12 IoT Best Practices When Designing an HVAC System

Ayla Networks

Contents

Overview: IoT Success Begins with the Right Mindset

Heating, ventilation and air conditioning (HVAC) manufacturers have spent years, even decades, honing their products' capabilities. But as they ponder the possible benefits of creating connected versions of their products for the Internet of Things (IoT), HVAC companies need to ask themselves an important question: Do we have all the specialized technical expertise needed to cloud connect and successfully scale an IoT HVAC system?

This best practices guide outlines some of the technologies and considerations important for designing, building and ultimately selling IoT connected products. The IoT is complex, and creating a connected HVAC product is not as simple as embedding a wireless chip or adding a sensor. HVAC (sometimes expanded to HVACR with the addition of refrigeration) manufacturers need to consider everything from network security to application software design, as well as how to budget for, scale, distribute and future-proof their products.

As an HVAC manufacturer, you will also need to make sure that as you move to the IoT, you are still able to devote your full time, attention and resources to continue doing what you do best: making and selling great HVAC products. IoT can either be a burden to your core competence, if done wrong, or can be a boost to your competence and brand.

IoT Best Practice #1:
Clearly define your use case

To be sure, IoT provides manufacturers with unprecedented visibility into how their products are performing in the field and how customers are using them. But, before you do anything else, you need to identify clear, compelling use cases for each of your connected products. Customers will not purchase a product because of the benefit you get, but because of the benefit the products bring them. The IoT enables capabilities not possible with traditional, discrete products, so your use cases for connected versions might be very different from what you're accustomed to.

The game-changing factor of the IoT lies in the data generated by connected products. When determining the use cases for your offerings, think about how you might unlock the value of IoT data to differentiate your products, evolve and enhance them over time, improve the experience of buying and using them, and generate new revenue streams.

Infrastructure Issues and How an IoT Platform Can Help

The first thing to realize about IoT products is that connectivity can not be an afterthought, or something simply added at the end of the product design process.

IoT Best Practice #2:
Don't skimp on security

Security is only as good as its weakest link. IoT security must be bullet-proof wherever the data flows, including to and from the connected product itself, the cloud, the mobile or web app used to control the product, and everyone who might have access to the data. Plan for end-to-end security from the very beginning.

But because security is invisible, and because you're always looking for ways to trim the product development budget, it's tempting to see security as a target for cost-cutting, or as something to "add later" when you see where the budget stands. This attitude is a disaster for the IoT, because it means going back and making sure that every link in the IoT chain is secure. As an afterthought, some security links may not exist and whole links may need to be recreated.

Say you spend $1 million to build the first version of your connected air conditioner, but without end-to-end security. It will cost you another $1 million to build that same version of your air conditioner with security, starting over to include security in every link of your connected product. In fact, costs are likely to be even higher, because areas not made secure originally may not have the ability to be hardened. Additionally, starting over can significantly increase your time to scale.

You do not want to be "that company" in the headlines for allowing a high-profile compromise to your IoT products or the data they generate. Resist the temptation to skimp on security.

IoT Best Practice #3:
Know how you will achieve enterprise scalability for your IoT products

What is enterprise scalability? It might mean producing 2,000 connected water heaters a month, or 100,000 thermostats a month, or being able to turn on millions of HVAC products in a short period of time. Like security, scalability at this level has to be planned from the outset of your product design process.

While many IaaS offerings support massive scale, you are responsible for managing that scaling process or risk paying very high stepped pricing models. Furthermore, certain database types do very well for initial product launch but need to be migrated or used in conjunction with other types when massive amounts of data start being created.

IoT Best Practice #4:
Design for end-to-end configurability

Like security and scalability, configurability is something that needs to be baked into every aspect of your connected product, from the beginning. Configurability is complicated, but it's an essential aspect of the IoT.

The biggest value of the IoT is extracting the data generated by your connected products, so you can learn about real-world performance and how actual customers use the products. IoT data represents a powerful way to gain knowledge and insight that has never before been available. You can use this insight to learn from what you've already done, to build better products, add new value-added services and establish new and stronger relationships with your customers.

Taking advantage of this learning to improve products in the field requires understanding how you will address configurability and product change, and having the tools to do so.

IoT Best Practice #5:
Use open standards-based IoT solutions

In addition to product-to-cloud connectivity, your connected products or product lines will need to reach global customers and support cloud-to-cloud connectivity with various IoT platform, manufacturer and retailer clouds. Your connected products will also need to integrate with related products and services from other providers. The best way to do that is through the use of open native libraries and other standards-based solutions.

For example, if you make a connected wall heater, you might want to integrate its use not only with other HVAC products, such as thermostats and air conditioners, but also with lighting systems, smart door locks, and other building automation or smart home products. You might also want to integrate with energy management, weather or other environmental monitoring services.

Choose a cloud architecture that is schema-less and agnostic to any particular data types. That way, for instance, smart home HVAC products can not only interoperate with existing clouds and connectivity approaches—such as Apple HomeKit, Nest Weave, Google Home, Amazon Echo, Wink Connected Home and others—but also with whatever new clouds and connectivity approaches emerge in the future.

Consider Control and Usability Factors

All IoT products will require some kind of control, whether that means frequent input from an end user via a mobile app or occasional servicing or adjustment by technical service professionals using a web application.

IoT Best Practice #6:
Think about remote control from the beginning

Manufacturers beginning their first IoT development process often make the mistake of assuming that mobile or remote control is simply an add-on feature. But as with everything else in the IoT, remote control needs to be woven into the architecture of a connected product from the outset.

If you're making a connected thermostat that will be controlled using a smartphone, will your mobile app support both iOS and Android? Whether you use a mobile app or web application for remote control, will it be able to control or manipulate multiple stand-alone HVAC systems all at once? Could the mobile app you're designing for your connected thermostat also control connected products such as ceiling fans or water heaters? What are the safety measures requiring special attention for local operation versus remote? This last item can also be part of an application level security implementation for safety critical products – eg. what is the maximum setting allowed by remote control?

The flip side of remote control is the local control needed if the Internet goes out or a product's battery dies. You need to devise a way to store local behavior and update it even in the absence of mains power or an Internet connection.

IoT Best Practice #7:
Make your connected product easy to install and use

This one sounds obvious, but the complexity of the IoT—and the increasing expectations of end users—presents ease-of-use challenges to manufacturers of connected products.

For example, who will be installing and setting up your connected product, and what information will they need to know? How will you provide that installation information? Will setup be done using a display on the product, a mobile app or a web application—or some combination? What kinds of PIN or password or other identification will be needed for installation? Will networking setup happen at the same time as the product installation or as a separate process? How will end users register their products?

Testing is critical here, with the different combinations you intend to support. For example, iOS devices can automatically change networks to strongest available and impact your connecting process if that is used in your process. Often, thermostats are placed on the opposite side of the wall from a furnace, and the large amounts of metal in a furnace and ducting can interfere with wireless connectivity. Proper testing can enable you to provide sufficient instructions to the end user for dealing with different connection behaviors.

IoT Best Practice #8:
Design for secure over-the-air (OTA) system updates

One of the biggest differences between a connected product and its traditional counterpart is that the connected product can continue to change and improve even after it's installed.

Through over-the-air (OTA) updates, you can update the firmware on your connected boiler or refrigerator, or add features to your connected thermostat based on analyzing real-world customer usage of that thermostat. Of course, you'll need to make sure that your OTA systems provide state-of-the-art security—and that the security itself can be updated via OTA communication as needed.

IoT Best Practice #9:
Include role-based access control (RBAC) and other advanced controls

Role-based access control (RBAC) is a method of granting either temporary or permanent access to a particular product by individuals based on their "role" or relationship to the product.

For example, service technicians could be granted access to a heating system during the four hours of a scheduled maintenance visit. Adults, children and guests in a household could all be given different degrees of ability to control the home's heating and cooling systems.

Owners of apartment buildings, office complexes or hotels could provide various levels of HVAC system access based on whether the individual is a facility manager, corporate energy manager, employee, building contractor, tenant or guest. Similarly, owners of vacation

properties could provide vacationers with temporary access to a unit's heating and air conditioning controls, as well as to its door locks, lighting and other connected features.

In addition to RBAC, other advanced controls to design into your connected HVAC products include custom scheduling, triggers and alerts, and notifications—to the end user/owner, dealers or other service professionals, and to you as the manufacturer.

Plan for Premium and Value-Added Services

Designing a connected HVAC product means rethinking the fundamentals of what a "product" really is, as well as the shifting boundaries between a product and a service.

IoT Best Practice #10:
Start thinking "service" rather than "product" for your connected offerings

When people say that the IoT changes everything, they're saying something important and true. To succeed in the connected world of the IoT, HVAC manufacturers need to shift their mindset to capitalize on all the new opportunities possible with the IoT.

Here are some things you can do or provide with an IoT connected version of your HVAC offerings that your traditional products could not achieve:

- Rules engines allow your products to be programmed to operate by evaluating various rules rather than following set procedures, which makes them more responsive to the needs of the humans using them.
- You can establish geo-fences—virtual barriers or boundaries for a real-world geographic area. Using global positioning system (GPS), radio frequency identification (RFID) or mobile beacon data, geo-fences can be predefined, such as a zone of control by a connected thermostat. They can also be generated dynamically, such as defining a physical area in which a particular air conditioner can be controlled by smartphones.

- Digital dashboards on web or mobile apps let you visualize data for activities such as diagnostics, predictive analytics and energy usage. Using these dashboards, you can offer fast or preventive maintenance, troubleshoot and solve problems without sending a service technician, and easily monitor—or allow end users to monitor—how much energy or water they are using.
- If you manufacture products that fall under Energy Star or similar programs, you can demonstrate compliance, or tune your connected product so that it achieves compliance.
- Extend the capabilities of your IoT connected offerings beyond what traditional products could achieve by integrating with third-party services such as energy demand response, weather feeds, pollen counts or air quality reports. Using data from these third-party services, you can design your connected IoT offerings to automatically adjust their operations to optimize performance, energy usage or other parameters.

For example, connected air conditioners could combine data from motion and proximity sensors with data from an integrated energy demand response system to reduce cooling force during peak energy times when it's known less people will be in the building. Multiple air conditioners can also be controlled in a manner that allows less peak energy use. Similarly, other connected environment products, such as humidifiers, fans, and air purifiers, could be controlled automatically based on an energy management system program.

Product Hardware Still Matters

While most discussions of IoT connectivity focus on software issues, you still need to pay attention to your products' hardware.

IoT Best Practice #11:
Stick with proven hardware solutions

It doesn't pay to get too creative with your hardware options. Electrical connectivity or networking protocols are not the place to express your differentiation or corporate personality or to take unnecessary risks.

For instance, if you're deciding which Wi-Fi chip to use in your connected product, go with a known, proven entity rather than shopping for a low-priced alternative. Choosing the same type of Wi-Fi chip used by leading smartphones will ensure that your wireless connectivity will have a full networking stack and be able to deliver the performance and security you need, especially at scale.

That $3 Wi-Fi chip from a no-name provider in China might be fine for simple connectivity in a prototype or proof-of-concept (POC) project, but it won't have a full networking stack or top-notch security. Using such a hardware option for production HVAC products could cripple your efforts as customers try to use products lacking sufficient wireless range, performance, compatibility or—most serious of all—security.

Proven hardware solutions will also mean your end customer won't have to deal with configuring or handling connectivity, networking stacks or security. After all, what does the typical air conditioning user know about AES-256?

Conclusion: Buying vs. Building is Probably Your Best Bet

Turning your successful discrete HVAC products into successful connected offerings means making dozens of small and large technical decisions and applying a broad range of technology expertise. Only a handful of the very largest manufacturers are likely to make the decision to fund and create the IoT expertise departments with the experience needed to create great connected products.

IoT Best Practice #12:
Work with a leading IoT platform

You could actually skip the first 11 best practices outlined here by starting with this final one. That's because the right IoT platform will include and take care of all the considerations in those other best practices, and more. When choices arise, a leading platform vendor can advise you based on actual field experience on best choices for your usage criteria.

Ultimately, the question you need to ask yourself as an HVAC manufacturer is this: Do you want to master all the skills, technical expertise and nuances demanded by the IoT, or do you want to focus on harnessing the value of the IoT to extend your leadership to have the best possible connected heating systems, air conditioners, humidifiers, thermostats and other HVAC offerings?

Instead of learning all the IoT best practices yourselves, use the ones listed here as a starting list for evaluating an IoT platform. You'll not only save your sanity but you'll also get to market faster and more affordably with a better connected offering.

For more information about IoT platform technology, visit the Ayla Networks website.

Request a Demo
of Ayla IoT Platform