Answers to Questions about the Internet of Things

Answers to Questions Asked at a Webinar Hosted by IEEE Educational Activities, and Given by Dr. Adam Drobot, Chair of the IEEE IoT Activities Board on August 22, 2017

IEEE

Table of Contents

Introduction

Dr. Adam Drobot is a technologist with over forty years of experience in industry, the public sector, and in research. Today his activities include strategic consulting, start-ups, and participation in industry associations and government advisory bodies. He Chairs the IEEE IoT Activities Board that oversees the multi-society IEEE IoT Initiative. He is the Chairman of the Board of OpenTechWorks, Inc. a company specializing in open source software.

Previously he was the Managing Director and CTO of 2M Companies in Dallas, TX, from 2010-2012, and President of the Applied Research and Government Business Units at Telcordia Technologies and the company's CTO from 2002 to 2010. Prior to that, Adam managed the Advanced Technology Group at Science Applications International Corporation (SAIC). He also served as the Senior Vice President for Science and Technology as part of his 27 years of service at SAIC from 1975 to 2002.

Dr. Drobot has been the principal or key participant in the development of several large, scientific code systems and software for managing the design and production of complex platforms. He has published more than 100 journal articles, and is a frequent contributor to industry literature. He currently holds 26 patents.

Dr. Drobot is the 2007 recipient of IEEE's Managerial Excellence Award. He is currently a member of Several Corporate Boards, the FCC Technology Advisory Council, and he also chairs the Awards Recognition Council for the IEEE. Adam is on the Board of the Telecommunications Industry Association where he chairs the TIA Technology Committee.

He holds a BS in Engineering Physics from Cornell University and a PhD. in Plasma Physics from the University of Texas.

Internet of Things Webinar with Dr. Drobot

On August 22, 2017, Dr. Drobot, in coordination with IEEE Educational Activities, offered a webinar titled "IEEE Internet of Things – Conquering Complexity One Step at a Time."

The webinar was moderated by Michael F. Violette. He is a Professional Engineer and is founder and CEO of Washington Laboratories and founder and Director of American Certification Body. He has worked in the industry for thirty years and has authored numerous articles and publications for and about the industry. He has expanded WLL's operation to Asia and co-founded American Certification Body, with operations in the US, EU and Asia, providing certification services to the global market. Mike represents the EMC Society on the IEEE IoT initiative.

The webinar covered these topics:

The Internet of Things, according to the consensus from the analyst community, is growing at a rapid pace that globally exceeds a compounded annual growth rate (CAGR) in revenues of 20% per year. It is also seen as one of the fastest expanding area of activity commercially, for public sector engagement, and for the research community. IoT is still in its early stages and can be characterized as inherently multi-disciplinary and

challengingly complex. In order to fully achieve its promise, IoT is very dependent on collaboration between many organizations to create effective ecosystems and to resolve hard problems in policy and regulations, and there are great expectations on IoT to profoundly affect society. One driving dynamics of IoT is the "deep digitization" of the way we design processes, products and services to deliver new functionality and, at the same time, create value by lowering the economic threshold for participation for industry, governments, and for individuals.

This webinar discussed the goals of the Multi-Society IEEE IoT Initiative and the role it plays in fostering and nurturing the adoption of IoT so that it truly benefits society, and to act as an informed and highly respected technical source of information about IoT.

Key points addressed:
- What IoT is all about and how it relates to other important technical areas
- How IoT is likely to evolve over time
- What are the ingredients that make up IoT offerings, solutions, and applications and which ones appear to be most important?
- Why IoT is attracting so much interest and why there is so much seemingly disjointed activity under the IoT "label"
- Examples of historical precursors to IoT and important application areas where IoT is already making an impact and giving us a glimmer of what can be achieved in the future.

The webinar also included the importance of education programs, standards, and the technological enablers that make IoT possible.

Questions and Answers

The following are questions that were asked during the webinar, for which Dr. Drobot provided answers.

IoT Industry Growth

Is there any forecast regarding what kind of market penetration that IoT will have? (industry IoT, home IoT, government IoT, etc)

The major analysts Gartner, IHS, Informa, IDC, and major consulting houses all publish prognostications of where IoT is likely to thrive.

Has the IoT industry peaked, or are we simply experiencing inflated expectations?

There are two common constructs that are used to view technology in its path to utility - one is the Hype Curve from Gartner and the other is from Goeffrey Moore described in his book "Crossing the Chasm". The characterization of IoT being at the peak comes from the Gartner curves published in 2012-2016. In fact IoT has not followed the usual pattern, and has and continues to see double digit growth without falling into the "valley of despair".

One of the main reasons cited as the key factor in slow market adoption of IoT that is often given is the lack of a killer application. Some of the early apps proposed during the late 90s as part of Berkeley's "Smart dust" project – precursor to many IoT projects – were mainly in the defense industry. What do you see as the main areas where there is potential for mass adoption of IoT?

I would not say so. From surveys, the three top concerns seem to be: (1) complexity; (2) security or privacy concerns; and (3) difficulty in defining a credible business case with a high probability of success - too much assembly required.

What is the current barrier/pinch point for the development and growth of IoT? Is it technological, managerial or political/societal?

It is elements of all of these. Conquering complexity on the technical side and then dealing with sociology and customs on the political end.

Is there any initiation from any organizations (like IEEE) to help people in underdeveloped countries who are not able to get access to IoT and its advantages?

There are quite a few - and IEEE is playing a major role in pushing for projects in IoT that fit the needs of underdeveloped countries, concentrating on both capacity building and implementation programs.

IoT Technology and Development

What are the programming platforms available for IoT development?

The IoT space is awash with "platforms." If you were to search the web for "IoT Platform," you would be overwhelmed. One reason I can think of is that it's a development environment; another is that it's a fairly complete and general software stack that includes many common functions encountered in IoT applications. Still another is that it is a combination of specific hardware (computing, communications, and some storage) that is broadly applicable. If you do a casual search on the web, you will find many examples of the three aspects I have mentioned. To be practical, the choice depends on the vertical in which you are building applications. The Eclipse Foundation did a survey of programming languages used and identified over twenty as "musts" and in common use. No platform deals with that well.

Which programming language offers the best support for IoT applications?

It really requires knowledge of a lot of languages and operating systems, depending on what you are dealing with. The old stalwarts like C, C++, Python, Java, and R, are all important, but so are the markup languages, the newer orchestration languages, and specialized languages for dealing with databases, as well as those common in embedded systems.

What type of algorithms are needed for IoT?

IoT is not about a single algorithm. There are literally thousands of algorithms that are in common use. It all depends on what you want to do. A relatively simple IoT application may end up using dozens of algorithms. A good book to get a feeling is the classic by Knuth titled: The Art of Computer Programming.

Will there be a different IP address allocation strategy for IoT devices?

Theoretically, IPV6 has enough address space to allow IoT devices to be covered by a common construct, providing a path to consistency and inter-operability. That does not mean that each IoT node is on the internet, and some deployments are architected to aggregate IoT nodes using non IP protocols at an internet gateway. There is a very wide range of opinions on how to do this, and is part of the learning curve.

You mentioned APIs and actuators. What are they, and how do they apply to the IoT?

An API is an Application Program Interface. It defines the parameters that are the input and output from an application, the range of those parameters, and the meaning behind them. An application program interface (API) is code that allows two software programs to communicate with each other.

An actuator is the action element in a control cycle. This is best illustrated through some simple examples:

- If you had an irrigation system, and a sensor indicated that it should be turned on, then the switch/valve that operates the sprinkler is the actuator;
- If you have a connected car, and wish to unlock it remotely, then the switch/motor that drives the car lock is the actuator.

You mentioned LTE in your presentation. Can you briefly review what LTE means?

LTE is a cellular telecommunication standard that comes from 3GPP and stands for Long Term Evolution. It is often referred to as the 4G Standard, meaning the 4th Generation of Cellular Systems.

How much data is used by IOT solutions?

There are solutions in the IoT landscape that are not very data intensive: it could be as little as one bit (is something on or off). On the other hand, it could be astronomical: think of a high-resolution camera that is producing a streaming video where you record all the bits, and then think of many such cameras producing data at the same time. Think of a major satellite system such as NASA's EOS (Earth Observing System) that has high-resolution instruments streaming high-resolution data.

How much power will IOT devices consume?

There is no monolithic IoT. A single instance may consume a small fraction of a watt. A single cloud rack in an IoT Data Center might consume 30-60KW. Meanwhile, a large robot or autonomous machine like an agricultural combine may consume more than 100KW. The aggregate in power consumption from 50 billion IoT devices might be considerable! A good exercise is to go through and compare IoT power usage to other sources of consumption.

Security

My question is about security in IoT. How well is security developed in IoT? Especially the low power devices? Are there any security architectures and algorithms developed? And what are the difficulties in implementing security in IoT?

Security is recognized as a challenge. Regulatory bodies are mandating that security or privacy must be built in from the scratch - but that's hardly realistic. My own view is that we are on a learning curve and security is one of the items we have to conquer - that does not mean it will impede deployment, but it will impact design and applications especially for critical functions.

Are there any compliance/best practice frameworks you would recommend regarding IT security?

In the EU there are a number of guides that were developed as part of the 7th Framework Initiative. In the US, the National Institute of Standards and Technology (NIST) recently published a "Security Framework" and a fairly specific document dealing with security for Cyber-Physical Systems.

Are IoT connectivity providers giving complete solutions for security and end-to-end reliable links?

They are trying - the difficulty is that transit and transport are just a small portion of an IoT solution and there are many aspects of security that are not under the operator's control. One example is who has access and authorization to IoT systems is usually determined by the end user and not the provider.

In IoT solutions, security is still an afterthought, and not up to the scale of IT security. How prepared is industry to manage cyber attacks where IoT can be a key actor? Currently the focus is more on business solutions and security comes as topping on top of a solution which can be a major threat once we have large IoT solutions running across the globe.

The bigger outfits are well prepared for dealing with security and have the advantage of resources and skill. When you look at where IoT is being deployed, a lot is happening in industry. Two examples that surprised me were the level of adoption in agriculture and in manufacturing.

Data Privacy Regulations
With the vast array of data generated by IoT technologies, how will this be impacted by the General Data Protection Regulations (GDPR)?

This will have quite an impact because it will dictate where the infrastructure is located, as well as who has access to it. The ability to do things from anywhere at any time will be restricted. It is an example where non-technical issues have real consequences.

IOT Use Cases
What uses and benefits can IoT have for the financial services industry?

I suspect that IoT will change the nature of financial services profoundly. You can think of an ATM machine as an early precursor. Over time, many aspects of financial services, from payment systems to the use of blockchain ledgers, will be mainstream.

IoT seems like a natural fit with Artificial Intelligence (AI), with IoT feeding AI from various sources. Have you given much thought to the possibilities and dangers of these two things together?

AI can play a major role in IoT. Good examples include autonomous cars (a branch of the IoT space), the machinery health system on a jet engine, or the data collected about a patient to diagnose the underlying condition.

Can IoT control the home?

You might control some functions in a home. It might be heating and cooling, maintenance for appliances, security, looking after the garden, etc.

IoT Job Market

Which part of IoT will create the most jobs? Is it the developing part or hardware maintenance?

If you have a good background and are adept at systems thinking, you will get your pick of what's available. IoT is not a bad area to grow your career.

How can I start working on IoT from home?

Pick a vertical or enabling technology area and stick to it. Take small steps first, and after you are proficient, expand your involvement. In order to begin developing your skills in this area, start with a small project using one of the popular kits from Raspberry or Arduino.

IoT Standards

How much does standardization play a role in IoT, and how can we take into consideration the needs of developing nations like India?

Standardization is very important for adoption, for scale, and consequently for cost structure. Some of the standards bodies don't pay enough attention to the needs of developing nations, so it is crucial to have venues where technology can be localized to take into account practice, customs, markets, and economics at the right level.

Is there an IEEE standard in development for IoT?

The IEEE Standards Association is pursuing a considerable number of standards in IoT, starting with P2413 which deals with IoT Architectures. In addition, individual societies like IEEE Communications Society, IEEE

Computer Society, the IEEE Vehicular Technology Society, IEEE Electromagnetic Compatibility Society, and the IEEE Sensors Council have initiatives in IoT Standards.

Additional IEEE IoT Resources

IEEE provides a number of resources to help you learn about the Internet of Things, and incorporate this technology. The following resources are available from IEEE.

IEEE Guide to the Internet of Things

IEEE offers an 8-course online learning program called **IEEE Guide to the Internet of Things**. This mobile-friendly online learning program covers topics such as:

- What the Internet of Things is, along with its applications, challenges, and future opportunities,
- How the Healthcare industry is applying Internet of Things concepts, to help you consider ways this technology may affect your industry, and
- Real-life applications of the Social Internet of Things, while exploring the underlying architecture needed to support these applications.

Courses may be purchased by individuals directly through IEEE Xplore. IEEE Member discounts are available: http://bit.ly/IOTcourses.

To learn more about purchasing this course program for your organization, visit http://bit.ly/IEEEIoTCourse.

IEEE IoT Initiative Website

The mission of the IEEE IoT Initiative is to serve as the gathering place for the global technical community working on the Internet of Things; to provide the platform where professionals learn, share knowledge, and collaborate on this sweeping convergence of technologies, markets, applications, and the Internet, and together change the world.

https://iot.ieee.org/