GENESYS

ELECTRONICS DESIGN

What you need to know **BEFORE**

Developing Smart Products

From a product designer who has done it many times before

GENESYS
ELECTRONICS DESIGN

What We Do

- Product design
- Electronics engineering
- Software development
- Regulatory compliance support
- Manufacturing management

About Genesys

Genesys Electronics Design developed this whitepaper to assist people and organisations in developing smart devices with electronic and software components.

Genesys is an electronics design house specialising in complex devices for mission-critical and highly-regulated environments. It has ISO 13485 medical quality certification, and it applies this rigorous quality process to all of its projects.

Genesys works closely with industrial designers and manufacturers – to provide an end-to-end product development service.

Genesys also provides consulting services on how to gain regulatory approval for products that require ISO 13485 or other such standards.

More information is available on our website at:
www.genesysdesign.com.au

GENESYS
ELECTRONICS DESIGN

bsi. ISO 13485:2016 Medical Device Quality Management

DISCLAIMER:

The information presented in this document is intended to provide general guidance on product development from the perspective of electronics, software and firmware development. Genesys recommends that anyone developing a device requiring regulatory compliance should seek formal advice from a recognised regulatory compliance expert, in order to determine the particular compliance obligations applicable to their product.

No one person or company can be expert in everything required to successfully commercialise smart products.

The key to success is to be an informed buyer of services that complement your core capabilities.

TABLE OF CONTENTS

Innovating your products and services

If you are a typical business producing products for the industrial, commercial or consumer markets, you are certain to be on a journey toward making your products "smarter". You have to do this because you know that competitors somewhere in the world certainly are. You want to do the disrupting, not be disrupted.

You have probably also heard of the Internet of Things (IoT) and realise this technology trend is the basis of a new generation of disruptive smart products. However, you realise your company can't be expert in all the fields the IoT covers. The technology is rapidly changing, with new connectivity options and IoT platforms emerging every day. You need help.

There are many consultants and IoT platform vendors out there that say they can do everything you need. Who are the best people with whom to work? How can you be confident of getting value for money? What is the smartest path forward to ensure you don't waste your precious resources?

This white paper provides an overview of the process for developing smart devices and provides some advice from two different perspectives:

- **Business considerations:** In the first part of the paper, we discuss the broader business requirements for successful IoT product development.
- **Technical considerations:** We then discuss an approach to planning and implementing the technology.

The audience of this white paper is Australian companies looking to develop IoT-based products compliant with ACMA regulations. However, the principles apply equally to FCC regulations in the US and in Europe under the CE Mark.

CASE STUDY
Creating Safer Construction Sites

Company X provides physical safety products to a particular segment of the construction industry, where they dominate their niche.

The company approached Genesys to develop a "smart product" that would complement its physical products and help differentiate its services from the competition.

As we move through this whitepaper, we will revisit the Company X case study to understand how it resolved the challenges outlined below.

Business considerations

The Internet of Things (IoT) is a classically disruptive technology trend, changing not only how businesses operate practically but driving changes to the actual business models of companies themselves. Companies that currently sell conventional products are being challenged by start-ups which, at one extreme, offer similar products for free in return for long term service contracts, enabled by the IoT.

Many companies are examining their existing product ranges and determining how they can be made "smart" and connected – supporting new organisational strategies.

However, the IoT is a daunting landscape. It is a term that connects many technologies encompassing sensing, electronics, communication, the cloud, data analytics, user interfaces, and a multitude of IT architectural layers. Interoperability and security challenges add another level of complexity.

Many vendors and consultants working in these fields claim to be doing IoT. However, the reality is that most consultants only play a small part in a bigger picture. Only you, the company or manager looking to innovate your product line, can understand what the IoT is in your context.

This section is designed to provide advice to managers on what they need to consider in developing a strategy to leverage IoT technologies. Introductory information on what the IoT is all about is on our IoT web page at **www.genesysdesign.com.au**

Company X is already established in the construction industry, with a range of safety products protecting workers from inadvertent injury and restricting access to dangerous areas. The company understands the market well and knows what its customers want.

The company's CEO recognised an opportunity to develop "smart" products that could detect unsafe activity and alert management.

Strategic analysis revealed that adding vision, motion and proximity sensors to their devices would enable them to provide a value added service, delivering superior safety and security features to their products.

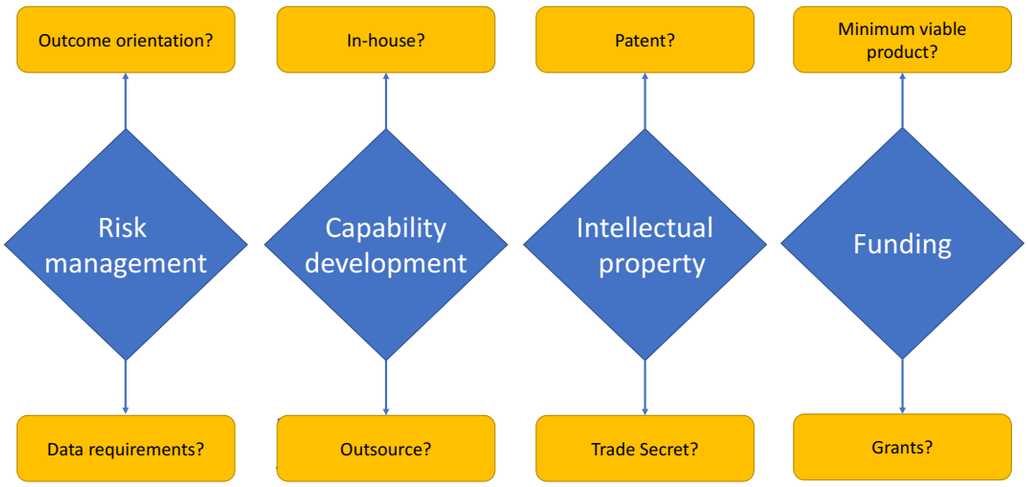
An examination of commercially available devices quickly established there was nothing meeting their particular needs.

An IoT business decision framework

Consider the following decisions in developing your IoT strategy, including:

- How to manage the commercial risks of a technically complex project
- Whether to build your IoT capability in-house or not
- Whether to protect your inventions through patents or pursue a path of trade secrecy
- How to fund your innovation

Illustrated below, we discuss each of these decision points in the sections which follow.



De-risk your project

C-suite executives have one thing in common when managing smart product development projects – management of risk and opportunity. CFOs look to manage the financial risk, CMOs manage the risk of building a device the market doesn't need, CTO's want to minimise the likelihood of technical failure, and so on. The CEO has to balance all these concerns to manage strategic risk and opportunity for the organisation. Below are four key points that help de-risk your project.

Focus on outcomes not features

When considering how to leverage IoT in your smart product design, it is easy to focus on the technology, and what new features (bells and whistles) to offer clients. However, this only changes the customer value incrementally. The real power of IoT comes from its ability to change business models and the entire value proposition for customers.

From a business perspective, consider the following questions:

- How will this disrupt your industry?
- What disruptive challenges do you face from competitors, and how can you maintain your edge?

The initial business requirements for Company X's product was for a device operating off small, low-cost batteries for up to a year, with detection of tampering or incorrect installation, communication of alerts, ability to turn some devices off during work hours, and regular health checks to ensure all devices are operational.

All data needed to be communicated wirelessly to a virtual cloud server and then to a mobile app.

- How can the measurement of data, and the value hidden in it, change the kinds of services you offer?
- Look beyond the immediate utility of your product to its role in the entire value/supply chain of your customers. How can your smart product interact with other participants?
- Do you need to own the underlying technology IP to secure the outcome? Can you buy off-the-shelf or configurable white label products and compete in other ways?

Our advice is to resist the temptation to get carried away with the technical possibilities, focus on core business outcomes and work backwards to business requirements.

In the initial discussion with Genesys, Company X's business requirements included a vision system. However, examining the technical complexity of including vision, it was quickly realised that the business case for this feature did not stack up.

Conversely, it was identified that measuring sound levels would help with the dectection of unsafe events and could be easily added.

The decision was made to include proximity, audio and Passive Infrared (PIR) sensors only.

Follow the data trail

A common mistake is to put sensors on anything that can be measured and then try to figure out how to derive value from the data. While there is an argument that machine learning and big data analytics may uncover hidden insights, the reality is that most of this data never gets used. Also, there is an erroneous perception that it is cheap to store and transport data. However, this is not true if the data volume starts to build up through large scale deployment of devices.

Our experience is that commercially successful projects work the other way around. Work out what data you need for what purpose, then work backward to what sensors you need, where the data must flow, and how to present it.

Working backwards from the user needs, Company X identified that users just wanted to be sure each sensor was working correctly and that, when an alarm is triggered, the user could easily visualise which alarm has been triggered overlayed on a map of the construction site, so they can act on it quickly.

> ***Work backward from purpose to what data you need***

If in doubt, the data can be stored locally on the device in high capacity SD cards, and accessed by exception when events require detailed investigation. Storing and pre-processing most of the data using edge computing on the device, and only transmitting essential information, also reduces communication costs and opens up a wider variety of communication options. You can then determine an architecture and IoT design supporting optimal data management.

Chart the most cost-effective path

In what has become a mantra for start-ups the world over, experts recommend that the first take-to-market offering should be the "minimum viable product" (MVP). The aim is to get to market quickly with low development cost and to use this minimally featured device to understand better your core customers and what they want, gaining rapid feedback in the development of your next version of the product.

This strategy is a two-edged sword. While it reduces the risk of product/market misalignment, it can also raise the risk of cost blow-outs in the overall product development cycle.

A better approach is to map out your likely product roadmap and make allowance in your initial design for likely future features. This approach minimises the redesign costs in each iteration of your product, dramatically reducing costs over the life the product.

> ***Minimum viable product is a two-edged sword***

When authorising the scope of the initial product, C-suite executives need to determine the sweet spot between the MVP costs and whole-of-life product development costs.

A key requirement was communicating the alarm data wirelessly and cost effectively. It was identified a Low Power Wide Area Network (LPWAN) technology would be appropriate. However, there were many competing and rapidly evolving technologies in this space.

The decision was made to include the LPWAN communication features on a plugin board, so that it could be easily

Apply due diligence

There are three broad categories of risk in any smart product. The first category relates to safety arising from the electrical powering of devices. Strict adherence to the standards governing the use of such devices will mostly address the risks. The second category relates to compliance with a raft of regulations relating to radio telecommunications. Even if your device is not connected wirelessly, it may be radiating electromagnetic noise which can interfere with other devices. Many devices have been developed ready for the market only to fail regulatory tests at the last minute. The cost of remedial design changes late in a project can be cripplingly expensive. So the regulatory aspects of device design need to be carefully considered.

Perhaps, the most significant risk is cost blowout from scope creep and design rework following technical failure. There is also the ever-present spectre of product recalls.

The construction industry is characterised by large sites and using traditional wide area communication methods would necessitate transmissions at a level beyond the legal limit.

The decision was made to move to TI15.4 which allowed frequency hopping to share the RF power over a number of different channels.

To complicate matters, the legal minimum number of channels varies by country. This was addressed by making the number of used channels a configurable parameter.

Ultimately, C-suite executives are responsible for identifying all possible risks through the application of due diligence and managing them both commercially and technically.

Executives don't need to understand the underlying technology of the projects they are overseeing. However, they do need to ensure they have a risk management plan in place and that the development team are thinking through all possible scenarios.

Building your IoT capability

As a manager, you will need to consider if you want to directly employ people with the expertise to build your IoT capability, outsource it on a turnkey basis to a product developer, or take a hybrid approach.

It's important to understand that it is generally impracticable for any one individual or product-focused company to be expert in every discipline required to develop smart products successfully. Even large multi-nationals employ specialist subcontractors for critical tasks. Therefore, to build an IoT capability, understand how to align IoT competencies with your core business competencies

and then determine the unique capabilities you want to develop in-house and what you can outsource.

The key criteria for this decision boil down to whether your unique value proposition relates more to customer service or technical innovation. For example, if your strategy is around understanding your customer better than anyone else, acting on the data you collect faster or building a better brand, then it may not matter if competitors have a similar or even better technology. In this case, you can outsource the product development, comfortable with the fact that your supplier's skill sets will be available to all your competitors. Reputable product developers will not service a direct competitor of their client and will happily sign an exclusivity clause. However, the supplier themselves will have competitors and rarely have unique skill sets. Your challenge then is to find a supplier you can trust.

Your key selection criteria for suppliers include:

- **Quality systems:** Does the supplier have a quality management system in place? Ask how they guarantee the performance of their deliverables.
- **Breadth of skill:** Does the supplier have engineers with expertise across all of the disciplines your project will require? Does it have reliable partners to fill their skill gaps? Refer to the technical considerations below.
- **Experience:** Has the supplier done similar projects to yours before? Avoid paying the supplier to learn about technology at your expense.
- **Scope creep:** How does your supplier deal with scope creep? Determine their effectiveness in anticipating future requirements and developing a road map, so there are no cost surprises.

When Company X first considered develop smart products it hired an electronics engineer to manage the project.

The company quickly realised the range of skills required for embedded electronics, firmware development, cloud systems, mobile aps and more was well beyond any individual engineer. The company's core capability was in marketing safety and security products and it did not want to develop a whole electronics and software team in-house.

After reviewing what was critical to their core capability, the company chose to employ just one addition inhouse resource – an expert in usability who would closely liaise with customers to understand what information they needed and develop new mobile interfaces for different use cases as the product evolved.

The company then looked around for a technology partner to outsource all other electronic and software development functions. Genesys was engaged with an agreement to not only develop the initial products but to maintain them over time.

If your product strategy is strongly reliant on technical innovation, then you will want to determine how many technical skills you need to have in-house. You need to know enough to know what you don't know.

For medium-sized companies, you should aim to have enough technology-aware staff in-house so that you can be an informed buyer. They should be able to talk the language of your suppliers, ask the right challenging questions and be able to recognise the level of the technical difficulty of each aspect of the project. They will be able to keep your supplier honest.

An alternative for very small companies is to engage a self-employed consulting engineer to provide independent advice and to project manage the technical aspects of the project. An independent advisor is particularly suitable for companies that only want to use the product, and are not interested in on-selling the device or owning the intellectual property. A key role of the independent advisor is to develop a rigorous set of business requirements. Good business requirements will smooth the technical development of the product, and reduce development costs and time to market.

Larger companies may want to capture more of the value of the innovation by building an in-house technical team, bearing in mind that it's generally impractical to have absolutely everything in-house. You will usually want to align the team mostly to the core intellectual property you aim to develop and own.

For example, if the core value of your product is in the software, then the bulk of your team should be software engineers. A key consideration in building the team is how to manage the quality of their work. Who will review requirements, designs, code, and conduct verification processes to ensure the product is delivering on the promise? An independent advisor could fulfil this role.

Note that many IT departments in companies don't have the skill sets required for the IoT and it may be best to have your product development team report to another function in the business most aligned with your value proposition.

Intellectual property

Having built your team, you will want to consider how best to protect your investment from competitors seeking to replicate your idea. For some ideas, there is a patentable core technology arising from fundamental research that provides a degree of commercial protection. However, it is also possible to generate IP through identifying unique and novel aspects in the technical specifications and implementation of the device itself. In choosing your designer, you need to consider their ability to generate IP for you.

Most companies develop an intellectual property strategy to protect their investment. There are a few critical points you should know upfront about IP.

Your invention must not be in the public domain already if you want to patent it. So don't talk about or publish any technical details of your idea in any public medium. You must also secure your patent before you start using the device commercially, even if done in secret.

Another key consideration is to ensure that any member of your technical team understands that the rights to any inventive work they do flow to you or your company. Under common law, this happens anyway for work done by employees, but its good to clarify it in any contracts, so there is no dispute. Its also common practice to get everyone involved in a project to sign a non-disclosure agreement.

A second key point about intellectual property is the concept of freedom to operate. It's not enough to have a patent protecting your idea. You have to be sure you are not infringing on someone else's patent.

> ***Carefully scrutinise the allocation of IP rights***

The IoT is the new wild west in intellectual property, and many people around the world are filing patents daily. However, computer-based technology patents are notoriously hard to obtain and many granted patents are later found to be invalid.

For many people, it makes more sense to develop their technology in secret, as the processing of a patent allows competitors to see the nub of your invention even before you know whether your patent application will be successful. Publishing a patent can open the door for them to use your idea, or find workarounds and different ways of achieving the same outcome.

However, from a business perspective, patents provide a lot of leverage in business negotiations. Many smaller businesses will seek a variety of business partners from financial investors to global distribution partners. Many of these companies will not spend a lot of time or money working with you unless there is an assurance that competitors will not walk in and take market share after they have gone to all the effort of establishing the market.

Secondly, many government grants have an unwritten condition of having a patent in place.
A final point to make about intellectual property is to carefully scrutinise the allocation of intellectual property rights when outsourcing product development to external contractors.

Most developers leverage previous designs and code when developing new products. As such they own the copyright or intellectual property inherent in that pre-existing work. Usually, they grant their clients a licence of some sort to use their intellectual property.

For some companies, owning the intellectual property is not important. In this case, explore opportunities for reducing the upfront costs of development in return for a longer-term licencing deal.

If owning intellectual property is important, then this needs to be made clear in upfront negotiations. Good suppliers can even assist you in gaining patents by developing new technology for you.

The most immediate requirement in Company X's IP strategy was to submit a Design Registration, which relates to the visual appearance of the device.

The casing was designed to be conspicuous and striking, adding to the perception of smarter and safer environment. The external look of the device is an important part of the company's brand strategy.

A patent was also submitted relating to the detection of unsafe activity, including the management of event triggers, from the sensor through to the user.

Funding your innovation

Companies need to be realistic about how much it will cost to fund an IoT innovation. Much of the excitement around IoT is that the cost of IoT devices has reached a tipping point of affordability that is enabling applications that were previously prohibitively expensive.The unit cost of devices can be as little as a few dollars, excluding batteries.

However, the upfront development costs are substantial to properly engineer a device, particularly in highly regulated environments like transportation, mining, health or aerospace. You can amortise these costs over the life of the product, which again makes it affordable in mass production.

A big trap for novices is the idea that a proof of concept developed on an Arduino board or Rasberry Pi means that the product is nearly ready to go. However, these are primarily hobbyist tools, and they are not immediately transferable to a production design ready for scalable commercial production.

Commercial prototypes involve the design of custom, multilayered circuit boards that can be produced cost-effectively at volume. Custom housing is often required as well as the design of any mechanical components, requiring industrial designers. All electrically powered products are subject to regulations, and many are subject to compliance checks before being allowed on the market.

There is much more involved, beyond the scope of this whitepaper. It is tempting to take short cuts on these elements. Don't. Ultimately, these elements underpin the viability of your product as a failure of any one of these elements will stop your market launch in its tracks.

> ***A proof of concept in Arduino is not ready for scalable commercial production***

When working with either in-house staff or contract product developers, most companies employ a phased approach to both quotation and development. Initial phases involve a modest upfront investment and include discovery and translation of business requirements into a technical product specification. Unknowns are researched, and the output is a document that sets out the agreed scope of the project – which you sign off. It also usually includes a quotation for the subsequent phases.

It is critically important that you, as an informed customer, engage heavily in this phase to get the detail right. The biggest risk is leaving out some important feature that will cost a lot to build in

later. The result can be scope creep and dramatically higher costs than you expected. Even if you don't include all the features in the first version of the product, plan for them in your roadmap. The bulk of the cost is in the development phase. This phase is where the design takes place, and the outputs are generated. If the first phase is executed correctly, the managerial input to this phase is minimal.

The final phases of a project relate to manufacturing management, which includes working with manufacturers to refine the component supplier selection, board assembly process and testing tools.

Funding sources

The good news for innovators is that there are many opportunities for obtaining government support through grants and other financial incentives. In Australia, funding is available federally or via the state/territory, usually on a 50/50 basis. The Jobs for NSW Funding Roadmap [https://www.jobsfornsw.com.au/__data/assets/pdf_file/0018/141327/Funding-roadmap.pdf] exemplifies what is typically on offer.

During the start-up or research phase, there are several incentives for pre-revenue businesses to connect with technical experts, develop marketing plans, create a minimum viable product, conduct underlying R&D and build partnerships. All these incentives lead toward gaining an Accelerating Commercialisation grant, which is usually the major step forward in realising the product. Post-launch, there are loans, guarantees and export assistance for emerging and scaling business.

The smaller grants are generally non-competitive, which means you only have to fulfil the criteria. Larger grants are usually competitive, so they need a significant investment in time and effort to get the applications right. There are dozens of potential grants to consider.

Company X is majority owned by a private family, with investments in a number of companies providing services and products to the construction industry. This investor demanded the risk in this new venture be carefully managed.

In order to manage the development risks, the company's management agreed milestone strategy was formulated.

As each milestone was reached, the project was reassessed in light of the learnings. The next milestone would then be revised and funds released.

An entire industry has evolved around obtaining grants. Some companies will manage the entire grant application process for you, in return for a success fee which is usually a percentage of the grant obtained. Note, you still have to supply the raw data. However, this option can be good for time-poor executives that don't want to tie up internal staff on this activity.

For start-ups, there is also a range of incubators and accelerator programs available. These will provide basic office facilities, maker-spaces, mentoring and a networking ecosystem and sometimes seed funding, in return for an equity stake in your business.

For an existing business that cannot afford to fund the project internally, there is a range of venture capitalists who can provide funding.

Returning to our opening statement on funding, product developers need to be realistic about funding and understand that commercial development of robust products involves a lot more beyond the proof of concept phase. However, financial concerns are all mitigated by a robust business plan and risk mitigation strategy. If you are confident about your product's success in the market, then it is worth the investment to do the engineering right.

Technical considerations

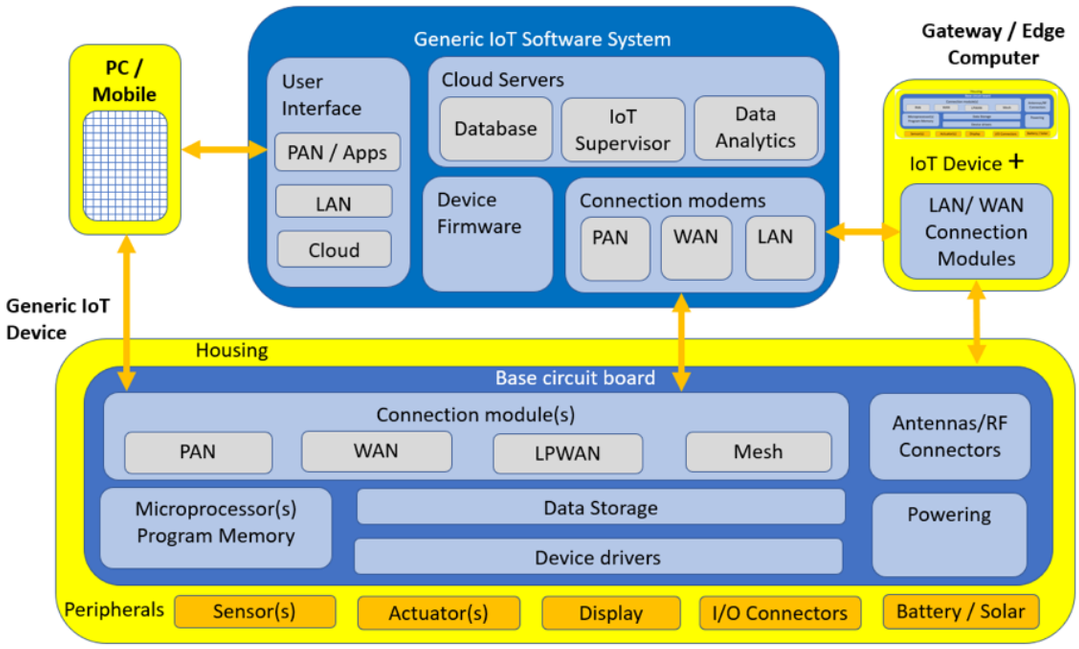
In this section, we discuss some of the key fields of IoT technology. There is a vast amount of technical information online and in other parts of our website. Our aim in this paper is to highlight options and common issues.

The main areas are:

- **Architecture**
- **Powering**
- **Sensors**
- **Communications**
- **Data management**
- **The user interface**

Architecture

In developing a smart product, the system architecture is quite generic to all devices, as outlined in the diagram below. A smart product is usually a system consisting of a device in the field connect to the internet, often including an interface via a smart device and a gateway device that aggregates data from many sensing devices.



The exact configuration of the system will vary depending on the specific application and context. However, most IoT systems will include many of the elements within each of the above blocks.

For example, a generic IoT device will usually include a sensor, some local processing capacity, connection modules to get the data out, antennas and a battery, or some other powering arrangement. Often there is a direct connection to the device with a mobile app or browser to facilitate configuration and commissioning.

The same elements appear on a gateway/edge computer, which usually does further processing of the aggregated data from multiple devices to enable local control and to minimise the size of data being uploaded.

The rest of the system usually operates on cloud servers and facilitates data visualisation, analytics and systems management.

While the functional block diagram above seems straightforward, it masks a level of complexity that challenges even the most experienced electronics and software designer. No one person can be expert in all of the fields encompassed by the above diagram.

Powering

Powering arrangements are important because they are the primary driver of practicality, as well as electrical safety considerations which are subject to strict safety regulation. The options include a direct connection to mains power, a broad array of battery types, solar panels and even "energy harvesting" where kinetic movement generates enough energy to run cleverly designed wearable devices.

For all of these options, the gap between a proof-of-concept device and commercially deployable devices is significant. The gap is often poorly understood by electronics designers if they do not have a long history in machine-to-machine communication.

For example, where mains power is readily available, it is a sensible option. However, regulations around any connection to the mains are stringent, and deployment in an industrial environment brings additional challenges. It is important to galvanically isolate your IoT's power supply to avoid problems arising from earth differentials and fault currents. Load dump protection is another challenge for many applications as transient spikes in power supplies can easily fry your device.
In a highly regulated context such as mining and medical environments, mains power also raises stringent safety issues and greatly increases the regulatory compliance burden. However, one technical workaround is the use of contactless inductive coupling for charging batteries, also known as Qi (pronounced chee) charging. Qi charging practically eliminates the risk of exposing users to hazardous voltages and currents.

Genesys included a number of low power features in the product design, all aimed a minimising the energy requirements of the device.
These features included a separate processor for handling motion, audio and proximity detection, so the main processor could be asleep most of the time.

The selection of Low Power Wide Area Networks for communication was another design choice to minimise power.

The result was that the device is powered using four AA battery cells for up to a year of continuous operation.

An additional benefit of using easily available batteries, is that the product can be more easily shipped without batteries, and is easily set up by users.

By far, the most widely used source of power in IoT devices is a battery. Batteries bring with them their own set of challenges which again are poorly understood. There is a widespread assumption that powering devices by a battery is just a case of selecting a convenient one from a catalogue and plugging it into the design. There are even some pretty good tools out their such as Element 14's battery life calculator (https://au.element14.com/calculating-battery-life-in-iot-applications). This approach might work for low-value, low-reliability markets, but for any high-quality device, the design is far from simple.

The source of the issue is that battery specification sheets supplied by manufacturers are notoriously unreliable. For high-performance devices, battery characterisation must be conducted to verify how the device will operate under a range of different temperatures and operating modes.

This characterisation then needs to be matched to an appropriate low-power design that maximises battery life.

The main message for product developers is to understand your designer's approach to battery selection to ensure reliable operation in the field.

Sensors and actuators

The source of innovation in IoT projects is often in the algorithms processing the data. The data is sourced from sensors that are largely stock-standard and available in any electronics supplier's components catalogue.

However, sensors can be a source of innovation if you choose to go down the route of developing a custom sensor, creating data not available to any of your competitors. Creating custom sensors requires a strong grasp of the physics or chemistry underpinning the sensing function, as well as the manufacturing processes involved.

Developing custom sensors is usually the preserve of large corporations but can be available to smaller organisations through university research arms. For example, the NSW Smart Sensing Network exists to do just that, connecting researchers to original equipment manufacturers. For more information, visit https://www.nssn.org.au/.

Be aware that it is also possible to create "virtual sensors" by combining the input from several sensors. The classic example of a virtual sensor is dew point, obtained by combining data from temperature and humidity sensors. For more complex applications, like managing losses from a water network, the inputs may come from thousands of instances of several classes of sensor and involve sophisticated algorithms.

The main message for product developers is don't dismiss the value of investing in smart sensor designs.

The company was concerned about devices being subverted by contractors looking to avoid the safety rules set by site managers.

A light sensor was included to detect masking of the device and an accelerometer was included to detect destructive abuse of the device.

A patentable innovation was the monitoring of sound to detect unusual noises on the site. To minimise false alarms, the system needed differentiate normal construction sounds from sounds potentially indicating safety issues.

An algorithm was developed to operate on the device and only send alerts are required.

Connectivity

Our CEO, Geoff Sizer, loves challenging the robustness of a communications solution by getting our engineers to show how it could be substituted with a carrier pigeon system and still work. This challenge is more than a jest. With the plethora of communication options now available, it is easy to get confused about the best solution. Much of the advice on the internet centres around the latest low-power, wide-area network (LPWAN) options, but this ignores the fact that you can connect devices via Bluetooth, WiFi, Ethernet, and a host of SCADA protocols.

The selection of the right technology boils down to a multi-dimensional trade-off between a range of conflicting requirements.

Key factors to be considered in this trade-off include the cost of communication data throughput, versus the cost of a module, the energy consumption of the technology, required battery life, security, latency, and the geographic area covered, to name a few.

The biggest issues we see are people specifying a particular technology in their business requirements, e.g. the device must have 4G mobile connectivity. However, the main message for product developers is don't jump to conclusions about what technology is required before the tradeoff process has begun. Let the engineers select the right tool for the job.

Company X wanted the device to operate using batteries for long periods, so a low power wide area network (LPWAN) was required.

The Sigfox network was chosen as the initial direct connectivity option, as the technology was being rolled out nationally at the time, the first such LPWAN service in Australia.

However, given the evolving state of the LPWAN market, the Sigfox module was included as a plug-in card.

When a major telecommunication provider started rolling out the NB-IoT option for LPWAN, Genesys developed an NB-IoT plugin module as an additional option.

Data management

Closely related to the choice of communication technologies are the tradeoffs to be made on how to manage and process the data from your IoT device. The core tradeoff has to do with edge versus cloud processing.

With cloud processing, most or all of the data is transmitted directly to an online repository such as AWS or Microsoft's Azure. IoT system primarily uses the cloud to take advantage of advanced algorithmic capabilities online, such as machine learning. A typical example would be remote monitoring or metering applications.

With edge processing, you do much of the analysis on the device and only transmit the results, often by exception. This approach greatly cuts down on data transmission costs and bandwidth requirements. A typical example would be systems that require real-time decision-making and control, such as airconditioning systems. One option product developers sometimes overlook is to locally log all the data onto a high-capacity SD card. In the event an operator wants to look at the full data set for a critical period or incident, this can be downloaded directly using a physical or Bluetooth connection.

Company X identified an opportunity to extend the capabilities of the device to act as a security sensor during non-working hours.

However, they wanted to avoid the need to set working times.
An algorithm was developed to determine "normal" construction sounds and movement. When normal activities finished the system automatically transitions from safety oriented mode to a security mode where all activities would generate an alarm.

Apart from the alert information, the only other data transmitted is a regular heart-beat signal so that the user or Company X knows if a device has gone offline.

A third option is to insert a mains powered gateway device in between multiple low-power terminal units that connect locally, often via a mesh network.

It isn't always clear what the best approach is, and the tradeoffs relate to a lot of other factors, like how conveniently power is available at the location, geographical location, and so forth.
Tied up with all of this is the approach to modelling the data of the IoT system architecture to facilitate smooth data flows. Modelling is particularly important for interoperability between sub-systems and when multiple developers and users of the data are involved.

Good data modelling supports modularity at all levels of an IoT system, including the data packets, the firmware and software coding and even the embedded electronics hardware. But what makes a good IoT data model? A good model it is one that supports the business logic of your product, the scalability of the device over its life, interoperability with other systems and between sub-systems, reuse and reliability of code, and allocation of responsibilities between development team members, to name a few.

In other words, data modelling is complicated and requires a firm hand to avoid the undocumented spaghetti code typically involved in hacked solutions.

A big temptation of product developers today is to choose one of the many IoT "platforms" out there, from an Arduino board through to a complete ecosystem from one of the global players such as Cisco, IBM and Amazon. If you can find a solution that exactly meets your needs, then these can be a good option. The issue is that all of these platforms come with compromises associated with cost, flexibility, longevity and support levels.

Again, the main advice for product developers is don't jump to conclusions about the best approach to how to develop a platform that is right for you. Allow the engineers to develop the design of a system that best meets your needs.

The user interface

The user interface is another area with an array of options. Data from a device can be displayed on an in-built screen, linked to a mobile app or served up via a website. While the user-friendliness of mobile devices makes them attractive for operational and marketing purposes, they are an area fraught with problems.

An industry-wide problem is that many app and web developers are not skilled software engineers, and are not familiar with integrating a real-world device into their system. Typical problems can include connections dropping out, scalability of the system architecture to incorporate hardware changes, the security of the connection and basic stability of the application, and apps that simply do not work.

Robust systems will have compartmentalised communication at the systems level. At the end of the day it's about having a systems engineering methodology to deliver reliability to the final product.

Working with Company X's usability expert, Genesys develop a web browser and mobile app for interfacing with the system.

The app had two main functions. The first function was to commission a device and configure it for the system. This was facilitated by a Bluetooth connection direct to the device.

The second function was management of alarms, including a visual representation of all the devices overlaid on a map of the construction site. Colours were used to indicate the operational status of each device and those which had an alarm.

Alerts were sent by multiple pathways to ensure they were acted on.

Find out more

Genesys Design periodically posts thought leadership blog posts and runs educational webinars on IoT and medical device product design.

To learn more and stay in touch, sign up to our newsletter at www.genesysdesign.com.au

If you have any specific questions, please call us on +61 (02) 9496 8900.

QUALITY - CERTIFIED

bsi. ISO 13485:2016 Medical Device Quality Management

30 YEARS

GENESYS
ELECTRONICS DESIGN

Genesys Electronics Design

Unit 5, 33 Ryde Road
Pymble NSW 2073 Australia
enquiries@genesysdesign.com.au

CALL US ON +61 2 9496 8900