IoT Benefits for Livestock Farmers

Tim Bell
Todd Steinbrueck
Roger D. Chamberlain
Brian Rieck

Tim Bell, Todd Steinbrueck, Roger D. Chamberlain, and Brian Rieck, "IoT Benefits for Livestock Farmers," in *Proc. of 18th International Conference on Distributed Computing in Sensor Systems* (DCOSS), May 2022, pp. 159-166. DOI: 10.1109/DCOSS54816.2022.00038

Presented at 4th International Workshop on IoT Applications and Industry 4.0 (IoTI4), Marina del Rey, CA, USA.

BECS Technology, Inc.
St. Louis, Missouri

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

AGCO Corporation
Assumption, Illinois

IoT Benefits for Livestock Farmers

Tim Bell
Todd Steinbrueck
BECS Technology, Inc.
St. Louis, MO, USA
{tim,todd}@becs.com

Roger D. Chamberlain
Washington Univ. in St. Louis
and *BECS Technology, Inc.*
St. Louis, MO, USA
roger@wustl.edu

Brian Rieck
AGCO Corporation
Assumption, IL, USA
brian.rieck@agcocorp.com

***Abstract*—The promise of benefit from instrumentation on the farm is substantial. However, simply connecting existing equipment to the network is not sufficient to achieve these benefits, as the resulting system is vulnerable to a multitude of reliability and security issues. We describe an approach to instrumenting livestock barns, describing some of the innovations that enable cost-efficiency, which explicitly requires paying attention to the integration of new instrumentation with existing equipment. We then articulate a range of benefits that accrue, both to the livestock and to the farmer. The result is a comprehensive understanding of barn operations, yielding many of the benefits one aspires to with IoT on the farm.**

***Index Terms*—Internet of Things (IoT), agriculture data, security, remote communications, legacy equipment**

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 [1]–[5].

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. Further, these legacy systems are predominately point solutions to individual monitoring and control applications (e.g., monitoring feed levels for inventory control). They do not make any attempt to provide an integrated, holistic view of the farm.

The benefits that can accrue from remote connectivity and access to these data are substantial. For instance, it 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 [6] and Vasilomanolakis et al. [7] describe these challenges as being pervasive across all the IoT.

Here, we describe the Feed-Link™ system, which enables legacy agricultural monitoring and control systems to effectively and securely join the Internet of Things. We will describe how it works, a number of innovative elements aimed at cost efficiency, and what benefits it provides to farmers. We will also articulate the specific security mechanisms put in place, and how these mechanisms (developed previously [8]) simultaneously enable security and ease-of-use. Essentially, what lessons have been learned about how to effectively utilize IoT on the farm.

II. Agricultural IoT Equipment and 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 a variety of firms. 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 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.

Several examples are illustrated in Figures 1 and 2. Figure 1(a) shows a hog barn that is being environmentally controlled using a VariFlame® heater, and the temperature in the barn is being monitored, while Figure 1(b) shows a poultry barn in which the feed is being delivered using the Flex-Flo™ feed distribution system [9]–[12]. In this case, both the quantity of feed and water consumed are instrumented. Figure 2 shows a pair of hopper tanks that have been instrumented to record the weight of the stored grain with load cells under each support leg [13].

A. Innovative Equipment

There is significant innovation represented in the examples above, and in many cases this reduces the costs to the farmer. In the hog barn, the heater will not source fuel to the burner unless it has a positive indication of flame (an important safety feature). Under the relevant safety regulations[1], a doubly

[1]UL 60730-2-5 / ANSI Z21.20-2014 / CSA-C22.2 No. 60730-2-5-14

2325-2944/22/$31.00 ©2022 IEEE
DOI 10.1109/DCOSS54816.2022.00038

(a) Hog barn.

(b) Poultry barn.

Fig. 1. Instrumented barns.

Fig. 2. Feed bins.

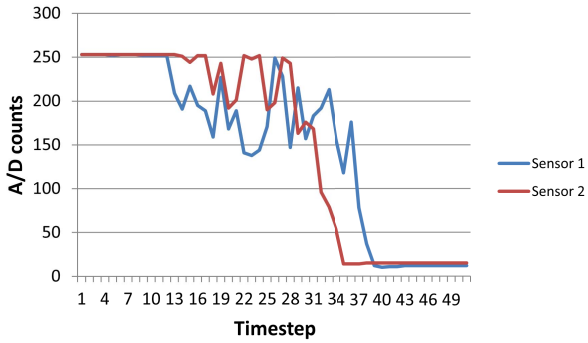

Fig. 3. Proximity detector raw data graph.

redundant control is required. The typical approach to provide this redundancy is to replicate the control in a second microprocessor and only allow the burner to operate if both control subsystems agree that it is safe. Our system improves safety and decreases costs by eliminating the second microprocessor, replacing it with custom logic that is solely dedicated to safety monitoring (not heater control). In this way, the costs associated with the second microprocessor are eliminated and the safety is improved because the redundant safety checks now benefit from divergence in design and implementation as well as simple redundancy [14].

In the poultry feeder, the feed is automatically delivered, via augers, from the on-site storage, with both hysteresis built-in to the empty/full decision at both junctions [9] and at the endpoints [11] as well as active circuitry [10] and signal processing [12] to adapt to variations across sensors and in the environment.

As an illustration of the above, Figure 3 shows the raw signal from an optical sensor. The feed detector has two light sources and two photodetectors, so we are seeing transmitted light intensity across two paths crossing a feed tube. Without feed, at the beginning of the trace, the signal is high on both sensors, indicating no feed is present. As feed is delivered and is falling through the tube, the transmitted light varies over a period of time. Once the feed fills the tube, the signal level stabilizes at a low level.

Between the initial condition of “no feed” and the final condition of “feed present” there is a transition region during which the signal(s) might be highly varying (as indicated in the figure). Conventional detectors establish a threshold signal level, and when the raw sensor reading passes this threshold, the sensor indicates “feed present”. Consider the operation, however, if a threshold of 150 were used with the above raw signals. Sensor 2 would operate just fine. However, sensor 1 would indicate “feed present” at time 22, return to “no feed” at time 25, again briefly indicate “feed present” at time 28, and toggle between “no feed” and “feed present” some more before finally stabilizing at “feed present” at time 37. One might consider simply lowering the detection threshold to 100, however, a different installation might exhibit the same behavior at this new threshold.

In our systems, the sensors used to detect the presence of feed explicitly consider this transition region, and compensate for its existence. In some cases, a pair of thresholds and hysteresis in the detection algorithm is sufficient (e.g,. if the signal values in the transition are in the middle of the signal range). In other cases, knowledge of the timing of the feed system can be used to ensure that the reading has stabilized before the ”feed present” signal is activated [12].

Another technique commonly used to measure the presence or absence of feed is a capacitive sensor, which responds to the

dielectric constant of the material that is being detected. While this works very well for feed with a high moisture content (since water has a very high dielectric constant), it can be problematic for feed with a low moisture content, and hence a low dielectric constant. Such low dielectric constant feeds can be difficult to sense using capacitive sensors because the relatively small changes in capacitance due to the presence or absence of the feed can become hidden by drift of the sensor electronics due to, for example, variations in power supply voltage. Our feed proximity detectors address this issue with innovative electronics that automatically compensate for expected variations in the reference voltage used in switched capacitor or charge pump capacitive sensors [10].

Knowledge of the quantity of grain in a feed bin is crucial inventory information, and the instrumentation of the hoppers of Figure 2 (adding a load cell to each support leg) is made more economical by the use of uncalibrated load cells, which are actively calibrated in the field under normal operation [13]. This substantially decreases the cost associated with instrumentation, as calibrated load cells are noticeably more expensive than uncalibrated ones.

In addition, there is sufficient redundancy in the raw data that it is possible to detect when a load cell has malfunctioned. Figure 4 shows both the raw data from several load cells (top graph) and the calibrated weight of feed in the bin (bottom graph). While the signal from each load cell is distinct, there are obvious similarities that can be observed.

Contrast this with the information in Figure 5, in which load cell 4 is not acting in concert with the remaining load cells. This is a clear indication of malfunctioning equipment.

B. Remote Communications

While the notion of IoT might be new, the fundamental capability to access controller information remotely is not. There are controllers that have supported remote communications for more than 2 decades. In the early years, 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 6 shows a screenshot of the Feed-Link dashboard for a specific farm (called Hilltop Farms) with 3 barns (called the North Barn, the East Barn, and the West Barn).[2] We are viewing the dashboard for the North Barn. All farm and barn names have been anonymized for privacy reasons.

The navigation panel on the left allows the user to query different barns within the same farm, or barns across different farms. Data shown in the main panel indicate bin weights, daily feed consumption, average feed consumption for the past week, auger run times, and water consumption (both daily and average over the past week). It is also possible for the user to retrieve detailed status reports, notification of anomalies, and customize his/her preferred data to view.

[2]Feed-Link is marketed under the AP® and Cumberland® brands of AGCO, as indicated by the banner across the top.

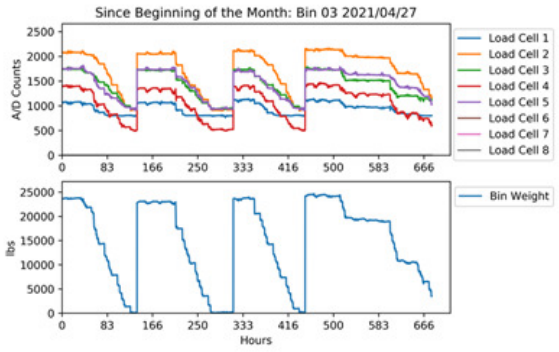

Fig. 4. Fully functioning load cells measuring bin weight.

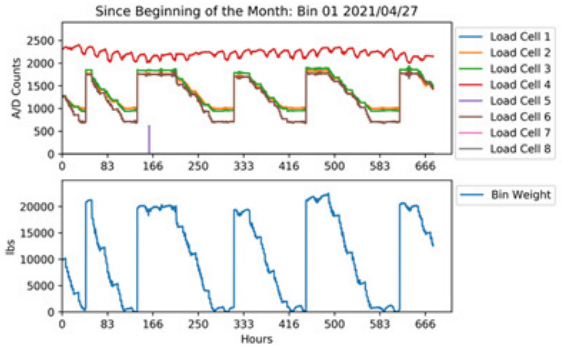

Fig. 5. Malfunctioning load cell measuring bin weight.

While the figure shows images from a desktop PC, 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 various notifications (e.g., feed added, bin empty, etc.) as well as support the demonstration and documentation of regulatory compliance. Using Feed-Link, these data logs are collected automatically and the information is 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 (this is elaborated upon next), 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. Below, 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 [15]–[17].

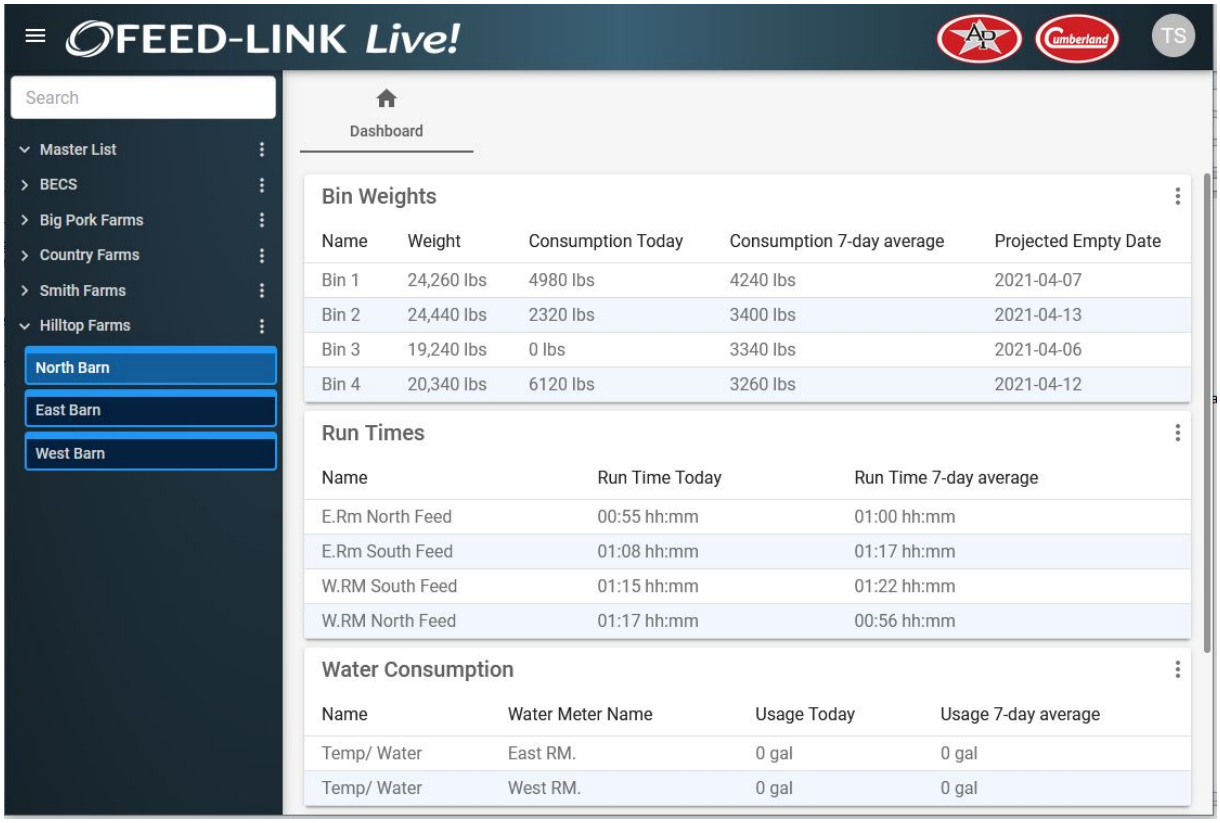

Fig. 6. Site dashboard display of Feed-Link system.

III. Benefits to Farmers

Their are numerous benefits that accrue with IoT-derived data made available to those who can take advantage of it. We articulate several of these benefits, roughly grouped into the categories of: (1) improving resource efficiency, (2) monitoring health of livestock, (3) monitoring health of equipment, (4) monitoring action of employees, and (5) managing logistics.

A common measure of the efficiency of a farm is the feed conversion ratio, or relationship between animal weight gain and feed consumed. While the obvious resource expenditure here is feed, it is also important to consider other resources, such as water, electricity, etc. If the environmental temperature is maintained effectively, this has a significant impact on feed conversion [18]–[20].

Resource efficiency can also be considered in terms of human effort as well. A significant number of farms are physically distributed in location, often with several miles of distance between individual barns (or separate farms). With more comprehensive up-to-date knowledge of the relevant circumstances at each location, the number of physical visits that are needed can be diminished. Also, limiting the number of times that a farmer needs to physically enter a barn reduces the opportunity for contamination of the barn environment.

The second category of benefit we consider is livestock health. While good environmental conditions are clearly to the benefit of livestock health [21], IoT-derived data can be an early indicator of health issues. Sudden changes in either feed or water consumption warrant the signalling of an alert, which enables fast response when health issues are present. Schillings et al. [22] recently published a comprehensive review of the various ways that electronic monitoring can impact animal health.

The third benefit category is monitoring the health of the equipment (recall the illustration shown in Figures 4 and 5). This is demonstrably one of those areas where a comprehensive view of the data is an advantage, because there are many instances in which an equipment failure is detected not so much from a sensor on the failed system, but rather by observing the impact of the failed system on other aspects of the barn. For example, when the feed control system engages an auger to pull feed from a hopper and feed the animals, the impact of the auger running is observable at both ends. First, the weight of the feed in the hopper should decrease (by a consistent amount). Second, feed should be detected at the feeders (the endpoints of the feed delivery system) within a predictable amount of time. Inconsistencies between any of these collected data are an indication of an equipment issue that needs to be addressed, since the animals are clearly not

being fed.

A second example is the environmental control equipment. Monitoring of the temperature and humidity in the barn supports the early warning of equipment issues on the part of heaters, curtain controls, fans, etc. A third example is the exploitation of redundant information in separate load cells that measure the weight of grain (this is the example from Figures 4 and 5). While it is typical to instrument each of the legs of a feed bin (e.g., illustrated in Figure 2) to ensure maximum accuracy of the grain weight data, under normal operation the load is roughly distributed evenly across the individual load cells. If one load cell is reporting data that is considerably out of line with the remaining load cells, that is a strong indication of load cell failure.

Figure 7 shows the bin weight for two bins (labeled bin 11 and 12) that are paired to provide feed for a single barn (labeled group 1) over a one month time frame. Vertical jumps in the graphs represent feed deliveries, and the linear downward slope shows feed consumption (shown in Figure 8 as well). Often, 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 (an artifact that is readily visible in these figures). These data are straightforward to mine when looking for anomalies (that could indicate either livestock health issues or equipment failure issues).

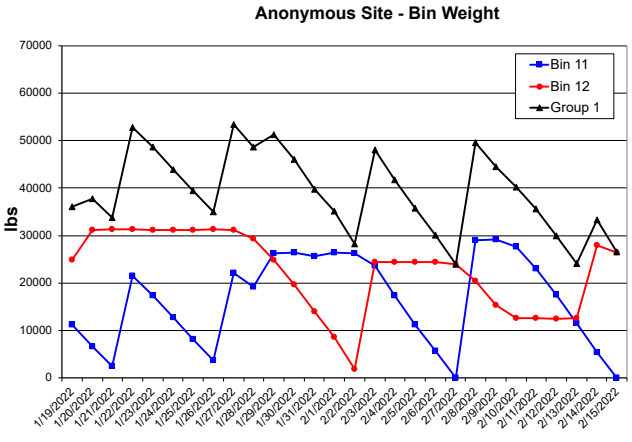

Fig. 7. Bin weight plot.

The fourth benefit category is keeping track of the actions of employees. In many modern farms, the owners/employers are physically remote, and the responsibility to perform many functions on-site on the farm is the duty of employees. Remote data availability is one of the tools that can be used to ensure those employees are effectively doing their job properly. A simple example is the corrective action needed for equipment failures. The data will show whether or not such corrective action has been successful.

The final benefit category we describe is that of managing logistics. This comes in multiple forms, some pertaining to an individual farm (or barn), others pertaining to a (potentially large) collection of farms. The logistics benefits for an individual farm include scheduling of external services of any kind, the most obvious being delivery of feed. The instrumentation of feed bins enables the projection of when each bin will be empty (see the site dashboard of Figure 6).

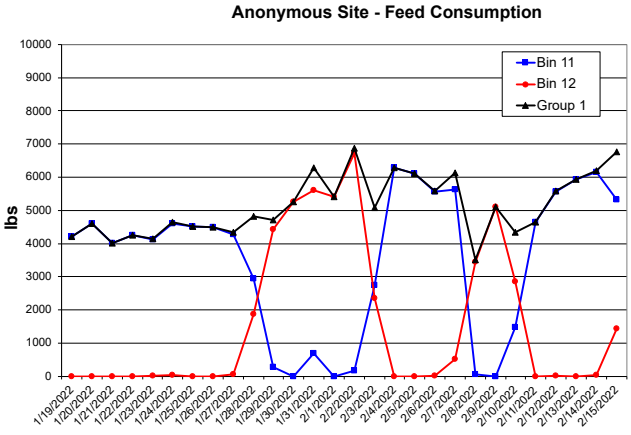

Fig. 8. Feed consumption plot.

For collections of farms, the system allows the aggregation of data across the entire set. Figure 9 shows the group dashboard associated with a collection of barns. Note the similarities between it and Figure 6, e.g., navigation on the left. Here, however, the view represents all of the barns operated by Hilltop Farms, not just a single barn. Feed-Link supports reporting of data aggregated across farms (including all the barns on each farm) for larger operators (e.g., for whom sifting through 10s of reports is much less efficient than a single, comprehensive report).

IV. Secure Operations

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

Figure 10 shows an example Feed-Link installation [23]. The Network Master™ at the center of the figure is connected to a number of instruments on the farm. These instruments might be manufactured by a wide variety of suppliers, and in many cases were not designed with sufficient security mechanisms in place (e.g., their design often pre-dates the Internet). The figure includes a SmartIR II feed proximity sensor, an Airstream ventilation controller, and an Integra temperature and water consumption monitor. Communications with the instruments are typically via hardwired connections with proprietary protocols. As long as the connections are dedicated links, they are not susceptible to eavesdropping or other network-based security vulnerabilities.

The difficulty arises when one wishes to use a public network to access these legacy instruments. While security is not a substantial concern on a dedicated link, it is crucial to get it right when the data are being communicated across the

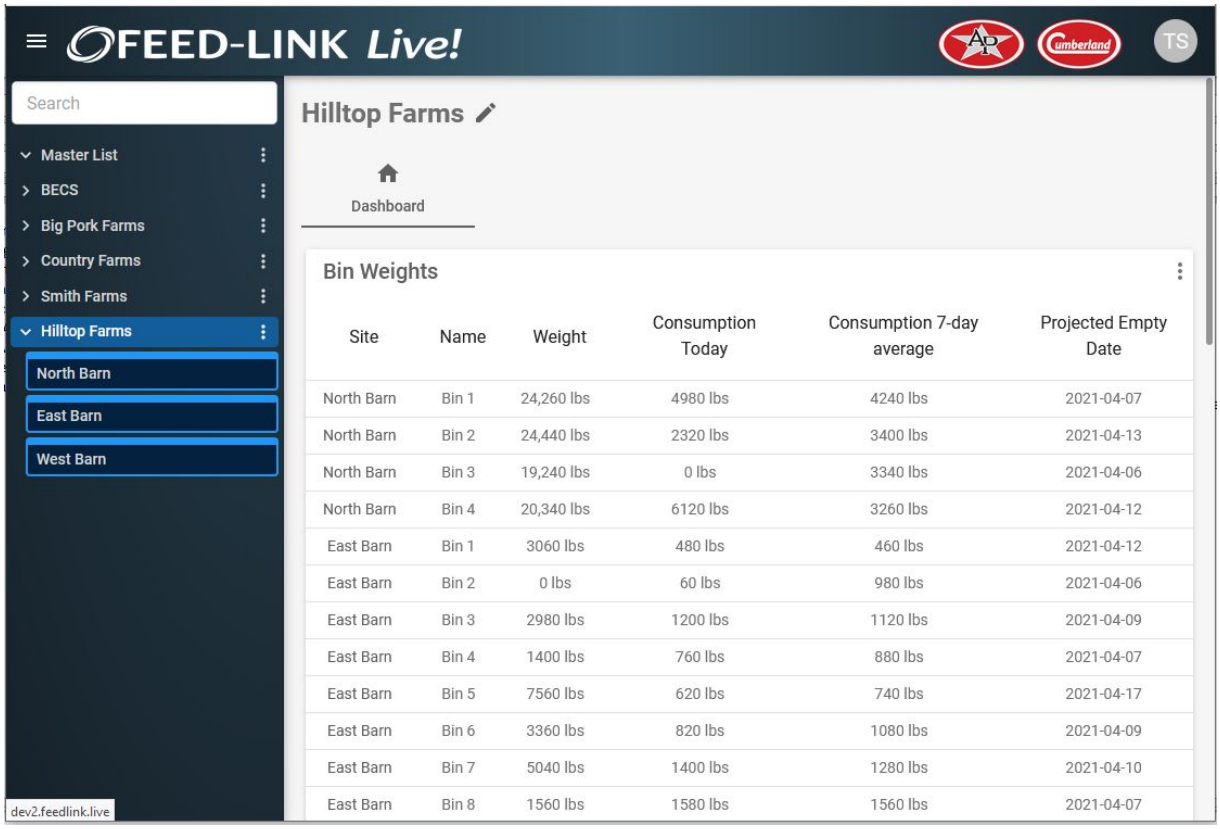

Fig. 9. Group dashboard display of Feed-Link system.

internet. In a number of cases, the equipment design actually predates the internet, so expecting the individual equipment designs to be effectively secure in the current landscape is completely unreasonable.

The initial line of defense for IoT equipment is the firewall; however, making a connection to the desired equipment through a firewall can be problematic. Two approaches that are commonly used to address this issue are the use of a VPN, or virtual private network, and the use of port forwarding [24]. We avoid both of these and implement a better approach.

The Network Master is responsible for communicating information that it collects from the local equipment to the Feed-Link server in the cloud, through a firewall, which it does using techniques described by Chamberlain et al. [8]. 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, a strong firewall can be installed between the Network Master and the public network 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 are encrypted with the industry standard TLS (Transport Layer Security) cryptographic protocol [25].
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. The ability to continue to utilize legacy equipment securely, rather than require its replacement, is an obvious economic benefit for the farmer.

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. Traditionally, a secure local-area network requires a firewall between it and the public Internet. The most common approach to enabling remote communication through this firewall is via port forwarding or VPN access, both of which have complications that it is nice to avoid. Both port forwarding or VPN access require significant IT knowledge

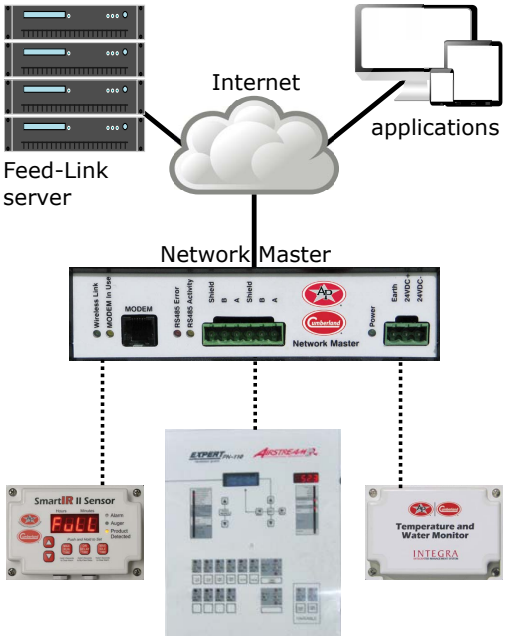

Fig. 10. Example Feed-Link system [23].

(not a common skill set on the farm), and can be insecure if not done properly. See, e.g., the description of the 'port forward' exploit described by Ammann et al. [26].

Rather than have the remote system connect to the Network Master directly, the Network Master, which is inside the firewall, makes an outbound connection to the Feed-Link server. The Network Master then maintains an open socket on the server, which will subsequently be used for authenticated remote connections.

The take-home message here is that the remote communications capability is install-and-go, without the need for complicated VPN or port forwarding setup requirements. And this ease of installation does not bring with it security vulnerabilities. State-of-the-art network security is maintained.

V. Conclusions and Future Challenges

The benefits of effective use of IoT-enabled data on the farm are huge. Health of the livestock is improved, repair of faulty equipment is facilitated, resource consumption is decreased, and situational awareness is substantially improved, both for an individual farm and large collections of farms. These benefits, however, do require comprehensive instrumentation, and much legacy installed equipment currently present on the farm was not designed for the modern, insecure networking environment. This leaves farmers with the unwelcome choice between forgoing some of the benefits of IoT-enabled data or replacing perfectly functional equipment with newer copies that are network secure.

The Feed-Link system enables farmers to avoid this choice. Legacy, insecure equipment is safely protected behind a firewall and safe, secure data are delivered to the Feed-Link server in the cloud. This enables a robust set of real-time data to be available remotely, facilitating all of the benefits mentioned above. A demonstration video is available [27], which illustrates the use of the capability both in agriculture and in an aquatics application.

The challenges before us now focus more on what use do we make of these data? In particular, what are the appropriate user interfaces for the presenting information to the various stakeholders? For example, farmers simply want the equipment to do its job effectively, while equipment suppliers are more interested in diagnostic assistance when equipment does fail.

Historically, user interfaces for IoT systems have tended to make everything available to every user, under the assumption that the user knows the system best and therefore wants access to all the raw data. This, frankly, is poor user interface design. It is incumbent on the designers of IoT-based systems to understand the various needs of the different users (e.g., farmers vs. equipment suppliers) and design interfaces that are tailored specifically to those needs. We are currently actively involved in this exercise.

Acknowledgment

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

References

[1] J.-C. Zhao, J.-F. Zhang, Y. Feng, and J.-X. Guo, "The study and application of the IOT technology in agriculture," in *Proc. of 3rd International Conference on Computer Science and Information Technology*, vol. 2. IEEE, 2010, pp. 462–465.

[2] S. Jaiganesh, K. Gunaseelan, and V. Ellappan, "IOT agriculture to improve food and farming technology," in *Proc. of Conference on Emerging Devices and Smart Systems*. IEEE, 2017, pp. 260–266.

[3] M. S. Mekala and P. Viswanathan, "A survey: Smart agriculture IoT with cloud computing," in *Proc. of International Conference on Microelectronic Devices, Circuits and Systems*. IEEE, 2017.

[4] O. Elijah, T. A. Rahman, I. Orikumhi, C. Y. Leow, and M. N. Hindia, "An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3758–3773, 2018.

[5] M. S. Farooq, S. Riaz, A. Abid, T. Umer, and Y. B. Zikria, "Role of IoT technology in agriculture: A systematic literature review," *Electronics*, vol. 9, no. 2, p. 319, 2020.

[6] 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, pp. 20–26, March 2014.

[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*. IEEE, September 2015, pp. 49–57.

[8] 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.

[9] T. D. Fleshner, *Infrared Feeder Controller*. U.S. Patent #8,056,506, issued November 15 2011.

[10] R. A. Livingston, *Balanced Charge Pump Capacitive Material Sensor*. U.S. Patent #6,362,632, issued March 26 2002.

[11] N. Pickens, *Poultry Feeder with Level Sensor*. U.S. Patent #9,247,718, issued February 2 2016.

[12] T. Steinbrueck, *Proximity Detector*. U.S. Patent #10,604,353, issued March 31 2020.

[13] R. A. Livingston, *Method and Apparatus for Measuring Weight Using Uncalibrated Load Cells*. U.S. Patent #6,636,820, issued October 21 2003.

[14] V. Kharchenko, "Diversity for safety and security of embedded and cyber physical systems: Fundamentals review and industrial cases," in *Proc. of 15th Biennial Baltic Electronics Conference*. IEEE, 2016, pp. 17–26.
[15] 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.
[16] 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, pp. 52–65, 2004.
[17] B. Schneier, "Stop trying to fix the user," *IEEE Security Privacy*, vol. 14, no. 5, pp. 96–96, September 2016.
[18] G. Straub, J. Weniger, E. Tawfik, and D. Steinhauf, "The effect of high environmental temperatures on fattening performance and growth of boars," *Livestock Production Science*, vol. 3, no. 1, pp. 65–74, 1976.
[19] A. Cahaner and F. Leenstra, "Effects of high temperature on growth and efficiency of male and female broilers from lines selected for high weight gain, favorable feed conversion, and high or low fat content," *Poultry Science*, vol. 71, no. 8, pp. 1237–1250, 1992.
[20] J. May and B. Lott, "The effect of environmental temperature on growth and feed conversion of broilers to 21 days of age," *Poultry Science*, vol. 79, no. 5, pp. 669–671, 2000.
[21] D. Sainsbury and P. Sainsbury, *Livestock Health and Housing*, 2nd ed. Bailliere Tindall, 1988.
[22] J. Schillings, R. Bennett, and D. Rose, "Exploring the potential of precision livestock farming technologies to help address farm animal welfare," *Frontiers in Animal Science*, vol. 2, p. 639678, 2021.
[23] T. Bell, R. Chamberlain, M. Chambers, B. Rieck, and T. Steinbrueck, "Security on the farm: Safely communicating with legacy agricultural instrumentation," in *Proc. of 15th International Conference on Distributed Computing in Sensor Systems*. IEEE, 2019, pp. 192–194.
[24] A. Apvrille and M. Pourzandi, "Secure software development by example," *IEEE Security & Privacy*, vol. 3, no. 4, pp. 10–17, 2005.
[25] E. Rescorla and T. Dierks, *The transport layer security (TLS) protocol version 1.3*. ITEF, August 2018, rFC8446.
[26] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in *Proc. of 9th ACM Conference on Computer and Communications Security*. ACM, 2002, pp. 217–224.
[27] R. D. Chamberlain and T. Steinbrueck, "Demo abstract: More than two decades of IoT," in *Proc. of IEEE/ACM 5th International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2020, pp. 268–269, demo video is available at https://wustl.app.box.com/s/43dpiluui9jfkmkhjku4jzzu0ogbtqvx.