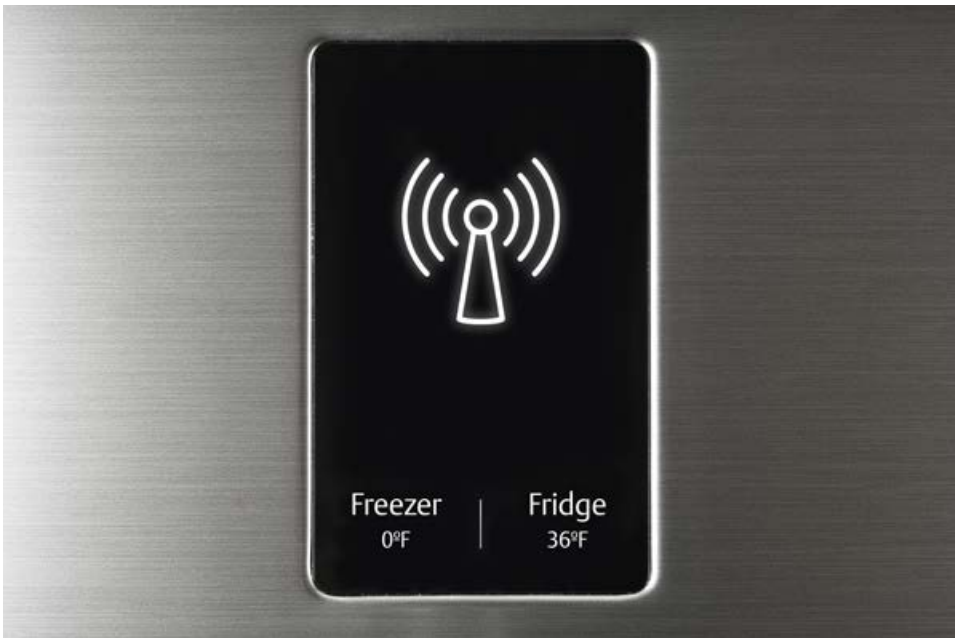
E360 Outlook | APRIL 2020

EMERSON

# Automating the Commercial Kitchen – Part 3

*What the future may hold, data security challenges, IoT protocols and standards*





By Paul Hepperla
Vice President, Solutions Strategy, Cold Chain
Emerson

The proliferation of internet of things (IoT) technologies in commercial restaurants represents potentially transformative benefits to operational efficiencies. From reducing labor and streamlining processes to ensuring food safety and improving service technician diagnostics, connecting the commercial kitchen promises to disrupt kitchen operations as we currently know them. But compared to other industries, IoT adoption is relatively slow in the foodservice sector — at a level of technological sophistication that industry insiders would refer to as "an experimentation phase."

In the final article of this series, we'll speculate on the future of IoT-driven kitchen automation while exploring prevalent concerns about data security and establishing standard communication protocols. As is the case from the first two articles in this series, the insights we'll present are based on the experiences and opinions of key industry stakeholders from a recent E360 panel discussion:

- Chuck Guerin, vice president for controls of the Middleby Corporation, a leading manufacturer of commercial cooking equipment
- Jim Kleva, director of equipment engineering of Wendy's, a global quick service restaurant (QSR) chain
- Matt Toone, vice president, sales & solutions, Cold Chain, Emerson

### The automated kitchen of the future

Today, the application of IoT technologies in the foodservice industry runs the gamut from tire-kicking and experimentation to full-scale implementation. But when we asked our panelists to speculate on what their current IoT applications could possibly lead to, their answers provided a glimpse into the future.

According to Kleva, Wendy's sees the greatest potential for IoT to improve speed and customer service levels in their drive-through procedures. "We're asking the question, 'Can we know

*Panelists (T to B): Matt Toone, Jim Kleva and Chuck Guerin*

*"When it comes to connectivity, our biggest focus is security, but it's also a tremendous challenge."*

what the customer's going to order before they order it?' so we can have it ready and fresh for them by the time they pull up to the drive-through window.

"We would need to analyze a lot of data to do that, such as: transaction history, transaction data in real time at nearby stores, traffic patterns, weather, school events, cars in the parking lot and people entering your building. Then, somehow combine all this information and determine when to cook two hamburgers," he said.

From a customer's perspective, this would require them to opt in for this level of service, potentially even allowing stores to read their license plates or use facial recognition technology. Regarding this degree of automation, Kleva conceded, "Currently, our customers don't want us to go there."

He added that customers would be more receptive to a scaled-back version of that scenario. "We could use technology to say, 'I know it's you, and this is what you ordered last time,' or we could base recognition decisions on a demographic level, or whether the customer is a child or an adult. Even a five- to 10-second heads-up could make a huge difference in our drive-through operation," he said.

Guerin added that since Middleby's connected equipment initiatives are already processing data for menu pushes and service-related alerts, the next generation of technologies will expand on these capabilities.

"Our next step is to improve on these processes," he said. "We have a tremendous amount of data going between machines and the cloud, and as we make that information available to more connected machines within the organization, we can provide assistance to a variety of processes.

"Not only could we predict what might be ordered, but we could potentially tell the controller, equipment and operator to put fries down or cook two hamburgers — and do that automatically. From our perspective, that's where we're going to start to see some real benefits of connected equipment and systems within the kitchen," he said.

**Ensuring data security**

Data security is often cited as one of the most common concerns and potential barriers to adopting IoT in commercial kitchens. And according to Toone, it's a key focus of their product development efforts — and a top priority for customers.

"When it comes to connectivity, our biggest focus is security, but it's also a tremendous challenge," he said. "As we work with other large QSRs, we're finding that different equipment providers each have their respective assets connected, and as a result, QSRs are dealing with multiple platforms. Our challenge is to safely and securely pull all of this data into meaningful, useable information. That's why establishing a common architecture, or at least flexible APIs, will become more important as the foodservice industry becomes more connected."

To maintain security across all franchisees, Kleva said that their goal is to first establish a common footprint. "We require certain pieces of equipment to be used within the restaurants — like POS (point-of-sale) equipment and things of that nature — so we can ensure that the items we promote and recommend are both secure and stable," he said.

"Stabilization is just as important to us as security," Kleva added. "Everything we do in our restaurants has to be scalable across the network. For example, if we have poor stability in rural areas, it's not scalable. This is one reason why we try to limit the

*"As OEMs, we're all competing and we're all trying to figure out an approach that meets our customers' needs."*

amount of communication needed outside of the restaurant, and why most of the communication within a restaurant is between the equipment and the restaurant server. Typically, we only need to reach outside of the restaurant a few times a day, and our IT group closely safeguards that communication."

Guerin said that Middleby addresses their customers' security concern on a case-by-case basis. "We work with their IT departments to identify a strategy that will ensure that the proper security measures are in place. Within our systems, we have security protocols to ensure that we minimize unauthorized access," he said.

"We also understand that stabilization is equally important — making sure all the necessary equipment is connected to Wi-Fi or cellular networks to enable functionality such as menu pushes," Guerin added. "If a customer does a menu push to 2,500 restaurants, and 10 percent of them don't get updated, who manages that? Who determines if the cause was Wi-Fi or if the equipment was off, and who pays for that service call? These are potential new questions and costs of automating the commercial kitchen."

**Establishing common standards and protocols**

Another emerging challenge associated with the trend toward kitchen connectivity is the proliferation of different types — typically proprietary to equipment providers — of communication protocols and connectivity standards. According to Guerin, establishing a common architecture is a chief component in allowing the disparate types of equipment to communicate more easily.

"We would love it for QSRs like Wendy's to simply rebrand one of our Connect systems and then allow other OEMs to integrate their equipment as well — but that's not likely going to be the case most the time. In reality, other providers will also have their own proprietary solutions. Creating an architecture where equipment simply connects with each other alone will not solve the problem; it's also about how these systems will collaborate and communicate messages among them. These are difficult things to accomplish, and as an industry, we're not there yet."

When evaluating the possibility of standardization of technology and protocols, Toone added that Emerson was adopting an API-based approach. "Relatively speaking, extracting the data is easy; putting it onto a common platform that's cost-effective is the hard part," he said. "The last thing a restaurant operator wants is 12 gateways sitting in their store. But there are so many companies competing in this space that it's going to be extremely difficult to bring them all underneath one common umbrella. In terms of aggregating data and then processing it into a useable form, we're finding that APIs may make the most sense."

Guerin stated that the industry as a whole has yet to make an appropriate financial case for adoption of a true standard. "Currently, there's not a safety or compelling critical infrastructure issue forcing the industry to adopt a standard system," he said. "As OEMs, we're all competing and we're all trying to figure out an approach that meets our customers' needs."

Kleva conceded that the smaller players are the ones who stand to suffer the most from a lack of a common standard. "I've got a large corporate IT department, and we've standardized our footprint to six to seven main pieces of equipment, so we can handle making those communicate," he said. "It's the smaller players that really stand to benefit from a common architecture."

Toone concluded that as an industry, it's in the customer's best interest to create a common architecture. "It may not be easy, but it's critically important for us to work toward a common platform or goal."

At Emerson, we believe these efforts are essential to providing what the industry needs: equipment that is financially viable and easily connectible across current and legacy systems. We welcome you to read Article 1 and Article 2 if you'd like to review the full series.