

# Internet of Everything – What is it and how will it affect you?

---

## Paul Gerrard Principal, Gerrard Consulting

There is an increasing amount of publicity, information and hype around the subject of the Internet of Things (IoT) and the Internet of Everything (IoE). What on earth are people talking about? Should I be interested? Will it affect me? What does it mean to me as a human being? What does it mean to me as a *tester*?

In this article series I want to explore what the IoT and IoE are and what we need to start thinking about. I'll approach this from the point of view of a society that embraces the technology. Then I will look more closely at the risks we face and finally how we as the IT community in general and the testing community in particular should respond.

In the first article of the series I will look at what IoE is and how it affects us all. It's important you get a perspective for what the IoE so you get a sense of the scale, the variety, the ubiquity, complexity and challenge of the technological wave that many people believe will dominate our industry for the next ten to twenty years.

Let me start the whole series off with what sounds a bit like science fiction, but will soon be science fact. John Smith and his family are an invention.

## The Human Perspective

John Smith's family live in a quiet suburb. He is married to Alice, has two children, works as an engineer for the local authority, and is a keen road bike rider. The family recently moved into their new house and are still coming to terms with the technologies that have been designed into it. It seems that every day, some new feature of the ubiquitous, embedded technologies emerges. All of these features are described in great detail in the user manual – but who has the time to read the manuals for a house?

At 6.00am, the alarm rings on John's side of the bed. The vibration and sound was chosen because John is sensitive to it, but his wife isn't. John gets up, grabs his phone and moves quietly to go cycling. The house has already turned the central heating on in the rooms that need heating and as he moves around the house, lights come on automatically. The security alarm turns itself off. As he leaves rooms, a sensor detects this and lights are dimmed and turned off after a pre-set delay. In the bathroom, he uses the toilet, weighs himself, brushes his teeth and washes. Like all the other electronic devices in the house, the toilet, weighing scales and toothbrush are all connected to a central hub installed in the house. Who knows what data they collect?

He gets a drink and an energy bar from the fridge. The fridge beeps - the energy bars are running out – and it logs the removed items and updates the shopping list. John touches the screen on the fridge to confirm he is eating more than 6 per week to adjust the re-order level. The door to the garage unlocks as he approaches it. He

puts the drink and energy bar in his rucksack, grabs his bike and pushes the bike out of the garage. The garage locks behind him, the lights fade, he pushes off and he's on the road.

His phone connects with the power sensor and odometer on the bike and the heart monitor he wears on the elastic belt around his chest. The phone logs the energy he uses, the distance travelled and his heart rate throughout the journey. In the meantime, his GPS position is tracked and saved to the phone. John is on a short route today as he needs to get to work early. His phone vibrates and alerts him – the weather later on is going to be wet – but he knows he'll be all done before the rain comes.

It is early, still dark, and the street lights are off, but automatically switch on just before he reaches them. The roads are still quiet and so, the street lights turn off again after he leaves them behind. At halfway around his route, he stops, eats the energy bar and take a drink. He logs the food and drink on his phone. John's route is circular and after a few more kilometres, he climbs the long, steep hill on the circuit. His bike reminds him not to exceed 165 heartbeats per minute and he settles into a steady rhythm. Today is meant to be an aerobic session. He speeds down the other side of the hill.

John returns home and as the garage door opens automatically, his phone uploads the statistics of the ride to a website that tracks all of John's exercise. As he puts the bike away, the phone reminds him that the rear tyre of the bike is 1000 kilometres old and might need to be replaced soon.

John goes to the bathroom to have a shower. His wife, woken by her own alarm – the radio – is just getting up. The kids are still asleep but they'll be waking up soon. A message from the school to the home hub warns Alice that they won't need their swimming kit today – the pool is closed for maintenance for 48 hours.

John dresses quickly and is ready to go to work. He says hello and hugs the kids as they sit and have breakfast. Alice will drive the kids to school a bit later. John kisses Alice, says "see you later" and walks out of the door to his car. The car unlocks as he approaches and he gets in after the seat automatically adjusts (as Alice drove it last night). He drives off. His journey lasts twenty minutes but on a bad day, it can take half an hour. The car, of course, knows the destination.

The car is in communication with the local traffic management network and the 'crowdsourced' cars on the network identify their location every few seconds. The network knows where the bottlenecks are and of course, so do the cars. John's car give an audible warning to take the ring road, rather than the direct route today.

His car is aware, through networking and radar, of the location of other cars on the road and the path of the road itself. The car gives warnings of hazards on the road, even around blind corners and issues 'do not pass' messages when it would be dangerous to overtake.

The car offers to read out his messages – IMs, texts and Twitter, as he drives. It knows already which messages are relevant to him at this time in the morning. One reminds him of his meeting with a client at 10am at the coffee shop in the atrium of his office building.

As John approaches the barrier to the car park of his office, the barrier automatically rises to let him through. His office operates a hot-parking space regime, so the car knows where to find the space nearest to the office entrance that will get him to his allocated hot-desk quickly. The car directs him to a space, and for a change, John parks the car himself rather than let the car do it automatically.

As he leaves the car, it locks and disables itself, although an authorised valet service that operates in the car park can open his car, with a code, to clean it – although they cannot start the car or its services.

John enters the secure building but doesn't need to swipe a card or show a pass. He grabs a coffee from a machine (which charges his account automatically) and walks to his desk. The surrounding lighting changes imperceptibly as he sits down and arranges his papers. The movement sensor in the office space also adjusts the air-conditioning and humidity in his area so he has a perfectly comfortable working environment. All these facilities are controlled by the local building management system which is constantly monitored by the landlord's central systems.

John has interacted with hundreds of sensors, computers and devices and it is only 8.30 am in the morning. Time to do another day's work.

## **The Technical Challenge**

In recent years, there has been much progress in developing connectivity between Internet-connected 'smart' devices for intelligent monitoring, remote sensing and control using advanced analytics and real-time processing. To date this has mostly been based upon IP and Internet-based communications but the pace of development means that soon, existing communications and networking technologies will be inappropriate, and probably inadequate, to handle the traffic generated by an Internet of Everything.

We are all familiar with the office- or home-based computer that connects to the internet through a wired or wireless connection. In recent years, the mobile phone and tablet technologies have extended the use of the Internet to people on the move. It is natural to assume that machine to machine (M2M) and wireless sensor networked (WSN) implementations are simply extensions of the Internet. But there are significant challenges to be overcome to make this a reality.

Firstly, many of the 'things' to be connected will be low-powered devices which need to successfully function for months or even years without attention or a re-charge. Secondly, these devices transmit relatively low volumes of data, but do so over lossy and noisy networks. The existing Internet protocol is not an ideal solution.

Currently, the web relies primarily on IPv4 addresses the HTTP and TCP/IP protocols. The IoT will be delivered with a variety of evolving standard protocols with unfamiliar names and acronyms like 802.15.4e, 6LoWPAN, RPL and CoAP. These emerging standards aim to integrate wireless networks of low power devices to the broader Internet.

## **IoE Standards are Required**

Needless to say, the IoE will significantly increase the number of devices connected to the internet by a factor of anything from ten to perhaps one hundred times. It is clear that the Internet needs the more efficient, emerging protocols to deliver the promise of IoE. These protocols are still evolving and are competing for attention and adoption somewhat, but the hope and expectation is that the standards will be refined and mature in the next couple of years.

The challenge for the developers of the new Internet will be, 'which architecture, which standards to adopt?' The low-power devices and WSNs are proliferating but these local systems cannot match the performance of standard Internet hardware at scale. The Internet architecture is familiar and provides a choice of protocols such as HTTP, SMTP and is scalable but does not work so well with low-power devices in lossy networks.

So, the race is on to develop standards that can interconnect low power devices using different proprietary protocols with a seamless integration to the Internet. For the time being, most IoT deployments will be hybrid arrangements using bridging, gateways and middleware between the Internet and specialised, proprietary networks of low-power.

## IoE Standards are Emerging

The huge increase in device numbers is driving the adoption of the IPv6 standard, which effectively allows for an infinite number of connected devices. The 6LoWPAN protocol enables IPv6 packets to be carried on Low Power, Lossy Networks (LLNs). A protocol for interconnecting such networks is also under development.

At the physical layer, the IEEE 802.15.4e standard will define the mechanism that allows for more resilient use of lossy networks (through channel hopping). At the application layer, the emerging protocol (that parallels HTTP) is a REST-based Web transfer protocol called Constrained Application Protocol or CoAP. It is similar to HTTP and uses its own URIs to identify resources and has, for example, GET, PUT and POST verbs, but it also has features that accommodate the low-power and energy consumption constraints of IoT devices.

The CoAP protocol implements a different dialog between internet devices (clients) and, for example, sensors. They are called 'observations'. The client sends a message to a sensor registering an interest in the output of the sensor. The sensor then sends data to the client without the need for long-standing connections or expensive polling by the client to the device. The nature of these dialogs is different to more familiar web, email or terminal-based dialogues between clients and servers.

Several other standards initiatives are in progress. Message Queue Telemetry Transport (MQTT) is being promoted by IBM. The ZigBee alliance is focusing on smart-home and smart-device applications. The Dash7 alliance has a different 'tag-to-tag' perspective. BACnet focuses on HVAC (heating, ventilation, and air conditioning), lighting and access control applications.

Now, if you are a non-techy, I must apologise for the headlong dunk into the murky waters of emerging technical standards.

The message I want to share is this: the efforts of the standards bodies makes for a dynamic and confusing state of affairs. It is not clear which standards will win the day. Whatever people are building now, it's unlikely their solutions will match the standards of tomorrow.

## To be continued...

In this article, I have tried to set the scene of the wonderful future world of the Internet of Everything. Right now, it is a very confusing state of affairs, but clearly, an awful lot of effort and money is being invested in defining the standards and building business opportunities from the promise of the new Internet world order.

In the next article, I'll take a look more closely into the emerging risks of the Internet of Everything, from both a social and technical viewpoint.

## Paul Gerrard

Paul Gerrard is a consultant, teacher, author, webmaster, developer, tester, conference speaker, rowing coach and a publisher. He has conducted consulting assignments in all aspects of software testing and quality assurance, specialising in test assurance. He has presented keynote talks and tutorials at testing conferences across Europe, the USA, Australia, South Africa and occasionally won awards for them.

Educated at the universities of Oxford and Imperial College London, in 2010, Paul won the Eurostar European Testing excellence Award and in 2013, won The European Software Testing Awards (TESTA) Lifetime Achievement Award.

In 2002, Paul wrote, with Neil Thompson, "Risk-Based E-Business Testing". In 2009, Paul wrote "The Tester's Pocketbook" and in 2012, with Susan Windsor, Paul co-authored "The Business Story Pocketbook".

He is Principal of Gerrard Consulting Limited and is the host of the UK Test Management Forum and the UK Business Analysis Forum.

Mail: [paul@gerrardconsulting.com](mailto:paul@gerrardconsulting.com)

Twitter: @paul\_gerrard

Web: [gerrardconsulting.com](http://gerrardconsulting.com)