E360 Outlook

EMERSON

Connecting the Commercial Kitchen

How IoT in foodservice is transforming equipment and end user operations

By Paul Hepperla
Vice President, Solutions Integration—Foodservice
Emerson Commercial & Residential Solutions

IoT in foodservice is often referred to as *the connected kitchen,* or the ability to transform common kitchen equipment into smart devices that communicate with each other when needed, but also connect to and leverage the power of cloud services for greater operational efficiencies.

At the core of any foodservice operation — whether it's a restaurant or modern convenience store — is its ability to consistently prepare and deliver safe, fresh and high-quality products to its customers. If the kitchen is considered the heart of a home, then the commercial kitchen is where foodservice operators capture the hearts of consumers. In recent years, we've heard a lot of noise about how the Internet of Things (IoT) is transforming nearly every aspect of modern life; among these is the operation of the commercial kitchen.

IoT in foodservice is often referred to as *the connected kitchen,* or the ability to transform common kitchen equipment into smart devices that communicate with each other when needed, but also connect to and leverage the power of cloud services for greater operational efficiencies. In doing so, the connected kitchen potentially addresses a variety of challenges at key points throughout the foodservice supply chain:

- Store managers and service technicians — automate the monitoring and reporting of equipment statuses; receive maintenance alerts for diagnostics and fast issue resolution
- Foodservice operators — establish centralized control of their store network, including visibility to not only kitchen equipment, but also HVAC, refrigeration and lighting systems
- Corporate analysts — track trending consumer behaviors for targeted marketing initiatives
- Original equipment manufacturers (OEMs) — gain access to performance analytics for research, development and product improvement purposes

From temperatures to cook times, energy consumption to consumer foot traffic, product hold times to refrigerated door openings, the range of information available grows every day. This data comes from communicating equipment, sensors, controls and local gateways and is then transferred to the cloud (or another data repository) for remote access. On the surface, the benefits of this data are self-evident, and the abundance of information seems valuable. But the inherent challenges of capturing data on this order of magnitude are compiling, parsing and presenting it in a way that's useful for each end user.

For example, let's imagine what a typical store manager would like to see from their connected kitchen and their facility's information dashboard. The store manager's priorities are likely much different than those of the engineer at the OEM gathering data on equipment performance. The manager wants to know that their operation is running well, which includes features such as visibility to identify problems quickly and escalate resolutions to the appropriate staff or service members. Key information should be presented plainly and quickly in an easy-to-read interface (or dashboard), without overloading the manager with unnecessary details.

Another misconception is that IoT and connected kitchens are simply prepackaged solutions that get installed and implemented the same way, regardless of the company's operational priorities or information technology (IT) infrastructures. In reality, these may vary widely depending on the organizational objectives and IT preferences, security considerations and preferred equipment providers. Regardless, the operator's goals of the program typically fall into one or more of the following data categories:

- Food safety and quality
- Operational efficiencies
- Maintenance and service
- Revenue growth
- Energy efficiencies

Proving the case for IoT in foodservice

Despite the inherent challenges, there are many examples of successful IoT implementations in the foodservice sector. We'll look at two examples where an OEM and an end user have leveraged IoT connectivity to achieve their unique operational objectives.

Foodservice operator — operational efficiency and revenue growth focus

Maintaining menu variety and product consistency are persistent challenges for many foodservice chains, where menu updates typically require a labor-intensive, oven-programming process for each store. To address these challenges, a leading foodservice operator sought to enable connectivity in their cooking ovens that would streamline this process and help ensure the highest-quality menu items.

Their solution was to remotely push recipe instructions to multiple ovens across an 800-store network. The new process eliminated the manual USB stick distribution and oven programming required at each store by automating the menu update process and confirming the recipe uploads upon completion. The operator's objective was to introduce more flexibility into their menus to better adapt with specialty seasonal offerings and regional menu preferences.

The equipment modification and IT architecture started with the installation of a new custom control board on existing ovens, which were then connected to the current stores' Wi-Fi networks. Instead of using the cloud, the operator then created its own proprietary FTP site to store to help protect their competitive data.

The results exceeded the operator's expectations:

- New recipes were digitally distributed at night to minimize disruptions, providing a simple method for updating menus and confirming their readiness to prepare the new items. This gave the chain the assurance that new foods were available to match their advertising and promotional investments.
- Process automation saved $100K annually in operating costs compared to the manual USB method.
- The modified ovens now have the capabilities to push remote firmware updates, while laying the groundwork for future kitchen equipment iterations.

Ice machine OEM — maintenance and service focus

As is the case with most OEMs, this particular ice machine manufacturer was looking to collect data in an effort to make continuous design improvements. They embarked on an eight-month connectivity field trial that would allow remote equipment monitoring in 90 field test units located around the globe. The system was set up to send text and email alerts about unit performance. Designated personnel would then evaluate the data, respond to specific alerts, and implement changes to the machine design.

To enable connectivity and remote communications, the test units were equipped with an updated control board (RS-485 with MODBUS for serial communication). A cellular gateway (TC/IP) was installed at the test sites to allow for communication between the ice machines and the cloud.

At the end of the trial, the test units had achieved multiple objectives:

- Transitioning from a reactive maintenance model to a proactive, preventative approach helped allow for remote diagnoses, the ability to provide the correct replacement parts, and service instructions for technicians, which often preempted an equipment shutdown.
- Ice machine connectivity enabled the OEM to analyze temperature trends and remotely adjust equipment data.
- Performance insights prompted a change in the unit design, resulting in an improved temperature probe.
- Remote updates to the firmware helped improve the operations of individual ice machines and across the field trial network of sites.

OEM data security and operator dashboards

While the examples mentioned herein demonstrate the potential for connectivity in foodservice OEM applications and end user operations, they also are indicative of how IoT architectures can vary depending on an organization's objectives. An OEM's goals are to inform the design and engineering processes by capturing as much data about the operation of their equipment as possible; a foodservice operator only needs a fraction of this data to keep the operation running smoothly.

OEMs and foodservice operators are also more concerned about protecting their proprietary information. Thus, the IoT infrastructure must be built with appropriate safeguards to help operators maintain data security. In the aforementioned foodservice operator example, this was accomplished with a secure, private FTP. As multiple OEM equipment and systems become connected to the IoT infrastructure, the ability to maintain that level of data security among them will become even more essential.

Conversely, foodservice operators will need tools to consolidate data from multiple OEMs and present it in a simple, easy-to-use dashboard. Fortunately, third party providers such as Emerson have the domain experience to serve as a neutral collector of information, helping OEMs preserve data security while creating intuitive user interfaces for foodservice operators.