Demo Abstract: More Than Two Decades of IoT

Roger D. Chamberlain
Todd Steinbrueck

Roger D. Chamberlain and Todd Steinbrueck, “Demo Abstract: More Than Two Decades of IoT,” in *Proc. of ACM/IEEE International Conference on Internet of Things Design and Implementation* (IoTDI), April 2020.

BECS Technology, Inc.
St. Louis, Missouri

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

Demo Abstract: More Than Two Decades of IoT

Roger D. Chamberlain
Dept. of Computer Science and Engineering
Washington University in St. Louis
BECS Technology, Inc.
roger@wustl.edu

Todd Steinbrueck
BECS Technology, Inc.
St. Louis, Missouri, USA
todd@becs.com

***Abstract*—While the popularity of the acronym IoT is fairly new, the concept certainly is not. In this demo, we illustrate the use of remote communications (all the way back to POTS) for monitoring and managing what are now called IoT systems.**

***Index Terms*—history of IoT, aquatic IoT, agricultural IoT**

I. Introduction

One the earliest uses of the IoT term is by Kevin Ashton, in a presentation at Proctor & Gable in 1999 [1]. Quoting from [1], "We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, ... without the limitations of human-entered data." Examples of devices that would clearly meet the definition predate the term, e.g., the instrumentation of the Coke vending machine at CMU in the early 1980s[1]. A comprehensive history of the early years was written by Suresh et al. [2].

BECS Technology, Inc., is a manufacturer of monitoring and control equipment in a number of markets (agriculture, aquatics, refrigeration) and has been providing remote connectivity to its equipment [3], [4] since its inception in 1991. In this demo, we illustrate the progression of remote connectivity, initially to individual controllers via dedicated links and progressing to collections of equipment under common owner/operator control.

II. History and Utility

BECS has been building the IoT for over two decades. Equipment manufactured by BECS monitors and controls the water chemistry in recirculating water systems (e.g., pools, drinking water, waste water) and feeds the livestock on the farm. Early connectivity was provided via modems over POTS, and current systems connect securely via the Internet [4], [5].

Initially, for equipment to support remote connectivity, it was necessary to install a modem and connect the modem to the telephone network (POTS). A user who wished to contact the controller needed to know the telephone number, and the use of dedicated numbers was an economic impediment to scaling up the number of controllers. While never implemented, we explored approaches to sharing telephone lines [6]; however, the ubiquitous availability of the Internet soon eliminated this bottleneck.

[1] https://www.cs.cmu.edu/~coke/

Figure 1 shows the modern approach to equipment connectivity. Controllers are typically installed behind firewalls, and (when enabled to do so) will initiate an outbound secure socket connection to a cloud-based server. This has the distinct advantage that equipment owner/operators (who are experts on water chemistry, not security of IT systems) can easily install controllers without having to setup VPNs or port forwarding mechanisms in the firewall (a practice that is frequently insecure [7]). Additional servers handle front-end tasks (BECSys Live! server) as well as managing access to both real-time data and historical logs. While the figure specifically is pertinent to the aquatics systems [3], the agricultural IoT infrastructure is very similar, with bridging equipment to support legacy controllers [4].

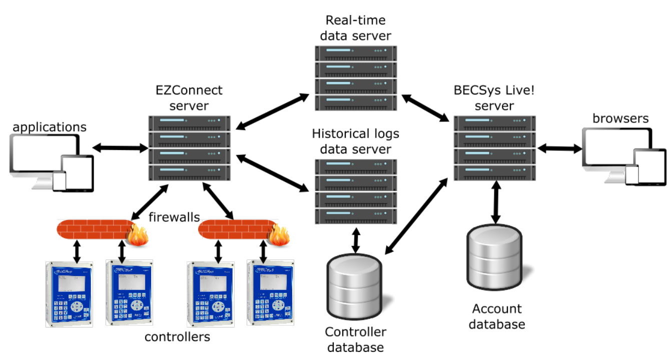

Fig. 1. Aquatic IoT infrastructure. Each of the servers (and databases) are deployed in the cloud and can be replicated to support increased capacity and/or fail-over reliability.

The ability to connect to an individual controller remotely has historically provided significant benefits, including: communicating alarm conditions, diagnosing the root causes of errors in the monitored system, tracking of parameter changes by operators, and remotely altering the configuration of the controller (e.g., changing setpoints, alarm levels, etc.). However, there are a number of limitations that this mechanism implies. First, data collection must be triggered by the user. Second, the data are not readily portable. Third, the data are low-level, i.e., little data analysis is performed.

We now regularly collect information from a set of controllers (all under common ownership), retain the information in the cloud, and benefit from the aggregation of the data.

III. User Experience

The demo illustrates several aspects of a user's experience. Starting with a connection to an individual controller, the user can view the current status of the controller, download accrued data logs, and configure the controller. Figure 2 illustrates the console (real-time) display for an aquatics controller monitoring a recreational body of water (a raft slide). Figure 3 shows the dashboard (summary) display for an agriculture controller monitoring three barns. Note how the needs of these two distinct markets result in primary displays that are substantiallly different from one another, even though there are strong similarities in the underlying technical infrastructure.

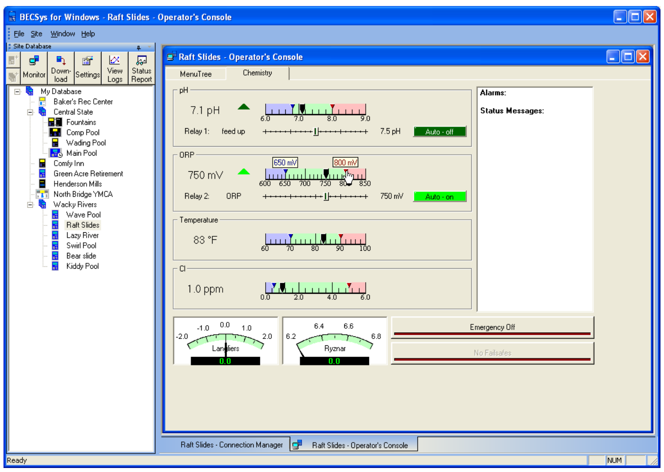

Fig. 2. Console display of remote aquatics controller [8].

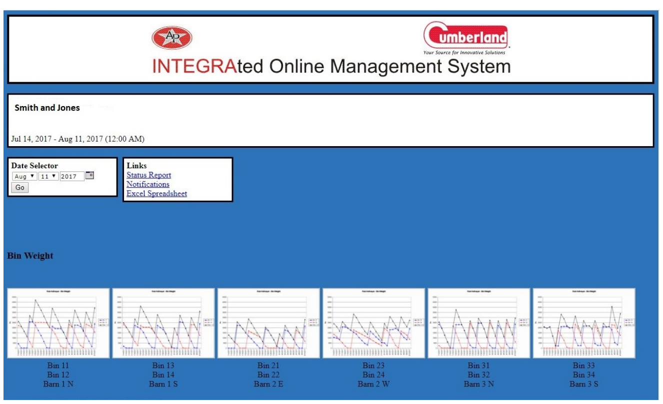

Fig. 3. Dashboard display of agricultural system [4].

While both of the above figures illustrate images from large displays (e.g., a desktop or laptop PC), this information is also available via smaller hand-held devices using a more compact presentation style (also included in the demo).

The true value of data in the cloud, however, is the impact it can have on the organization as a whole. By combining data from many controllers we can learn more than is possible from any one in isolation. A number of benefits accrue from access to these data, including:

1) verifying regulatory compliance,
2) maintaining inventory stocks at appropriate levels,
3) remote notification of alarms, and
4) diagnosing and correcting problems without having to be physically on-site.

Each of these provides significant economic benefits for the equipment owner/operators.

Figure 4 shows a sample summary view from a collection of aquatics controllers. Here, each body of water has a row in the summary, which contains the primary sensor readings. This is precisely the information operators want to know across the set of installations for which they are responsible.

Water World

Site	System Time	Alarms	p H	ORP	Alkalinity	Flow Rate 1	Temperature	Total Chlorine	F
Spa	12:57:22 PM	2	6.96	220 mV		0.0 gpm	56 F	0.00 ppm	
Lap Pool	10:59:20 AM	2	7.20	834 mV		318.6 gpm	83 F	3.7 ppm	
Main Pool	12:02:50 PM	0	7.49	799 mV		360.9 gpm	79 F	0.0 ppm	

Fig. 4. Screen capture of summary view data presentation for a group of water bodies. Additional details are available via a link associated with each individual row [3].

The demo includes live connectivity to running systems, both in aquatics and in agriculture, an illustration of both individual controller access as well as aggregate data analysis from multiple sites. The demo will show how the systems for the two distinct markets are similar and how they are different. We illustrate the progression of IoT capabilities from its inception to the present, a span of over two decades.

References

[1] K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, Jun. 2009. [Online]. Available: http://www.rfidjournal.com/articles/view?4986

[2] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in *Proc. of Int'l Conference on Science Engineering and Management Research*. IEEE, Nov. 2014.

[3] R. D. Chamberlain, M. Chambers, D. Greenwalt, M. Scharth, B. Steinbrueck, T. Steinbrueck, and D. Thomas, "Water in the cloud: Understanding water chemistry via the internet of things," in *Proc. of 15th Int'l Conference on Distributed Computing in Sensor Systems*. IEEE, May 2019, pp. 408–415.

[4] 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 Int'l Conference on Distributed Computing in Sensor Systems*. IEEE, May 2019, pp. 192–193.

[5] R. D. Chamberlain, M. Chambers, D. Greenwalt, B. Steinbrueck, and T. Steinbrueck, "Layered security and ease of installation for devices on the Internet of Things," in *Proc. of 1st Int'l Conference on Internet-of-Things Design and Implementation*. IEEE, Apr. 2016, pp. 297–300.

[6] R. D. Chamberlain and J. C. Bell, "Method and apparatus for efficient use of communication channels for remote telemetry," U.S. Patent 6,940,421, Sep. 6, 2005.

[7] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," in *Proc. of 9th Conference on Computer and Communications Security*. ACM, Nov. 2002, pp. 217–224.

[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.