Making sense of smart sensor technology

What to consider when choosing sensors to integrate with your application

Pressac

Technology that makes buildings talk

Breathe life into your software with smart sensor technology

What if a building could talk to your software? If you always knew what was happening inside a building? If you knew how rooms and resources were being used, how equipment was functioning, or what the conditions were? What if you knew all this in real time?

Integrating smart sensor technology into your software enables you to accurately collect data, detect changes and control an environment and assets, automatically and in real-time.

However, it's important to choose the right hardware to deliver the best end-to-end solution.

Using our **60+ years' industry experience**, we've written this guide to set out the key considerations to help you find the best way forward.

The Internet of Things (IoT) is fast gathering traction, as organisations are realising the benefits of smart sensors to help them organise their operations. In fact, it's estimated that by the end of 2021 up to 50 billion objects worldwide will be connected to the internet and 50% of these will be for some type of industrial application[1].

Source: 1 (quote from EEWorld's IoT Design & Development digital e-book Sept 2019)

Wired or wireless?

There's such a strong argument for installing sensors and automating building controls that many organisations we talk to are already convinced it's the way forward. But what people do want to know is whether they should opt for a wired or a wireless system.

We've taken the main factors you should consider when choosing smart sensors and run through the advantages and disadvantages of wired and wireless sensor systems.

Installation

Wireless systems may be your only viable option where hard wiring is difficult or impractical, such as retrofitting into existing buildings, or where there are construction limitations such as glass meeting rooms.

Installing a wireless sensor system doesn't need any drilling, wiring or structural building changes. This means you'll have lower installation costs, minimal disruption and a system that's up and running much sooner.

But while system installation is often just a case of clicking or sticking the sensors into place, you do need to make sure the system is resilient and offers maximum coverage – which you can do with careful placement planning.

Maintenance

In wired systems, the devices will need to be mains powered. Wireless systems are powered using either battery or self-powering technology. If you have a smaller building, battery power might be fine, but a large building could prove impractical. Batteries need to be changed, stocked and stored ready for use, then safely disposed of. Ultra-low power sensors are increasingly desirable, reducing the need for regular battery changing and are more environmentally friendly.

Self-powered wireless devices harvest the energy they need to function properly. Tiny changes in movement, pressure, light, temperature or vibration are all that's needed to power each device, making them virtually maintenance-free. However, these won't work in all locations. For example, some will only work in direct sunlight, so it's crucial to check this before making your decision. Those seeking a low-energy, low-maintenance solution should consider a battery-free, wireless system.

Cost

There are two strands to consider here: the cost of the components and installation and ongoing maintenance costs. Initial costs can be slightly higher for a wireless system, but any future modifications will be much cheaper.

Flexibility

One of the biggest benefits of a wireless network is that it's easy to add to or modify. If you're planning to expand your network in the future or you need some degree of flexibility, a wireless system is far more accommodating. One important thing to remember is that not all wireless frequencies work across all regions of the world, so you need the right systems for your locations.

Scalability

New sensors and receivers can be easily added to an existing network. Wireless technology also makes it easy to take advantage of upgrades and new technologies as they become available, so buildings become more efficient and save more energy over time.

While wired and wireless sensors can co-exist without interference problems, you will need specialist advice if you want to add wireless sensors to a network of existing wired sensors.

Which wireless protocol is best?

Before you implement a wireless smart sensor system, you'll need to establish which wireless standard – also known as a protocol – best meets your needs. All have slightly different features and capabilities.

Wireless protocols are the technologies used to get information from sensor to receiver. Different protocols have different ranges, data requirements, security and power demands. Some – such as Bluetooth, EnOcean, Wi-Fi and ZigBee – are particularly suited to IoT networks, as they can support a number of low-power devices spread around a home or building.

How much data do you need to transmit?

Both Wi-Fi and Bluetooth standards offer this capability. While Wi-Fi can use a lot of energy in the process, Bluetooth is fast becoming a prime contender as an energy-efficient protocol with iterations such as Bluetooth Low Energy (BLE).

Most smart sensor systems only require short-term wireless transmission of small amounts of information. Here, low-powered solutions - such as EnOcean, LoRaWAN or ZigBee - are usually the most suitable.

How many devices will be transmitting data at the same time?

Too many devices using the same frequency band in the same vicinity can crowd radio signals, leading to interference. In turn, this can cause delays in data transmission and even data losses. Some frequency bands are more widely used than others, so systems using certain protocols are more prone to interference.

The 2.4 Gigahertz (GHz) band is a good example. This is used for wirelessly networking computers, printers and other IT equipment and is licence-free all over the world, making it a popular choice. Bluetooth and Wi-Fi both use this, as do the majority of ZigBee devices.

For some installations, the best protocols may fall into the sub-1 GHz band. This means the protocol transmits data using radio waves with a frequency of less than one GHz. The laws of physics mean that sub-1 GHz radio waves will penetrate further, reflecting less in a building than 2.4 GHz signals.

This is particularly useful for IoT devices as it's less crowded. The 868 MHz band, one of the bands used by EnOcean and Z-Wave, falls into this category and generally provides more reliable signal transmission as a result.

How will sensors be powered?

Energy consumption is big factor in your decision-making. If sensors are battery powered, make sure you know the expected life of the batteries. As well as monitoring sensors for battery condition, you'll also need to change them, dispose of them safely and make sure you've always got replacements in stock.

An alternative is to use a protocol designed for use with extremely low-power, battery-free sensors such as EnOcean.

The EnOcean protocol only requires about 0.12 µWs to securely transmit one bit of information over a distance of 300 metres in free space. A conventional wireless radio, powered by an electrodynamic generator, would need 100 times the actuating force of an EnOcean switch, and a conventional wireless sensor in a living room would need a solar cell 100 times the size.

Do you need interoperability and scalability?

The key consideration here is compatibility. As there are so many device manufacturers, you need the wireless protocol you select to work with any existing equipment, as well as any you're intending to use in the future.

Open protocols enable multiple devices from different manufacturers to talk to each other, offering you more flexibility in designing your smart building systems and making it easier to adopt across a wide variety of IoT devices and platforms.

Closed protocols mean you have to buy all components from one specific manufacturer in order for them to speak to each other.

Plus, not all wireless protocols are global, which can reduce flexibility. So, this is a crucial point to consider for business growth. If you have a global customer base, your sensor system needs to work across different regions, or have the facility to be added to further regions quickly and easily.

Wireless protocols are the technologies used to get information from sensor to receiver. Different protocols have different ranges, data requirements, security and power demands. Some – such as Bluetooth, EnOcean, Wi-Fi and ZigBee – are particularly suited to IoT networks, as they can support a number of low-power devices spread around a home or building.

How do you need the data?

The real-time data transmitted by smart sensors is known as ‘telemetry data’ – basically, numbers and letters which need converting into a language you can integrate with and send to the cloud or your local network. The factors below can help you understand which smart sensors will integrate best with your software.

What format do you need the data in?

Think of sensor data as a language which needs translating. You need the right interpreter to fully understand it. You can use a gateway to collect and convert the data into a usable format, such as JSON. If your system uses a language that’s incompatible with your software, then an IoT platform - like IBM Watson, Microsoft Azure or Amazon AWS - can act as a go-between and translate it into a more compatible language.

As telemetry data is often extremely high-volume, you also need to consider whether you need to index, store or organise it before sending to your application. Do you want to receive real-time data, time series data or summarised data? You may be using your data in different ways – some will be immediately processed, some analysed in depth and others stored for future analysis. Again, using an IoT platform can bring added value here, such as applying a wide range of managed analytics capabilities to your data.

How do you need to access the sensor data?

If you’re accessing data locally you can use a gateway connected to your local network. Remote monitoring needs data sending to the cloud-based broker or IoT platform to route the messages to the right locations.

An IoT platform will also store and manage large volumes of data from thousands of different devices, simply and effectively.

What messaging protocol will you be using?

Messaging protocols refer to communications between devices and the cloud.

There are a number of messaging protocols available and it makes sense to pick one of the more widely used ones. This ensures interoperability, making it easier to expand or scale-up your systems in the future. MQTT and HTTP are probably the most widely used in the IoT world.

MQTT	HTTP
MQTT is one of the most popular protocols for the Internet of Things (IoT) systems and for mobile web apps.	HTTP is the most popular and widely used protocol.
Data centric. This publish-subscribe protocol is perfect for resource-constrained devices, providing clients with independent existence from one another to enhance the reliability.	**Document centric.** A request-response protocol for client-server computing.
Energy efficient. These messages can be as small as 2mb and are capped at a maximum size of 256mb, meaning they use less data and energy, conserving battery life.	**Good for sending large data packages.** This uses larger bandwidth than MQTT, so can be slower, but is better for transmitting larger amounts of data.
Fast. If real-time data is a must, you need a protocol that gets information to where it's needed as quickly as possible. According to measurements in 3G networks, throughput of MQTT is 93 times faster than HTTP's.	**Worldwide infrastructure.** HTTP has been around longer than MQTT, so you can take advantage of a huge, tried-and-tested, global infrastructure.
High delivery. There are three levels of quality of services: - at most once: a best effort delivery. - at least once: a message will be delivered at least once, but can also be delivered more than once. - exactly once: each message is received only once by the counterpart. You also have options of 'last will and testament' and 'retained' messages. The former means that in case of an unexpected disconnection of a client, all subscribed clients will get a message from a broker. The latter means that a newly subscribed client will get an immediate status update.	

Choosing the best sensor hardware

Which smart sensor hardware is right for your business? The nature and scale of your project will determine the importance you need to place on each factor, but here's a good guide to drive your final decision.

Compliance and quality

Quality is key when installing systems on a national or international scale. If things don't work properly the impacts could be far-reaching, costing far more than the savings made from buying something cheaper initially. There are also issues around credibility and reputation. For example, if desk occupancy sensors don't work properly and people constantly find themselves turning up to meetings in double-booked rooms, they'll simply stop using the systems.

The best way to have confidence in the quality of the product is to look for an international standard like ISO. Companies with ISO 9001 accreditation have strict quality management processes in place to ensure they are producing goods to a high standard, while ISO 14001 means they are taking their environmental responsibilities seriously.

It goes without saying that you want your smart sensor solution to be safe. Look for fire retardant plastics and internationally recognised safety standards. Local standards may not be enough, as what's deemed safe in one country may not be up to standard in another.

For example, European fire regulations are generally much stricter than those in the UK. Make sure the solution you're implementing will meet standards across all the regions you intend to use it.

Scalability and adaptability

Solutions need to be future proof so it's important to choose a system that can adapt quickly to meet new demand and volumes, and which can be added to easily. You also need to check that additional equipment can be purchased quickly and easily. It's also a good idea to check whether new functionalities can be added without disrupting the existing system.

Security and data protection

IoT systems constantly collect, exchange and process vast amounts of data, and it's vital that any system you implement uses the highest-possible security standards.

The most common method of protecting your data is encryption, which means the data is safe from the point it is produced and throughout transmission to its eventual destination. The standard encryption level for most smart sensor products is 128-bit – considered to be the 'gold standard' because it is logically unbreakable. Even software which continually generates random sequences of bits would take an estimated 100 billion years to crack a 128-bit code. Reassuringly, there are no known cases of anyone cracking a 128-bit encryption.

You may also hear some technologies refer to 'stream ciphers' - these use a continuous stream of ever-changing signals to keep information safe.

Always ask potential hardware providers how they meet the highest security requirements.

Interoperability and compatibility

If you are a large company with different divisions around the world, you need a solution that can work across the regions, with component parts seamlessly speaking to each other.

Consider the business as a whole, rather than allowing different divisions to implement their own systems. This can become costly down the line if purchasing decisions are not aligned. It's also important to consider business growth and future regions you might extend to.

Be aware, not all solutions will talk to one another, as some require all components to be made by the same manufacturer. Look for systems that are manufacturer agnostic and use the most common protocols, such as MQTT (outlined earlier in this guide) to ensure they can interact with existing or future systems. Some technology is also built ready to connect easily to cloud platforms you may already be using, like Microsoft Azure and IBM Watson.

Cost

Of course, you need hardware that fits your budget. But bear in mind, the cheapest isn't always the most economical, and a cheaper system may end up costing you more if it needs regular maintenance or is unreliable.

Cheaper parts also often use an unsophisticated calibration routine that needs more time spent on costly testing and environmental chambers.

Get the balance right between cost-effective and high-performance sensors. Don't forget to factor in testing and calibration costs, especially for high-volume applications.

How to choose the right partner

When you've decided the type of sensor solution you want to provide and the technical specification, the next step is to choose the right hardware partner.

There are a number of key questions to ask to make sure you're getting the highest-quality, best-value-for-money project. In the previous section we mentioned quality and safety, so make sure you check ISO credentials and safety compliance.

What is the company's experience like?

Taking some time to research a company's history and reputation can pay dividends. Many IoT companies are relatively new and will be in the early phases of business development. Choosing an established and experienced sensor hardware company, with a good track record of delivering products, can help to future-proof your systems and means it's less likely that the company will disappear within a few years.

It's also a good idea to research the types of projects they've worked on and look for testimonials from previous customers. Are they trustworthy and reliable? Do they provide good customer service and a positive experience? Reputable companies should be happy to provide these for you.

How quickly can products be designed and manufactured?

Ideally, you need your time-to-market to be as short as possible, getting products completely ready in a short time frame. Choosing a reputable manufacturer who is experienced at quickly producing high-volume products can minimise lead-time, whilst still retaining the quality of the product.

Depending on your needs or a customer's specifications, you may require customised sensor types or functionality. Therefore, it's worth finding out whether a company has the expertise and capabilities to manage the full production process, from design and prototyping to manufacture and distribution.

What testing do they carry out?

Look for a company with a proven track record of rigorous testing, not just of their own products but of the combined software and hardware at the earliest possible stage. Do they have the right equipment for an effective test environment? The more complex the system, the more robustly it needs to be tested before the operational phase.

What pricing models do they offer?

Different pricing models can save you money, so explore what's on offer. For example, you could be entitled to a discount if you adopt a reseller model or a financial rebate for partnering with a sensor hardware company.

What added value do they bring?

Industry experience can offer huge added value. A long-standing sensor hardware manufacturer can bring insights and expertise that will really enhance your offering. For example, making sure the system is as resilient and offers as much coverage as possible, by carefully planning the placement of sensors and receivers.

For smooth and seamless implementation, ask what testing, training, implementation support and experience a company offers.

Look for companies who offer the potential to test 'proof of concept' and then scale up quickly if successful.

Making smart technology work for you

The importance of the practical and logistical considerations will vary by project and business. For some, cost will be the overriding priority, while for others ease of maintenance or scalability will be the deciding factors.

It's clear that taking time to ask the questions we've outlined in this guide is essential, helping you to not only find the right product, but avoid costly mistakes and false starts.

Successful end-to-end solutions need a highly proficient, experienced smart sensor hardware vendor that understands the complexities of the IoT environment, provides a choice of high-performance sensors and proposes just the right solution for your application.

Bringing their in-depth understanding of the complexities of IoT, they can design innovative and effective products for you to take to market. As the march of smart technology continues apace, you'll be placing yourself in good hands to keep your company competitive… and connected.

Pressac smart building and connected technology

Pressac design and manufacture the technology that makes buildings talk. We help millions of businesses and consumers worldwide to connect their buildings and equipment to the network, enabling them to talk to applications, to each other, and to you. All in real time.

As a trusted partner to some of the world's leading companies, we've been designing and manufacturing smart technology for over 60 years. As well as off-the-shelf solutions, we also offer bespoke manufacturing in high volumes. With in-house design, development and quality-assurance experts, plus our own high-tech UK manufacturing facility, we can manage the full lifecycle of product creation, from design and prototyping to manufacture and distribution.

We partner with our customers to help deliver scalable, cost-effective, compliant solutions that offer the very best performance, flexibility and reliability.

Over 60 years' experience and technical expertise

Compliance with UK health and safety regulations

Quality and environmental management assured

5,000 sqm high-tech UK manufacturing facility

Find out more

If you're looking for a partner who understands technology – and can offer reliable, cost-effective solutions in high volumes – get in touch.

Call us: +44 (0)115 936 5200 Email us: Info@pressac.com Visit us: www.pressac.com

Pressac