

Smart home technology is intended to solve a variety of issues and make our lives easier but while we have been promised various versions of the smart home going back decades, the necessary technology and the supporting structures have never really been readily available, until today.

Clumsy initial attempts with smart home technology failed to ignite the market as they were relatively expensive, and installation was difficult, often involving disruptive rewiring.

The situation has changed as the prices of smart devices, like sensors and controllers, have fallen and as suitable wireless technologies have emerged. These developments have helped to transform the prospects of the sector with a growing range of easily integrated, multi-purpose but simple, solution-based devices.

When it comes to connectivity, Bluetooth mesh networking is being widely adopted in smart home solutions. At the Consumer Electronics Show (CES) earlier this year, the Bluetooth Special Interest Group (SIG) established a new Smart Home Subgroup in response to the growing number of OEMs looking to adopt Bluetooth mesh networking as the communications protocol for their smart home solutions.

The Subgroup is looking to create additional Bluetooth mesh model specifications for the smart home and related applications and define the behaviour of devices that are connected to a Bluetooth mesh network.

"Mesh models will be able to define how a Bluetooth mesh light is controlled by a Bluetooth mesh switch," explained Martin Wooley, Developer Relations Manager, EMEA, Bluetooth SIG, "and like all Bluetooth technology specifications, the mesh models that are developed will then be available to all member companies

CLOSING THE GAP

Smart home technology has been promising much, for so long, but helped by new wireless standards and the use of voice technology is it now beginning to deliver? By **Neil Tyler**



for use in conjunction with the Bluetooth mesh networking specifications."

The aim of which is to provide, "multi-vendor interoperability in the smart home," said Wooley.

These mesh models are seen as playing an important role in strengthening the connectivity and interoperability in smart home devices and over 60 companies have already joined the Subgroup.

"For the smart home market to develop, it needs true global wireless mesh networking standards that can meet the reliability, security, and performance needs of the market," said Dian Fan, General Manager of Xiaomi IoT Platform, one of the

companies that have joined the Subgroup. "Bluetooth mesh is one of those standards and will enable tremendous growth and innovation in home automation."

"The release of Bluetooth mesh networking and the recent formation of the Smart Home Subgroup are important milestones in the development of the smart home market," explained Mark Powell, Bluetooth SIG Executive Director. "With mesh networking support, Bluetooth is in a position to help the home automation market reach mass scale."

So how is the smart home evolving and what are the key applications and technologies that are driving it?

Key drivers are home disaster management, home security and deeper integration, all of which are helping to drive the market but possibly the most potent driving force has been the advent of voice control, which has helped to transform the market over the past two years - voice-controlled AI-powered speakers have taken the industry by storm.

"If any confirmation were needed at the impact of voice, Amazon's keynote at IFA 2018 fired out a few key stats - there are now more than 20,000 compatible Alexa devices - up from 12,000 in May and 4,000 at the end of 2017. Alexa now has over 50,000 skills, and there were 50 new Alexa devices announced at IFA 2018 alone," recalled Martin Keenan, the Technical Director at Avnet Abacus.

According to Keenan, however, the importance of AI and voice to the future of the smart home is not just about those impressive numbers, significant though they are, but it is due to the ability of voice control to bridge the technological gap, removing the need for users to grapple with the details of each device and solution in order to access their benefits. This applies to everything from navigating TV EPGs to controlling disparate in-home devices.

Voice is now perceived as the essential channel of the future, and the current levels of manufacturer integration tend to support that assumption.

Security drivers

The global smart home security market has been estimated at \$670m and is expected to reach \$2.7billion by the end of 2025, that represents growth of almost 20 per cent, year-on-year, making it among the more successful niches for the smart home.

According to Keenan, a major factor in the success of this sector has been in overcoming the upfront hardware costs and installation fees.

“The highly modular structure of today’s smart home security systems allows them to be expanded with new sensors, lights and cameras incrementally, rather than in the single, costly financial hit required by the traditional security industry system install model,” Keenan suggested.

And it is true to say that there has been a rapidly improving array of sensors available to manufacturers, from incredibly sensitive pressure sensors through to ultrasonic and various types of light sensors, all of which have become significantly smaller, easier to integrate and most importantly, much cheaper, over the last few years.

The Eyes Outdoor Camera from Bosch, for example, is able to stream 1080p HD video straight to a smartphone or tablet and has integrated sensors so that clips are

not filled with swaying tress or pets inadvertently walking past, instead it only records the events that are significant.

Another trend has been in home disaster management, which is closely associated with home security and which covers a wide range of potential incidents, from the security-related, through to moisture detectors such as Notion and GROHE Sense in key locations.

“Interesting examples include integrated pressure sensors in boiler systems and also in bathroom fixtures. The latter delivers two benefits - the flow control (to remotely run a bath), and perhaps more importantly, the ability to alert the user if low or high thresholds are breached. Sudden loss of water pressure could indicate a serious leak, while a sudden increase could indicate a local issue such as a blockage, or a more serious failure,” Keenan explained.

In the early days of the smart home market single-use devices were common, now smaller sensors and multi-purpose chipsets mean that more complex and capable devices are now available.

Samsung’s Family Hub fridge, for example, is not only fully integrated with Samsung’s SmartThings IoT ecosystem, but also provides a touchscreen control interface and AI voice control thanks to Bixby.

Smart home technology is also being sold as having a critical role to play in helping to reduce waste, so smart heating systems are being encouraged by national regulators and utility companies as they demonstrate clear efficiency benefits, while consumer devices, like washing machines, are specifically designed for not only convenience, but to exploit

“For the smart home market to develop, it needs true global wireless mesh networking standards that can meet the reliability, security and performance needs of the market.”

Dian Fan

Below: Voice control has bridged the technological gap enabling users to more easily access the benefits of devices and solutions



cheaper energy tariffs and which minimise water usage.

The increasing proliferation of smart devices in our homes, however, raises concerns over security and researchers are regularly uncovering fundamental vulnerabilities in many off-the-shelf products.

Reports have revealed that devices are insecure and can be compromised in a matter of minutes whether that’s a baby monitor, home security cameras, doorbells or thermostats – one of the simplest methods of hacking was found to be tracking down the default factory-set passwords.

According to Stuart Spice of B9 Systems, which has developed a threat intelligence platform to monitor and identify possible attacks, “The use of encryption and polymorphism and the large scale and systematic distribution of attacks at a commercial level, means that most anti-virus software is redundant as it continually fails to identify and prevent attacks.”

B9 has developed a Wi Fi router that sits outside an existing router and allows the user to monitor applications and websites showing them where an internet connection is communicating in real-time – highlighting possible suspect virus or malware attacks.

As we reported in New Electronics last month, surveys are finding that consumers are increasingly concerned by reports of data breaches and hacker attacks and companies need to do more to inform and educate consumers on how to stay safe.

But despite concerns over security, the smart home market is continuing to mature fast and, as such, we can expect the technology in our homes to continue to improve and evolve incredibly rapidly.