Challenges of Wireless Control in Process Industry

Jianping Song[*], Aloysius K. Mok[*], Deji Chen[!], and Mark Nixon[!]

[*]*Department of Computer Sciences*
The University of Texas at Austin
Austin, TX 78712, USA

[!]*Emerson Process Management*
12301 Research Blvd. Bldg. III
Austin, TX 78759, USA

Abstract

There has been tremendous interest in the research and development of wireless technology. In general wireless for the control industry is not a new topic, either. Many industry organizations; such as, WINA, ZigBee, and ISA have been pushing wireless technology for years. There is a set of well-known and agreed upon challenges that we have to overcome to apply wireless to industry control; such as, security, robustness, delay, and power. After touching on those concerns briefly, we will analyze the challenges in applying control over process sensor networks. While using sensor network for process monitoring has been studied extensively and we already see products on the market, doing control over a sensor network is still considered impractical. While people agree this will eventually happen, a continued long term effort from both academia and industry is required. This paper lists several areas to collaborate on.

1. Process control networks and their wireless counterparts

There are three levels of networks in a typical process control system as shown in Figure 1. Figure 2 depicts its projected wireless counterpart. At the bottom of Figure 1 are control networks that physically manage the plant process. The controllers are connected with the devices, including both sensors and actuators, via the control networks. The controller reads data from the sensors and writes data to the actuators. The network protocols are usually industry standards that provide real-time support and have high predictability and reliability. The range is short and the data size is small. The wireless network at this level is usually called sensor network. We shall address its challenges in Section 2.

We call the middle-level network an area asset control network. It connects controllers that control devices in the field and workstations that interface with the user. Area asset control networks carry user interaction data for configuration, control command, monitoring, and diagnostics. It has less timing requirements, but still needs good reliability. The range is longer and the data size is bigger then for the sensor network. Area asset control networks can be proprietary protocol that utilizes industry communication standards or use industry standards such as Ethernet. Since it is not immediately connected to the field devices, we might use commercial wireless networks as its replacement. Challenges for wireless network at this level are mostly the same as those for commercial networks.

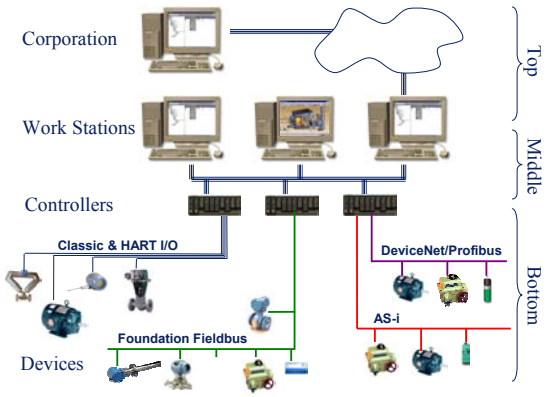

Figure 1: A Process Control System

At the top level is the corporate office network that the control network happens to be connected to. It is the gateway to other corporate systems like accounting, inventory, management decision systems, etc. Its wireless counterpart is the commercial wireless network. There are no special wireless challenges with regard to process control at this level. Of course, connecting control networks to office networks poses security concerns.

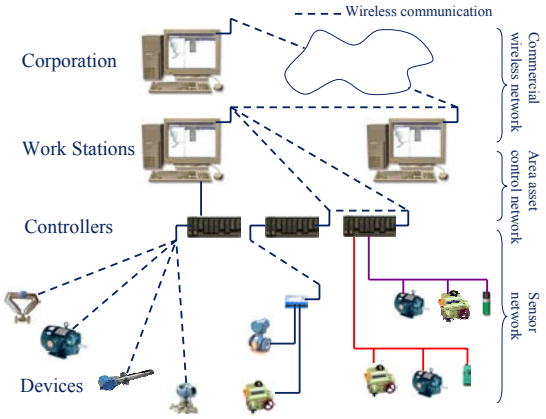

Figure 2: A Wireless Process Control System

Challenges for wireless applications are well documented; challenges for wireless applications for process control are also studied extensively. Major industrial organizations that push for wireless adoption have been established for quite a while, such as WINA [12], ZigBee [13], ISA Wireless Systems for Automation [10], wireless HART [8], etc. Some of the issues related to wireless become more important for process control, such as security, robustness, and power.

Security becomes more and more important for social reasons. Connecting the control system to the Web aggravates the concern. According to [5], "Control systems are susceptible to attack because they weren't designed to meet cyber threats"; and, "More than 60 identified (though not publicly documented) real-world cases have occurred where electronic means have impacted the control systems' reliable operations." Wireless security was one of the biggest topics during the ISA 2005 Expo. ISA's SP99 Committee has defined a common set of information security requirements for control systems that users and vendors alike can reference.

Robustness, including reliability and safety, is a concern because the interference in the process field and the consequence of a failure are much worse. Robustness in many environments that are common in a plant may requires a powerful antenna, but higher transmission power poses danger in inflammable space in addition to longer interference ranges. Battery replacement is also more difficult in a plant environment.

2. Process control with sensor networks

Sensor network studies concentrate on system monitoring. The majority of wireless systems in the field play an auxiliary role to the existing control system. They collect additional data that the control system does not provide. The term "sensor network" unintentionally limited its scope to sensing only. To perform control we need actuators; we need networks of sensors and actuators. Using sensor network to control process poses technical challenges, yet people believe it will eventually happen. The benefit of replacing wire in a process plant is huge and people will always want to apply control over wireless. It shouldn't be hard for future wireless technology to simulate the same level of functionality as current fieldbuses. We believe advances will come sooner if both the industry and academia spend more effort tackling wireless control.

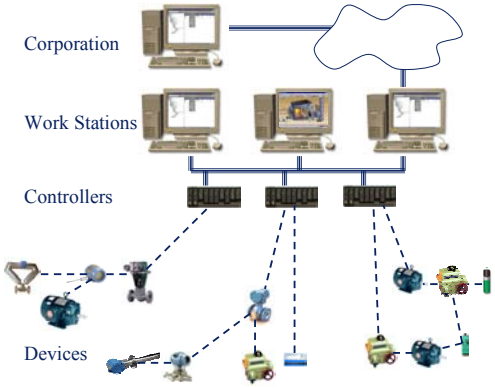

Figure 3: Sensor Networks in Process Control System (Large System)

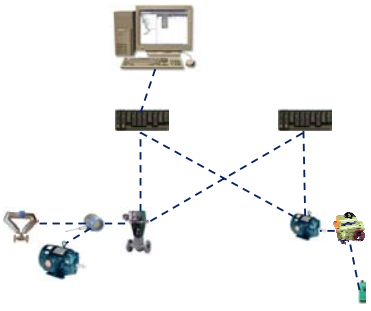

Figure 4: Sensor Networks in Process Control System (Small System)

Figure 3 illustrates a possible sensor network in a large control system; figure 4 illustrates a possible small control system. Let's look at the fieldbuses they replace. To achieve process control, the fieldbus network communication and associated control function and scheduling are designed to be fully deterministic. There is no traffic interference or variation in control organization. Other than a security concern, many technical issues must be resolved for wireless control.

- **Temporary interference**: Sensor networks use the open air as communication medium. Whatever happens in open air can cause interference to the data transmission. Events such as the weather, people and things moving around, and other wireless signals can interfere with transmissions. Temporary interference impacts timely data transmission which directly challenges the objective of real-time process control.
- **Permanent interference**: Once a fieldbus is deployed, it will function throughout the lifetime of the control system. A deployed wireless control network however, must be re-configured through its life cycle. The communication between two nodes may change permanently due to addition or removal of field devices that are not related to the wireless network.
- **Power usage**: Power issues related directly to real-time control include the contingency handling of power outage, data transmission delay variance due to battery levels, etc.

Beyond duplicating what fieldbus could do, sensor networks open up new possibilities and hence new challenges for real time control. One of the next steps is to connect the sensor network directly to the user workstation instead of the dedicated controller. As shown in Figure 4, for small systems there will be no controllers and the devices talk directly to the workstations which also run user applications. In the future, every operating system should have some flavor of a real-time operating system. As shown in Figure 3, for large system, the controllers still are required for control coordination and data processing and servicing, e.g., alarm management and history data collection.

Fieldbus and sensor network differ in many ways. While sensor network is inherently less robust, it compensates with multipath capability. Also low cost and higher communication speed than are available with fieldbus networks mean more devices could be deployed and more process data could be monitored and controlled. To simply mimic fieldbus, sensor network must synchronize all the nodes so that data could be time-stamped with the global clock, a central node must coordinate all the data traffic. This increases the complexity of a sensor, which goes against the other goals of sensor network: to reduce cost, reduce energy consumption, and have plenty of small sensors/actuators.

A better question could be asked: how could sensor network achieve the same level or even better process control compared with fieldbus? Is there an approach different from that of the fieldbus? To answer this question, we should understand what the goal of process control is.

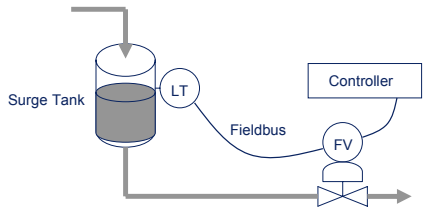

Figure 5: Tank Level Control with Fieldbus

Figure 5 is an example of a plant process and a fieldbus solution. The input pipe fills the tank at a rate based on the upstream process operation. The goal is to keep the tank fluid within a level range by controlling the output flow. The controller receives tank level value via the fieldbus from the level transmitter and sends valve position value via the fieldbus to the valve. In many process plants, significant loss will occur if the tank level exceeds upper or lower range limits.

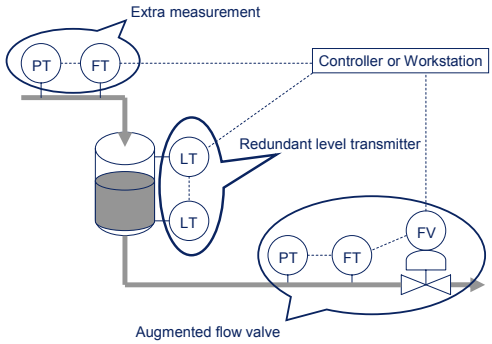

Figure 6: Tank Level Control with Sensor Network

Figure 6 applies sensor network to achieve the same goal. The challenge is if we could beat the performance of the system in Figure 5 by using more sensors in field devices and make use of other current and future technologies of sensor network. Additional or redundant measurements can be built into the next generation of field devices, e.g., flow and upstream pressure measurement as part of the control valve. Maybe a new control paradigm could emerge.

3. Conclusion

People are pushing hard to adopt wireless for process control. At present wireless applications in process control are mainly for monitoring purposes. Issues and challenges are also well-known and agreed upon in this area. However, the long term challenge lies in control with sensor network. We think there is significant benefit in the industry and academia working together to address these problems.

4. References

[1] Deji Chen, Mark Nixon, Tom Aneweer, Rusty Shepard, and Aloysius K. Mok, Middleware for Wireless Process Control Systems, Architectures for Cooperative Embedded Real-Time Systems Workshop, December 2004

[2] Deji Chen, Mark Nixon, Tom Aneweer, Rusty Shepard, Kent Burr, and Aloysius K. Mok, Wireless Process Control Products from ISA 2004, International Workshop on Wireless and Industrial Automation, March 2005.

[3] Dick Caro, "Wireless Networks for Industrial Automation", ISA - The Instrumentation, Systems, and Automation Society, 2004.

[4] D. Culler, D. Estrin, and M. Srivastava, Overview of Sensor Networks, Computer, August 2004

[5] Joseph M. Weiss, Cyber Security Meets Plant Politics, InTech Magazine, July 2005.

[6] Bluetooth Standard, https://www.bluetooth.org/.

[7] Foundation Fieldbus standard, http://www.fieldbus.org/.

[8] HART standard, http://www.hartcomm.org/.

[9] IEEE wireless standards, http://standards.ieee.org/wireless/.

[10] The Instrumentation, Systems and Automation Society, http://www.isa.org/.

[11] Profibus standard, http://www.profibus.org/.

[12] Wireless Industrial Networking Alliance, http://www.wina.org/.

[13] ZigBee Alliance, http://www.zigbee.org/.