Security on the Farm: Safely Communicating with Legacy Agricultural Instrumentation

Tim Bell
Roger D. Chamberlain
Mike Chambers
Brian Rieck
Todd Steinbrueck

Tim Bell, Roger D. Chamberlain, Mike Chambers, Brian Rieck, and Todd Steinbrueck, "Security on the Farm: Safely Communicating with Legacy Agricultural Instrumentation," in *Proc. of 15th International Conference on Distributed Computing in Sensor Systems* (DCOSS), May 2019, pp. 192-194. DOI: 10.1109/DCOSS.2019.00052

BECS Technology, Inc.
St. Louis, Missouri

Dept. of Computer Science and Engineering
Washington University in St. Louis

AGCO Corporation
Assumption, Illinois

2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)

Security on the Farm: Safely Communicating with Legacy Agricultural Instrumentation

Tim Bell*, Roger D. Chamberlain*†, Mike Chambers*, Brian Rieck‡, Todd Steinbrueck*

*BECS Technology, Inc.
St. Louis, MO, USA
{tim,roger,mike_c,todd}@becs.com

†Dept. of Computer Science and Engineering
Washington University in St. Louis
St. Louis, MO, USA

‡AGCO Corporation
Assumption, IL, USA
{brian.rieck}@agcocorp.com

***Abstract*—The notion of IoT has taken the farm by storm. Irrigation is controlled to the resolution of individual plants, fertilizer is dispensed based on yields from previous growing cycles, and livestock feed, water, and environment are all monitored and under automatic control. Much of the equipment that performs this monitoring and control, however, predates the Internet of Things, and integrating this legacy equipment into modern communication systems is fraught with issues, particularly security issues. We describe our approach to providing secure, ubiquitous connectivity to a variety of previously isolated systems on the farm, enabling these systems to safely become part of the IoT.**

***Index Terms*—IoT, agriculture**

I. Introduction

The Internet of Things (IoT) is ushering in an era where significant numbers of devices that perform monitoring and control functions (e.g., process control, manufacturing, etc.) are connected via wired or wireless networks. Modern agriculture is a leader in experiencing this transformation, with ubiquitous data collection associated with planting, fertilizing, and harvesting of crops as well as with feeding, environmental control, and monitoring of livestock. AGCO Corporation is a multi-billion dollar company that designs, manufactures, and distributes systems in the agriculture market worldwide. BECS Technology, Inc., (BECS) is a small business that manufactures monitoring and control equipment for a number of markets (agriculture, aquatics, refrigeration, etc.) and partners with AGCO® in the poultry and swine markets.

Not all equipment, however, was designed with the IoT in mind. Many legacy monitoring and control systems were installed well before universal connectivity was common, and while that equipment often includes mechanisms for remote access, these mechanisms are woefully inadequate to the modern need for robust secure communication.

The benefits that can accrue from remote connectivity and access to these data are substantial. For instance, this can lead to better feed conversion and diminished usage of feed, water, and electricity. We can use machine learning techniques to improve yields as well as catch health-related issues earlier. Maintenance costs can also be reduced, by effectively predicting maintenance needs rather than simply reacting to emergent systems failures. While these opportunities can and do provide real benefit to farmers, there are challenges related to security, privacy, and data communication that must be overcome. Both Kumar and Patel [5] and Vasilomanolakis et al. [7] describe these challenges as being pervasive across all the IoT.

EZConnect™ is the security infrastructure BECS has developed to provide remote access capability to equipment it manufactures in the aquatics market. This remote access capability satisfies the need for security yet balances that need with the equivalent need for ease of installation and maintenance [1].

Here, we describe the Feed-Link™ system, an AGCO product that is manufactured under private label by BECS, which enables a number of legacy agricultural monitoring and control systems to effectively, securely join the Internet of Things. We will articulate the specific security mechanisms put in place, and how this simultaneously enables security and ease-of-use.

II. Agricultural IoT Data

The equipment of interest are fairly typical devices in the Internet of Things (IoT). The devices monitor various aspects of animal husbandry: barn temperature, feed stocks, feed consumption, water consumption, ventilation control, etc., manufactured by AGCO, BECS, and others. Based on this information, the various controllers take actions (starting/stopping feed delivery augers, starting/stopping ventilation fans, etc.) to maintain the barn environment at the proper levels and ensure the animals are properly fed. Alarm conditions trigger notifications to service personnel. Sensor values and

2325-2944/19/$31.00 ©2019 IEEE
DOI 10.1109/DCOSS.2019.00052

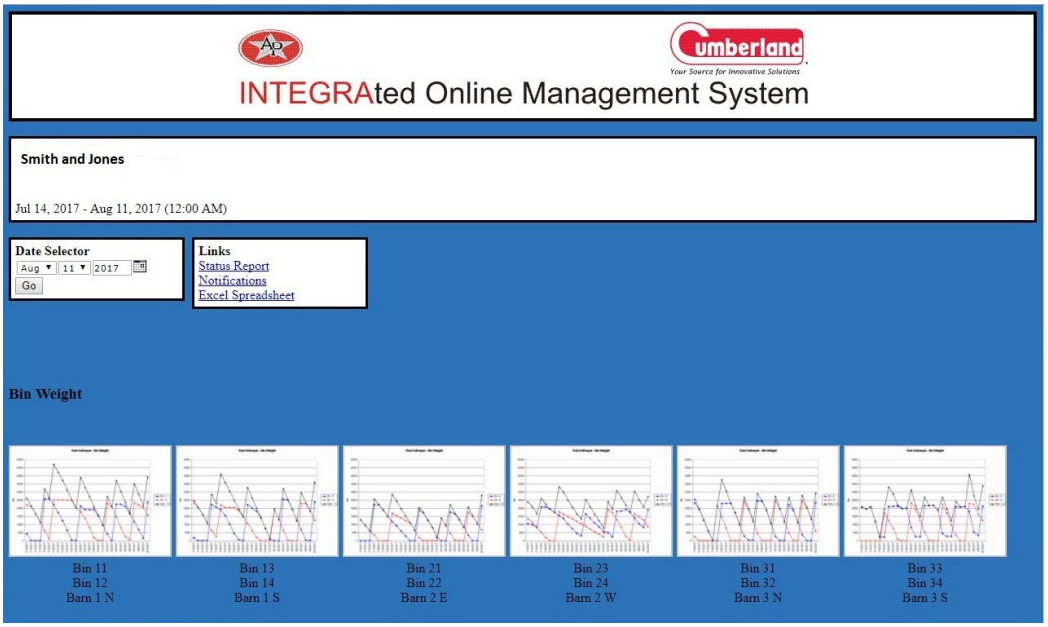


Fig. 1. Dashboard display of Feed-Link system.

actions are logged, and these logs are frequently used when diagnosing the causes of alarms or other anomalous events. Remote access to all of the above information is clearly to the benefit of the animal owners/farmers.

While the notion of IoT might be new, the fundamental capability to access controller information remotely is not. BECS Technology's controllers have supported remote communications for more than 2 decades. Early controllers used modems attached to the telephone network (an option still available for those that need it), today controllers support TCP/IP connectivity via the Internet.

Remote capabilities include viewing of current status, downloading of data logs, and configuration of the equipment. Figure 1 shows a screenshot of the Feed-Link dashboard for a specific farm with 3 barns (organized into 2 distinct sides, North and South) in which the 12 grain bins have been instrumented. Note that Feed-Link is sold under the AP® and Cumberland® brands of AGCO. The banner near the top indicates we are viewing data from the "Smith and Jones" farm from mid-July to mid-August.

There are links on the middle portion of the screen that drill down into more detailed status reports, notifications of anomalies, and options to download the logs in a spreadsheet-compatible form. This is also where the user indicates the range of data he/she wishes to view.

Each plot along the bottom shows bin weight over a one month timeframe for each bin and also totals for each side of each barn. Vertical jumps in the graphs represent feed deliveries, and the linear downward slope shows feed consumption. Nominally, bins are paired for each side of the barn, with one bin operational at a time, so there should also be portions of the plots that are horizontal, indicating that bin is not providing feed.

Figure 2 illustrates data logs collected over a month, showing the clear correlation between low feed consumption and high temperatures on two occasions. This is an indication of the kinds of things that can be learned from the collected data.

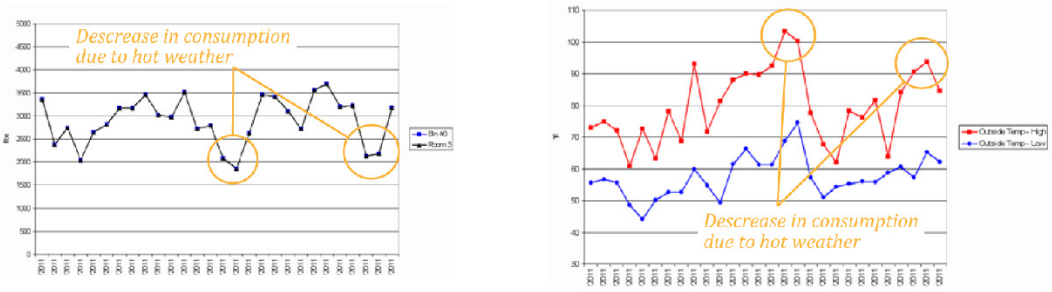
While the two figures show images from a desktop PC screen, modern remote communications capability is also supported via apps that run on smartphones and tablets.

In addition to diagnosing the root causes of issues in the barn the historical logs also enable the tracking of parameter changes by operators as well as support the demonstration and documentation of regulatory compliance. Using Feed-Link, these data logs are collected automatically and the information retained in the cloud for easy access by the owners/operators of the equipment (the farmer, in most instances).

While it should be clear that the distributed data collection and control represented by these systems is of significant value, doing so without concurrently ensuring security would be a completely unacceptable state of affairs. This is a challenge when some fraction of the equipment was not designed with secure communications in mind. Next, we describe our approach to securing these systems, with special attention given to ease-of-use considerations, as there is ample evidence that security measures that are difficult to implement are frequently circumvented by users [3], [4], [6].

III. Secure Communication

A substantial issue that the Feed-Link system addresses is the fact that there are substantial quantities of equipment that, while they provide the basic capability to communicate, their communications infrastructure is not sufficiently secure.



(a) Daily feed consumption.

(b) Daily high and low barn temperature.

Fig. 2. Plot of data logs.

Figure 3 shows an example Feed-Link installation. The Network Master™ at the center of the figure is connected to a number of instruments on the farm. The communications with these instruments are via hardwired connections with protocols that are proprietary to the specific instruments. Since they are dedicated links, they are not succeptible to eavesdropping or other network-based security vulnerabilities.

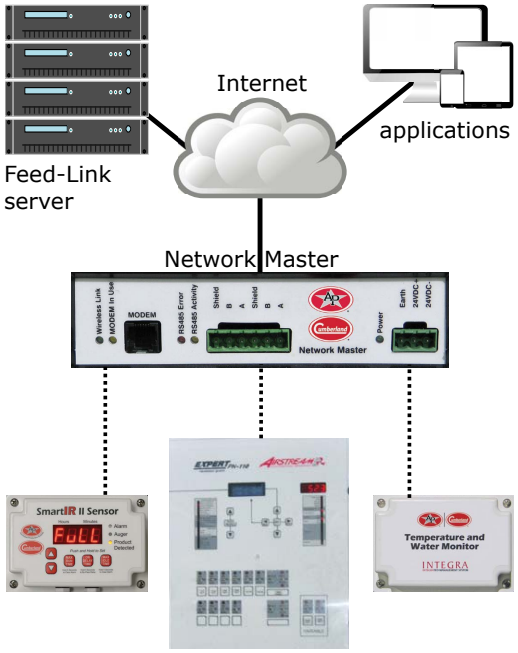


Fig. 3. Example Feed-Link system.

The Network Master is responsible for communicating information that it collects from the local equipment to the Feed-Link server in the cloud. It also maintains the data in a persistent database. When applications wish to access the data, they connect to the Feed-Link server, which checks the provided authentication credentials and then provides the requested data to the application.

There are several salient properties of this security infrastructure.

1) No connections are allowed from remote applications directly to the Network Master. In this way, the Network Master can be safely behind a strong firewall and there is no need for port forwarding or VPN access to be configured or even allowed.
2) Communications between the Feed-Link server, applications, and Network Master can be encrypted with the industry standard TLS (Transport Layer Security) cryptographic protocol [2].
3) Any proprietary communications mechanisms needed by specific equipment on the farm are not exposed to the public network.

What results is an infrastructure that allows secure communication to legacy equipment that was not designed for the threats that are commonplace in the modern world. In addition, the system balances the need for secure communications with the benefit of ease of installation. There is no need to configure firewalls, etc., for the system to be operational.

Acknowledgements

All referenced trademarks and copyrights are property of their relative owners and used by permission.

References

[1] R. D. Chamberlain, M. Chambers, D. Greenwalt, B. Steinbrueck, and T. Steinbrueck, "Devices can be secure and easy to install on the Internet of Things," in *Interconnection, Integration, and Interoperability of IoT Systems*, R. Gravina, C. Palau, M. Manso, A. Liotta, and G. Fortino, Eds. Springer, 2018, pp. 59–76.

[2] T. Dierks, "The transport layer security (TLS) protocol version 1.2," 2008, rfc5246. [Online]. Available: http://tools.ietf.org/pdf/rfc5246.pdf

[3] D. Gefen and D. W. Straub, "The relative importance of perceived ease of use in IS adoption: a study of e-commerce adoption," *Journal of the Association for Information Systems*, vol. 1, no. 1, p. 8, 2000.

[4] M. Hertzum, N. Jørgensen, and M. Nørgaard, "Usable security and e-banking: Ease of use vis-a-vis security," *Australasian Journal of Information Systems*, vol. 11, no. 2, 2004.

[5] J. S. Kumar and D. R. Patel, "A survey on Internet of Things: Security and privacy issues," *International Journal of Computer Applications*, vol. 90, no. 11, Mar. 2014.

[6] B. Schneier, "Stop trying to fix the user," *IEEE Security Privacy*, vol. 14, no. 5, pp. 96–96, Sep. 2016.

[7] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, "On the security and privacy of Internet of Things architectures and systems," in *Proc. of International Workshop on Secure Internet of Things (SIoT)*. IEEE, Sep. 2015, pp. 49–57.