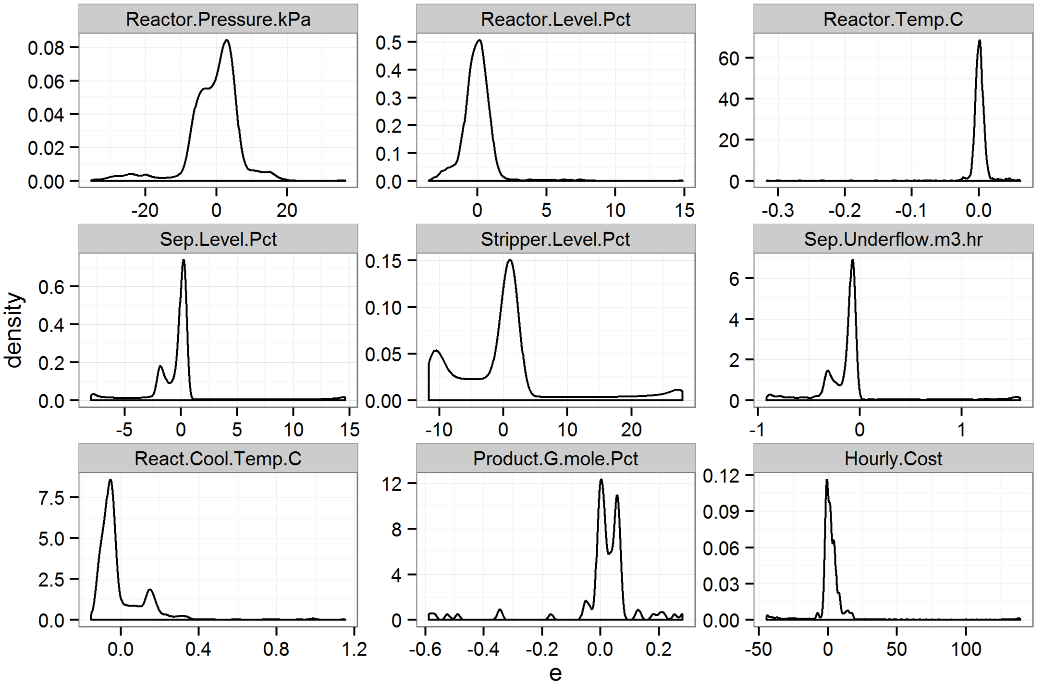

Figure 5. Probability Distribution of Percent Deviation (e) for a Change in Reactor Pressure to 2700 kPa. The horizontal axis is the percent error, and the vertical axis is the probability of deviation.

Another scenario considered was disturbance rejection for which a stuck valve condition was created. In this scenario, the valve controlling the flow of cold water to the reactor was rendered “stuck” in the closed position. The figure shows that when the cooling valve malfunctions, the wireless network impacts the performance of all process variables especially stripper inventories. In this case, an update rate limitation of the Modbus/TCP server within the wireless gateway could be considered a root cause for deviations reported by the plant simulator; however, this would be a legitimate concern for network control integrators and indicates the need for careful study of all system components prior to a wireless network deployment.

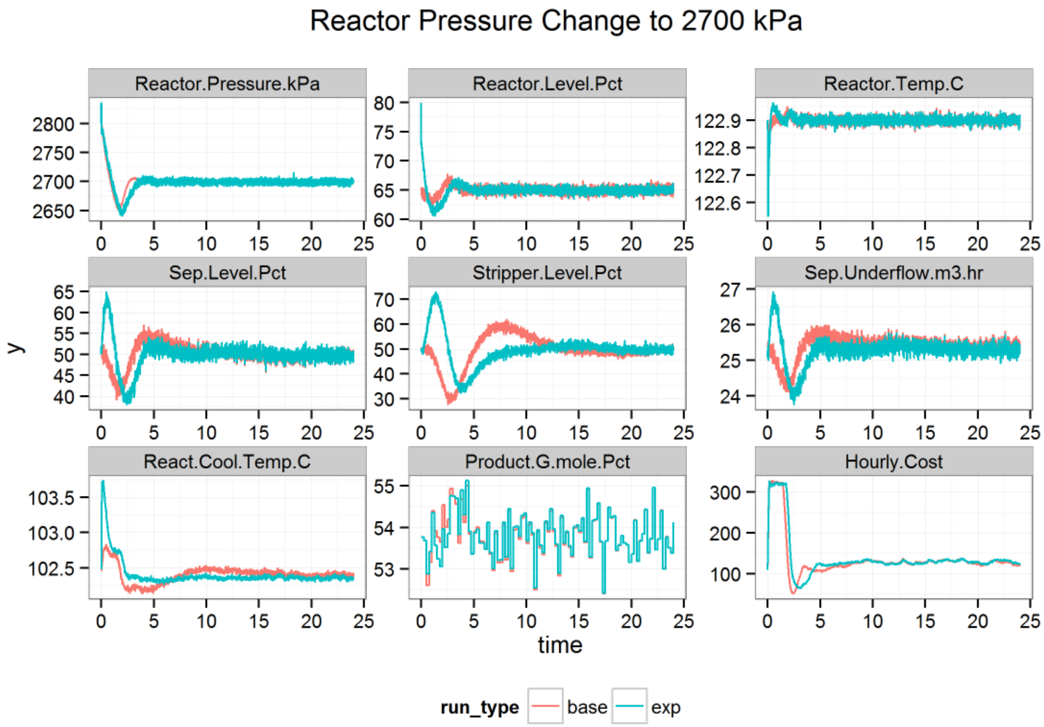

Figure 6. Time Series Evaluation for Change in Reactor Pressure.
Legend: *base*=wired/ideal, and *exp*=wireless

Table 3. Summary of % Difference from Baseline for Stuck Valve Scenario

Variable	*Min*	*Max*	*Mean*	*Std. Dev.*
Reactor.Pressure.kPa	-0.7	1.0	-0.00399	0.2
Reactor.Level.Pct	-5.2	13.1	-0.05651	1.6
Reactor.Temp.C	-0.5	0.5	0.00003	0.2
Sep.Level.Pct	-11.1	28.8	-0.23135	6.6
Stripper.Level.Pct	-33.9	55.5	0.46037	19.9
Sep.Underflow.m3.hr	-2.7	6.0	-0.45053	1.5
React.Cool.Temp.C	-1.2	1.5	0.01762	0.5
Product.G.mole.Pct	-1.1	0.5	-0.01470	0.3
Hourly.Cost	-37.1	22.9	-1.56317	10.4

VII. Future Work

The work presented here provides a workable prototype for the development of well-thought scenarios for studying wireless networks used by the process control industry. As a prototype, areas of improvement are necessary for the development of more accurate test scenarios that reflect the real world process control environments. Future iterations of the testbed will include the following elements:

- RF channel emulation. A channel emulator provides a means to recreate the RF environment in a laboratory setting. Conditions, such as interference, propagation effects, and jamming can be applied to RF signals and the effects on the physical process may be studied.
- Calibration: While steps were taken to overcome calibration error uncertainty, better current sensing circuits should be added to minimize the possibility that sensing error contributes to deviations from baseline more than the network.
- Actuators: The current implementation of the testbed does not allow for closed-loop control over wireless. An objective of the testbed is to evaluate the impacts of closed-loop control over wireless networks; therefore, wireless actuators will be added to the testbed as they are made available.
- Timestamps: Timestamp allows for improved signal processing, such as interpolation and extrapolation. Timestamping is not available with the current Modbus/TCP interface to the controller. Using another industrial interface would allow for more advanced signal processing, such as predictive filtering and model-based control.

VIII. Conclusions

A testbed for the study of chemical process control was constructed for the purpose of studying the effects of wireless network performance on the control of physical processes. The Tennessee Eastman chemical reactor process was chosen as a genuine example of a real-world manufacturing process using a model that has been widely accepted by researchers and practicing engineers. The testbed implements a hardware-in-the-loop architecture by incorporating a simulation of the plant process and decentralized controller with an IEEE 802.15.4 TDMA-based wireless sensor network for measured variables and a wired factory automation network for manipulated variables. In addition, the testbed provides the ability to recreate the RF environment unique to any factory and measure the performance impacts of the RF environment on both the wireless network as well as the performance of the physical process. Time series data of measured process variables and performance metrics of the physical process were collected to demonstrate the impact of a wireless sensing network on factory performance. Preliminary results were collected without the RF emulation capability in place. These results demonstrate the capability of the testbed to generate and collect plant-centric sensor data for process control and performance evaluation. Future data will include RF channel emulation of the plant environments.

Acknowledgments

We would like to thank Rushad Antia and Luke Roepe for their contributions in software development in support of the experimentation.

SOURCE CODE

All software code for the TE simulator may be found at the *tesim* GitHub repository by visiting http://www.github.com/usnistgov/tesim. Researchers are encouraged to reuse the software for their own investigations.

DISCLAIMER

Certain commercial equipment, instruments, or materials are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

REFERENCES

[1] World Economic Forum, "Industrial Internet of Things : Unleashing the Potential of Connected Products and Services," Cologny/Geneva , Switzerland, 2015.

[2] "Industrial WSN Report 2014," ON World, San Diego, CA, 2014.

[3] T. Moore, "Research: Wireless use in industry," *Control Engineering Magazine*, 2013. [Online]. Available: http://www.controleng.com/single-article/research-wireless-use-in-industry/5b97f5d429813c649a05240ad5efd280.html.

[4] W. J. Miller, "Wireless Takes Control," *International Cement Review*, p. 88, 2008.

[5] P. Radmand, A. Talevski, S. Petersen, and S. Carlsen, "Comparison of Industrial WSN Standards," pp. 632–637, 2010.

[6] D. Chen, M. Nixon, and A. Mok, *WirelessHART^{TM}*. Boston, MA: Springer US, 2010.

[7] "ZigBee Wiki Article." [Online]. Available: https://en.wikipedia.org/wiki/ZigBee.

[8] G. Wang, "Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100 . 11a and Wireless HART Master of Science Thesis , Communication Engineering," Gothenburg, Sweden, 2011.

[9] C. Alcaraz and J. Lopez, "A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems," *IEEE Trans. Syst. Man, Cybern. Part C (Applications Rev.*, vol. 40, no. 4, pp. 419–428, 2010.

[10] J. J. Downs and E. F. Vogel, “A Plant-wide Industrial Problem Process,” *Comput. Chem. Eng.*, vol. 17, no. 3, pp. 245–255, 1993.

[11] R. Candell, K. Stouffer, and D. Anand, “A Cybersecurity Testbed for Industrial Control Systems,” in *Proceedings of the 2014 Process Control and Safety Symposium*, 2014.

[12] L. Ricker, “Decentralized control of the Tennessee Eastman Challenge Process,” *J. Process Control*, vol. 6, no. 4, pp. 205–221, Aug. 1996.

[13] M. M. Krotofil and D. Gollmann, “Industrial control systems security: What is happening?,” in *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, 2013, pp. 670–675.

[14] L. Ricker, “Tennessee Eastman Challenge Archive.” [Online]. Available: http://depts.washington.edu/control/LARRY/TE/download.html.