

# Are Smart Buildings More Work?

Ian Haberman

## THE QUEST TO WORK SMARTER, NOT HARDER

Are smart buildings and smart equipment creating more complexity and work for facility managers? It stands to reason if you are adding more things to the facility, you are also adding to your list of things to maintain and repair. It's counterintuitive because these smart products are promoted as tools for facility managers. However, our industry doesn't often discuss that the tools themselves need upkeep, too.

If done correctly, the new internet-enabled devices will bring your facility new powers of remote control, visibility, equipment fault detection and automation. But if you make poor choices around product selection and architecture, you may find yourself looking back, dreaming of simpler times.

Before adding new Internet of Things (IoT) devices in your facility, consider these often-neglected topics for discussion:

### BATTERY REPLACEMENTS

Sensors that require batteries are setting a facility management program up for more work. You now have new parts to manage: battery type A for equipment X; battery type B for equipment Y. How often will batteries need to be replaced, and how much of a forgiveness window will you have? Will this be a new task for property managers? How much time will it take to replace the batteries, and is there better use of their limited time on site?

When evaluating battery life, it is critical to understand how often sensor data is transmitting. Most sensor values should have a minimum data-collection frequency of once per minute. Beware of systems that need five-, 10- and even 60-minute intervals in order to offer acceptable battery life. You are not going to get great alarms or analytics with such poor data resolution, which ultimately puts the net value of the system in question.

Replacing batteries may not seem like a lot of work, but as with any multi-site operation, when you are talking about managing 15, 50 or 500 sites, it starts to add up. Refraining from using battery-based sensors wherever possible is an easy way to keep data quality in check and the added work of IoT to a minimum.

### WIRELESS SIGNAL MANAGEMENT

With wireless sensors comes wireless signals, and the restaurant is not the most forgiving wireless environment. Kitchen equipment, walk-in refrigerators, hoods and stainless-steel backsplashes create unfriendly barriers to a wireless ecosystem. You may think once you're installed you're in the clear, but what happens when the facility next door installs a new wireless gadget? What happens when microwave usage increases or was not considered during install of the wireless equipment?

Choppy signals result in bad data quality. Bad data quality results in false alarms and inferior reporting results. An inconsistent signal can also mean improper equipment operation if that system depends on the accuracy of the sensor.

Wireless signal management is an unspoken new problem brought on by the emerging IoT. It's going to be more work, but you can manage it by ensuring each wireless sensor is capable of reporting its signal strength and reception rates. Track these values over time and address changes as they occur.

#### SMART DEVICE REPLACEMENT

Replacing smart devices is not the same as replacing traditional non-networked equipment. Every smart device needs to be configured to know who it is and where it is, period. Who in your operation will handle this? Do your technicians know how to replace the devices and get them back online? Can only the product manufacturer do it? What is the cost of this support when out of warranty?

It's not often discussed, but smart device replacement takes a little more forethought and work. You'll need a formal process. Aim for smart devices that allow an end user to replace a device on the go with an app, and you can mitigate time and money spent on this often-underestimated amount of added work.

#### SENSITIVE ELECTRONICS

Computers and electronics are particularly prone to failure from power surges due to their low dielectric strength. If you're in an area with poor power distribution, or at risk of lightning surges, protect sensitive IT and IoT equipment with surge-suppression devices.

This worthy investment will save you from more work in the form of emergency replacements and facility or equipment downtime.

## OFFLINE EQUIPMENT

You were never too concerned before, but now you'll have a keen interest in the quality and consistency of the internet connections at each site. When your smart equipment goes offline, is it because the power is out, the equipment is broken or the IT network is down?

Eliminate the power loss variable by providing uninterruptible power supplies (UPS) for your IT and IoT equipment. The loss of power signal from the UPS should be communicated to your IoT platform so you know when a power loss occurred and can act accordingly.

The IoT platform should also accept a signal from the IT department that informs whether the local network connection is solid or under scheduled maintenance.

Knowing that the loss of communication from a device is not a power loss, and is not the IT network, can save you from more work evaluating false loss-of-communication alarms and what-if scenarios. If it's not the power, and it's not the IT network, it's something else.

## FALSE ALARMS

With today's technology, "smart buildings" and "smart equipment" typically refer to buildings and equipment that can "talk" or, in other words, communicate digitally over the network. If you've ever been on social media, you know there is a big difference between being able to communicate and saying something smart!

The problem (in both cases) is a lack of information and analytic capabilities. Systems that provide the end user with the ability to create alarms oversimplify the complex subject and result in alarms that are either too noisy or miss critical issues.

One common approach to dealing with too many alarms is to mute them or create filters, but then you lose the value of fault detection that you were looking for in the first place.

Annoying emails, texts and web applications are IoT's No. 1 enemy, because they have the potential to create more work than before. If you are receiving a high volume of false alarms, seek help from data scientists who can bring the data into more sophisticated platforms. Take a zero-tolerance approach to false alarms, and you can realize new workflows that add true value to your program.

## Net Work

Often times, smart commercial products tout the ability to predict equipment failures on the equipment they are monitoring or controlling. But the manufacturers rarely discuss what it takes to keep the added complexities of the device itself up and running. Someone has to watch the watchmen, and that's you.

It's time to admit this is a new maintenance category. You must develop a full plan to prevent failures and repairs. Take every step you can to ensure a rigid, reliable system, because small matters add up quickly across the portfolio.

When it comes to data quality and resolution, use one-minute data collection intervals at a minimum. Use wired sensors wherever possible, track the quality of your wireless signals and provide battery backups for smart equipment to keep big data analysis as accurate as possible.

If done correctly, smart buildings will save you net time, as well as fulfill the benefits they promised to begin with: data-based decision making, labor-saving automation, increased facility uptime and improved occupant experience.

Ian Habermann has been designing, programming and implementing enterprise-level building automation systems in restaurants for more than a decade. His current objective at Active Facility Monitoring is to use the latest in artificial intelligence and machine learning to create a facility management system that alarms when it should and, more importantly, doesn't alarm when it shouldn't.