NETEVENTS

APAC PRESS & SERVICE PROVIDER VIP SUMMIT

FINAL

Round Table Session I
Testing Times in the Internet of Things

Chaired by: Nikhil Batra

Research Manager - Telecommunications
IDC

Panellists:	
Neil Holmquist	Senior Director, Product Marketing/Management - Cloud & IP, Spirent Communications
Derrick Loi	Head of Cloud Business for APAC, Orange Business Services
Helen Wong	Director, Partner & Product Strategy Asia Pacific, Verizon.
Amit Sinha Roy	Vice President, Tata Communications

Nikhil Batra

Good morning all of you and I would like to welcome Helen Wong from Verizon; Neil Holmquist, Senior Director, Product Marketing and Management from Spirent Communication; Derrick Loi, Head of Cloud Business for APAC, Orange Business Services and Amit Sinha Roy, from Tata Communications. So welcome all.

So good morning everybody and welcome to the panel discussion on 'Testing for Internet of Things'. I'm Nikhil from IDC and I'd like to begin by giving you a brief overview of the IoT industry.

So recently, there have been a lot of buzzwords thrown around like machine to machine (M2M), Internet of Things (IoT), Internet of Everything (IoE). So what does all of this actually mean?

So let's consider the example of a datacentre which has a few server racks which are equipped with temperature sensors. So in an M2M scenario these temperature sensors would be sending across information of the temperature of the server to a central

control panel and in that case, typically there would be a server guy who would be sitting there, monitoring that. If he sees one of the servers overheating, he would go and switch on probably a cooling system.

When we move from M2M to IoT, the cooling system would switch it on by itself. So that's what IoT brings to the table. It removes in a way the human interaction part and brings that kind of analytic systems to it to manage these and to take these intelligent actions.

And then we move on to Internet of Everything which brings together the people, processes, data and these connected things. And as a result, this could give us more relevant information, something like why the server heated in the first place and then trying to fix that problem instead.

So as we spoke about, the IoT ecosystem consists of the modules and devices which is essentially the sensors, which then connects over a network through these platforms and servers to these intelligent applications. These intelligent applications are basically analytical systems which process this unstructured data in real time to provide more meaningful inputs.

And then everything needs to be secure-we need to do this securely. Everybody says we understand security in IoT, but the hackers and co. have proven otherwise. They've tried to hack into -- hack successfully into connected cars and wireless heart pacemakers, things like that which show that we are far away from actually where we would like to be.

And this presents a huge opportunity for professional services, for vendors, for system integrators to provide these as packaged products to consumers in the form of smart vehicles or smart health monitoring devices, in the form of smart traffic management or intelligent service system for governments. Or for enterprises as smart manufacturing lanes or value chains or probably intelligent automation to some extent.

So the world that IDC sees in 2020 would be of about 30 billion devices connected globally, of which one-third would be in the Asia Pacific region. One out of every five connected devices will be in China and this represents a huge market opportunity for service providers, for vendors, for everybody, of about $600 billion.

Now testing has always been a very critical part of the development effort and finding the bugs has always been a challenge, even in standalone programs. But with IoT coming into the picture, when we are talking about all the devices connected, everything connected, this takes the next step. In an IoT world, a problematic software could be lurking anywhere in any device, in anything, just waiting to explode and strike back with litigation at the company which probably failed to test properly these devices.

[Blue Screen Of Death] - I hope everybody would remember this. There was a time, when I was a developer a few years back, this was the worst thing that could happen to us, in a manner of saying. But now imagine that a system in an autonomous car on a highway running a buggy software which crashes like this. What would happen to

the passengers of the car? What would happen to their safety? Who would be liable for that? It just raises too many questions for us at the moment.

And it's not just fictitious things we are talking about, things like this have happened in the past. There have been companies which have been robbed of a large market value - something which happened with Toyota. This was one of the serious things that happened with Toyota - that millions of its Prius vehicles had to be recalled to fix a software glitch.

The software glitch overheated the hybrid components of the Prius and in a way, forced the car into a failsafe method. In failsafe mode, it would continue to drive but with a very reduced speed. And this could happen anywhere. So imagine a Prius driving on a highway in the fast lane and suddenly going into this failsafe mode. It could mean disaster for the Prius and cars around at that moment.

And then drones have been falling from the skies long enough now. So between 2011 and 2013, one of the reports by the Washington Post indicates that there were about 400 military drones that crashed. They crashed everywhere, right from a school backyard, in the neighbourhood areas, to backyards of people's houses.

So now in an era when the government has opened this air space up for Amazons and DHLs for chopper copter delivery, the number of these drones in the sky are only set to increase and who knows what we are up for? And telcos and postal services have always frowned upon these dropped packets, but it's not about just packet loss anymore. Things like this could lead to loss of human lives - placing human lives at risk.

So with that in the back of our mind, I'd like to invite Mr. Neil Holmquist from Spirent Communications to address some of these challenges.

Neil Holmquist - Spirent Communications.

Thank you, Nikhil. So you guys have heard of the connected car. We now have the connected cow.

So my name is Neil Holmquist. I'm from Spirent. A lot of people wonder who Spirent is. We are a company that builds test solutions that help ensure and verify that the complex network of today can reach and communicate as well as scale up for the network that's needed for tomorrow as we talk about the Internet of Things and how that scale is beginning more and more complex.

So I was going to go and create a fancy slide on all the different areas where the Internet of Things can play (a part). I figured I would legally steal that from Intel. They're one of the leading vendors in this space, so I thought it would be good to just walk you through the five areas or so that we see and the industry sees Internet of Things really taking off.

The one up there in the upper left is communications. I thought that was a funny statistic. You probably can't read it from the back of the room, but it says in 2020, the average person will have seven connected devices. So I went and looked at my house, I looked in my pockets, and my laptops, I have about 15. And I'm pretty sure

everyone in this room has about 15 or so connected devices from your home. But when you think of the average person, that probably makes a lot more sense.

One of the big challenges that I see and Intel put it up here as well is managing these devices. I thought I was nice, I bought my parents a new TV for Christmas. I bought them a smart TV and I didn't realise I'd have to manage all the upgrades and software updates for that TV as well as their PCs and phones and everything else. But I actually think that's going to be a really big problem moving forward.

Nikhil mentioned this from the security aspect, but I think most of the industry now is going to go and put a product out there and then offer a firmware upgrade, a software upgrade later to add features or enhance features. I think that's going to be a huge problem for the mass audiences. Us, in the tech industry, we can manage that, but I think managed services from the provider or the carrier is going to have to enhance to support the billions of devices that we'll be consuming.

Moving over into the retail space, this is the optimiser business. Today, I still see people walking around doing inventory of stores. If that shelf is a little low on this product or that product, we'll go and order more. Pretty soon that's going to be automated.

We're going to have RFID chips, they're going to have everything connected, where they'll now not need to go and manually order more toilet paper for this particular store or more food for this grocery store. So there's a big opportunity that the Internet of Things is enabling for retailers and shoppers.

The one that's probably more obvious and that we see today is around the connected car. You can see just over the past few years, it's gone from about 8 million Internet connected cars to almost 23 or almost 24 million by the end of next year. I have a section that I'm going to talk about what we see from the connected car and some of the challenges.

Over here that I think is probably the next biggest area and I would actually lump this with industrial and energy or utility companies. This is where a lot of the machine to machine communication is being implemented. And from a utility perspective, smart meters etc, this is how a lot of these utility and energy companies are going to save billions of dollars moving forward. And I'll explain that using Google and Nest as an example.

And then lastly, the medical. It would be excellent to go to any doctor and have them automatically pull up my health records, be able to go in and scan myself and have everything updated with any device I have, my wearable, my phone etc, everything connected.

But with that I don't want my personal health information easily available from anybody that wanted to hack into the systems. So security here is going to be a big, big concern. Even now our personal information is out there on Facebook, LinkedIn etc. Now some of our more intimate details are going to be available and that's something we all need to be very careful about.

So looking at the Internet of Things in action, the connected car. And one of the things that I didn't realise until we at Spirent started getting involved in the automotive Ethernet, is the third most expensive component in a car and the third heaviest component in a car is the cabling for the communication in that car.

And that is moving now to Ethernet, where everything is talking over Ethernet in the car. And that car is also connected via cellular to some carrier that everything communicates with.

The example there in the upper left is the automatic emergency call. So now there's sensors in your car that will let you know if the airbag goes off or if you had a sudden stop or some tragic event happened. It talks to the cellular base station nearby, sends a signal over to the emergency services that then dispatch emergency help or fire to your location.

So if I'm a purchaser of a car, I want to be guaranteed that that works. I'm going to pay a premium for that and I want to make sure that works and companies like Verizon and AT&T in North America are building up a completely connected, almost ubiquitous cellular network to manage this.

Moving over to the infotainment, I think it's quite funny. I don't know the laws here or in Asia, but I'm not allowed to text and drive in the US where I live. But you have a ten-inch iPad sitting in front of you that you can play movies, connect and actually I think this is probably responsible for more accidents than texting. But a lot of more information is coming. Your traffic and your weather etc is available now in your car and cars are marketing themselves that they have connectivity.

Going into the -- you may not be able to see here on the bottom left -- is the autonomous driving. I was in Silicon Valley a few months ago and I saw one of the Google driverless cars running around, driving around and I was curious of how does that car know when to stop. How does it distinguish between a ball bouncing across the road and a kid running after the ball?

So a lot of technology and a lot of testing has to go into that and to make that split second decision on what to do. Gathering all that information, communicating, constant communication between car's components, constant communication with other cars, other wearables, other devices. Everything is going to be connected and they're going to be talking to each other. You won't know it but your phone will be talking to cars to let you know the proximity of where you are from it.

And lastly, the one I'm more interested in is the stolen vehicle tracking, iPhone tracking. These are -- you want to make sure that if you're buying into that, it has to work. It has to work across networks. In the US, it's a little easier. In Europe and Asia where you have different service providers different carriers, it has to be autonomous -- it has to be ubiquitous. You can't distinguish between the two. You can't cross a border somewhere and lose connectivity.

Amongst everything else, the thing that I'm really interested in is on the health side. You can see here the guy with his wearable and the statistics. But imagine your wearable, your devices, all communicating your health statistics and aggregating that

into some database. And you have people analysing that databases and maybe it can proactively say, hey, Neil I noticed your heart rate was a lot lower over the past week, maybe you should go see a doctor. Maybe I can do some predictive analysis on that data so that we can maybe save cost and improve our health.

The other item there is -- you can't really read it, but AT& T had a very close partnership with this company called Vitality GlowCaps. And what they did is they allowed access. There was a little cellular chip in [that cap] that talked to pharmacies and it informs them of hey, this person is running low on pills or it will send alerts on your phone to remind you to take your pills, so it can help us be healthy. And that's where service providers and the Internet of Things manufacturers can marry and provide services for us.

Retail and vending, this is kind of a worst case scenario. I don't want a vending machine knowing my name, but that's coming. A smart vending machine will pick you up from your phone, it'll know you are and offer you snacks that you like.

A little known fact, in 1982 in Carnegie Mellon, some engineers developed the first Internet of Things. They were so lazy that they did not want to walk to the Coke machine to find it was empty. So they built a solution that monitored the Coke machines in there so they could check from their desks if there was Coke or not. So if you do a Google search for Internet Coke machine, in 1982 was the first IoT device.

Talking about energy real quick, Google bought Nest and they didn't buy Nest to have a really cool thermostat sitting in the homes. That's not really their play. What they wanted to do is collect data and they collect data of usage. And they sell that usage back to the utility companies. And in fact I think it's in 2016 they expect that the service revenue from the data of Nest will be more than the Nest sales themselves.

And what that means and I didn't really realise this till I started researching. An energy company that makes energy, it's use it or lose it. And once I read it, it became obvious. So companies, these energy companies will spend millions and billions of dollars to produce the exact amount, to correct demand forecasting. And that's what companies like Nest and anything else like that that allows us to get that data, bring it back in house and verify it. And then you have the anything else, and that will -- I'll show you why that's important in a moment.

So the buzz, everybody know there's billions of devices, billions of dollars to be made and companies buying companies to capitalise on this. This is not news to anybody. But just looking out there, there's billions of dollars in transactions happening today.

The connections, we all know, billions of connections, billion dollars in revenue. In the interests of time, so we can get to the debate, I'll skip through this and get to something that I think is interesting.

So of those billions of dollars and billions of connected devices, this report actually broke down the verticals of those devices. You have your utilities and smart grid are at the bottom in the light blue; your automotive your trains, your transportation is orange, it's the big bulk of things. And then you have the smaller players, retail healthcare etc and then that big bar on top is other.

So that's your connected cow, that's your wearables. That's everything else. And why that becomes important is you have thousands and thousands of companies building out these Internet of Things devices to sell maybe 10,000 of them, maybe 50,000 of them. They can't afford testing. They're going to have to push that testing on somebody else. It doesn't make fiscal sense for them to have to do that themselves.

So either a) they're going to skip testing, ship it out and hope it works; if it doesn't I'll fix it with a software upgrade. Or b) they're going to have to partner. They have to partner somebody who creates a cellular module; they're going to have partner with a carrier and test that way. So as we buy more and more of these devices and industrial utilities etc, testing is going to have to become very, very critical. You can't push that on to the end user.

And the other issue that I see is there is no standardisation right now. There's over 140 organisations trying to create a standard and there's about 125 different, just machine to machine standards, which is a subset of the Internet of Things trying to come up with a standard communication mechanism. Without that it means you can't plug and play.

That means you're going to have a lot of proprietary vendor locked-in solutions. And that's fine for now because people are trying to work things out, but pretty soon no one wants to get locked into a Cisco only environment. They don't want to get locked into a single vendor. They want the flexibility to mix and match and grow their needs. So today this is where we are, locked in. You can get multi-vendors work together, but that's more of a NDA or bilateral agreement. But you can't bring something new in, plug it in and make it work.

There is one organisation (OneM2M). I don't work for it so I'm not pitching it. But OneM2M, it seems to be more of an open data kind of general team. They don't have a hidden agenda and they're not tied to any business or organisation. This seems to be the standard body that is leading the charge and most likely will come up with a win. And their whole point is just agreeing on a way to communicate from a machine to machine which is predominantly what's going to happen over the next few years. That's the big move.

I think in closing, the challenges that I see and we see bringing the Internet of Things to reality is maturity. As I just showed with the standard organisation, with the devices, there's a level of maturity that's going to have to happen.

Operations. As a carrier, how do I manage millions of devices? How do I manage millions of consumers with multiple devices?

Performance. I need to make sure my network stays reliable as I have all these new devices connecting.

Scalability, the same thing. With millions of devices all connecting where today you have a few hundred devices connecting to one cell tower, you're going to have thousands in one cell tower. In fact they just had the first IEEE meeting I think last week or two weeks ago on the 5G technology and one of their big goals is to be able to connect trillions of UEs, user endpoints, geared towards the Internet of Things.

Reliability, I think this is going to be the next biggest challenge outside of security. I mentioned being able to have your systems stay up and running. You have a software upgrade, what do you do? Do I upgrade my live network? I think that would be very risky. Do I need as a company to build a sandbox environment where I simulate all these devices so I can play with my software upgrades, much like service providers do, with the Cisco and Juniper equipment today? But it's going to become problematic from a scale perspective because there's so many different devices.

Security. This is my biggest concern. And it reminded me this morning of the story I just read a few weeks ago that a hacker was on a United flight I believe it was. He jacked around with the infotainment system in the airplane and then was able to take control of the engine. That's very scary to me. In fact, my flight was delayed last night because the parking brake didn't work. So I was a little concerned. I looked around. Was that dude on my plane? But that's a big concern. Safety, privacy and keeping your network up.

And ultimately it boils down to profitability. All those things boil down to that. I have to spend money to test. There is no doubt about it. You have to test. How much money do you want to put into it? Because a bad product, a bad experience, people will leave for other options. We're not going to be the only players in town. There's going to be a lot of different things people can switch to. So if they have a bad experience that can affect it or if I don't manage my costs correctly I won't be as profitable as my competitor.

So I think that was my last slide, so I think we'll open up to debate. Thank you.

Nikhil Batra - IDC

Thanks a lot Neil for the presentation. It was pretty insightful. And I think you mentioned a lot about security. You said it was your biggest concern. So let's start talking about that.

Generally what we have tested the devices for is for functionality of the applications that are out there, because the application resides somewhere in a safe datacentre and we are just accessing it. But now tomorrow we are talking about the Internet of Things in which the devices in itself would be ubiquitous, it would be present everywhere.

So I'd like to start with you Helen. What do you think about how the testing would need to evolve or how just the approach around the products would need to evolve to address these security concerns?

Helen Wong - Verizon

I think from an Internet of Things perspective it's quite different to what the carriers used to do on our network. We would go to the nth degree on certifying every bit of equipment, interfacing cards before we would deploy it out in the network. But with the Internet of Things like you said, a lot of the functionalities are tested out, but does anyone really put it out into real life environment where you are going to have all

these hackers that's available globally, trying everything they can to hack into your device?

I think it will be up to the users and also the vendors or the suppliers or the manufacturers to consider how critical is that device to a user. Is it a life threatening device or is it something that is just like a monitoring device that is not going to be critical? Then they would need to decide at that level, what sort of testing they would need to do.

I think to Neil's point, the testing, there's just no standard around these days today. And even with Verizon we do have in Boston, in Waltham, we've got an environment where we open it up. We allow anybody to bring their device in to test in, because our wireless coverage in US is -- it means that currently we've got, like last count we've got 15 million devices connected on to the LTE 3G network.

And because there's no standard, we need to provide the environment therefore people want to have that testing done to be able to come in and make sure it can work over the network and that we do have a record of devices or things that have been tested, that has been interoperable and we're able to support on the network.

So yes, I don't think there's a perfect answer. There's still a long, long way to go on that one.

Nikhil Batra

Thanks for your answer. Derrick, would you like to weigh in with your thoughts on this? The testing part, how important the testing is going to be and how our approach will need to change towards testing of these devices for security.

Derrick Loi - Orange Business Services

Well, I think in terms of the Internet of Things, from the testing perspective, as probably we have just seen earlier, the Internet of Things is not just about machine to machine. It's not just about the machine exchanging information between each other. It's also about how it relates to the processes and the workflow of the enterprise and how they engage with the end devices as well as internally within the enterprise database.

And I think today that is an element of security and testing that has not been addressed, because we all know that a lot of enterprises who are branching into Internet of Things, they still have their legacy applications, they still have their legacy database, they still have their legacy infrastructure.

Now how that catches up and is securely connected to the devices that are just growing in volume, how the current workflow of those enterprises and how they get their business done internally, how that catches up with the very dynamic nature of transactions that we are seeing between devices, that aspect of testing has not been addressed.

So I think this is my comments to the trend and the gap in the trend that we have to address going forward.

Nikhil Batra

Okay, thanks a lot. So in case we say that we'll test these systems perfectly, they do work in a test environment, once we put them out there, what would happen in case something goes wrong. Who would be responsible? So are the SLAs being written that way or is that something that's being addressed right now? Amit, maybe you can --

Amit Sinha Roy - Tata Communications

So to come back to the point of security, if we look at the various aspects, I think Helen mentioned it, it's also the criticality. So you have the device that connects to another device locally and typically that is not having much issues in terms of privacy or hacking because it's a local Bluetooth connection. Of course Bluetooth can be hacked by somebody locally, but typically it's not going to go on the Internet.

But if we look at it from a holistic point of view, then it comes across, the application, the firmware, the connectivity, if it is browser based, the security of the browser, the whole nine yards going all the way back to the datacentre, both in terms of security as well as privacy. Privacy is equally important.

So in order to secure the entire end to end, it requires multiple interventions. It's not just one. It's not that one person or one company can be blamed at this point in time. Of course the fault may lie in one of the areas, but then it is an end-to-end service delivery both from security as well as from privacy.

So one of the points I did not really cover in the earlier session, Mike asked me about what are the new areas, one of the things we were looking at, although today Tata Communications' services are B2B, we are looking at how we could potentially extend some of these services like the IZO Internet WAN or the connectivity over wireless last mile. Today the wireless last mile is not having the capability to give such SLAs.

But as it moves forward, you talked about 5G or maybe with 4G itself, we're looking at actively how we can extend that. And that will give a solution capability of security at least over the network. The device, the application firmware still is something that needs to be looked at. So that's the kind of thing that we're looking at in terms of providing security and capabilities across, for the Internet of Things.

Nikhil Batra

Okay. That brings to me to my next question. Neil, so as a provider of these testing services to top organisations around the world, have you in a way worked your way around or probably developed new ways of writing these SLAs? Who would in a way be responsible in case, say autonomous cars, the Google car you were talking about, stops somewhere or God forbid, it probably hits a child or something on the road? So would it be that the testing guys who would be responsible, the product developers? Are we looking at it in that way right now or we are still far from it?

Neil Holmquist

So our CTO reminds me very carefully that hey if we go and test a connected car and stamp our approval, are we liable in case something happens. So honestly we are looking into that.

But I think what it boils down to is everyone will want a single point. It was that person's fault, it was that person's fault. So I think one way to get around that is not wait until something happens, but bake in active monitoring and active testing all the time.

Netflix does this. They have something called Chaos Monkey. I don't know if you've heard of this. But they have a tool that randomly goes and creates chaos in the over the top network. And it's the Netflix engineer's job to go find that problem and fix it before it impacts anybody.

I think in this world you're going to have the carriers that create the connectivity. They're going to have to make sure that connectivity stays solid. I think from the vendors, they buy a module from Qualcomm or whoever it is for that connectivity and they're going to have to get a stamp of approval from Qualcomm that it works but they're going to have to do their testing. So I think everyone is going to have to bake in that cover your butt scenario. And be able to prove that at any point in time.

Nikhil Batra

Helen, I'd like to ask that as a telco Verizon is pretty much very heavily invested into IoT. But then development and testing is not a telco's forte per se. So are there any specific challenges that you are facing when you are embracing IoT in terms of testing or developing these new softwares or solutions around these (intelligent) systems?

Helen Wong

We are a big customer of Spirent. So it's obviously that we do spend a lot of money with companies that do testing on all our equipment.

But to Neil's point about yes, the vendor will have to test it; the telco provider will have to provide the SLA. But more importantly, I think when somebody develops something, it's important to put in scenarios, the crash testing scenario right. So assume the worst, something happens, you want to create those scenarios to be able to test it. And that's how you address the security side of things as well. Don't just test what you think might go wrong, but put it into scenarios that are going to cause problems.

Those people that are probably doing more and more that might come ahead [inaudible]. But in terms there are -- still there are demarcations. In some ways, plug and play you can't guarantee it's end to end. You're always going to be -- there is a demarcation point. But hopefully with a lot more collaboration between -- the line becomes pretty blurred on where's the carrier line and where do you stop the service and your liability.

I think people need to take it to a step further is you've got to look at it from a user experience, the application what are you providing end to end and take that into consideration and try to not draw the line this is where we stop.

Nikhil Batra

Okay, sounds great. And most of the IoT industry as we believe it will in a way thrive on interoperability. Nobody will be able to go out and just say that I have this product (which works by itself) - they can't work themselves alone. They need to collabarate. The devices and the products will be intertwined with each other. A lot more will be inputs and outputs coming out of devices and going into other places all the time.

So simulating testing or setting up a test environment to test a whole end-to-end of this sort of solution would always be a challenge. Just like Helen mentioned that plug and play would hardly be an option for a new person coming into market. And somebody who comes into market will not only disrupt and not only change the dynamics of what is existing there today, but also it will not be probably an ideal scenario for them. So are we looking more towards a virtualised testing and simulated testing environment today? Derrick, if you might --

Derrick Loi

That's a very good question, Nikhil. For Orange Business Services, we firmly believe that in order to enable Internet of Things, our core competence is to actually connect between the various platform, the various clouds securely to enable the devices that we site on the various clouds, to enable the infrastructure as a service or the cloud computing services, SaaS, that we site on different clouds to talk between each other.

So for Orange Business Services we are very focused on providing a multi-cloud orchestration platform that enables that. And this multi-cloud orchestration platform which we call MCloud for short provides the ability for enterprises to actually host their applications on a platform as a service that is dedicated to their enterprise. And to therefore do all the testing, all the data analytics, all the database, all the CRM applications, OSS, BSS applications.

This allows the enterprise to actually host it on that platform and automate the provisioning of these applications on to different clouds profiles or in a single automated portal. So that's what we firmly believe in.

And therefore my answer to your question is that be it from a testing perspective, be it from a data analytics perspective, be it from hosting the MDM, MAM, that supports the Internet of Things, Orange Business Services will provide the platform as well as the orchestration of the multi-cloud in order to support the Internet of Things.

Nikhil Batra

So you've touched really well on the virtualised testing and the orchestration part of it. But Amit do you believe that a virtualised testing can actually match the rigours of physical and actual testing?

Amit Sinha Roy

Absolutely. Absolutely, it can do that because we're talking about software over here. So if you look at the way there is now capabilities to do simulation even for building very sophisticated aircrafts, automobiles which are physical products, that knowledge is already available to build physical products. And software testing is something that's also been pretty much there for many years, more from a bug fixing scenario.

So I don't think it's a challenge at all to be able to do a simulation, to be able to do software testing for these kind of devices and applications and firmware solutions that are being created.

Will it be perfect? Maybe not. But will it be 99.9 or .99 or .999? I think that's the question we're looking at. So absolutely yes, I think that's a possibility and I would support that approach.

Nikhil Batra

So you say that software testing would be pretty good, 99.99 or 99.999 or 99.99999 or whatever it could be. But when we're talking about IoT, we are talking about us relinquishing control in the hands of these machines, say an autonomous car we have been speaking about all along. So for these kind of scenarios, if we're talking about (99.9s), this is not just a software we are talking about. It might be human lives at stake that we are talking about. So the same question to Neil that, would virtualised testing or would simulated testing match the rigours of probably having physically tested these solutions?

Neil Holmquist

I would say no. There's going to be certain areas absolutely. But car manufacturers today, they don't simulate crashes. They actually put a dummy in a car. I have a couple of people I'd like to go in that car. But they put a dummy in the car, crash it and they analyse it and the same thing is going to happen with the connected car etc.

In the mission critical lives at stake scenarios, the rigours of testing are going to be the same as the automobile today. Governments will get involved. There's going to be testing standards being defined by government and lobbies for things that -- aircraft trains, planes and automobiles etc.

But you can use virtualisation to test scale. You can use virtualisation to test other aspects. But there are certain things that will require real things.

Nikhil Batra

That's pretty clear. And in terms of, we talk about big data analytics all the time. We have been talking about various aspects. Do you think big data analytics could be used for testing in some way or the other to come up with more relevant test results or to have historical data that last time these kind of things were in there? So are we heading towards that or do we have something around that currently or --?

Neil Holmquist

So we're getting into the minority report of things and precogs. But I actually do think that's the case. With enough analytics, with enough data, you can -- not me, but very smart people can find patterns in that data and with that, can make predictions of that data to help better things.

I can't even imagine what things they would better, but it should not be without reason to think that with petabytes of data you can figure out something that will help people.

Derrick Loi

If I could chip in -- sorry Nikhil if I could chip in, I think let's be very clear here right. There's testing which serves to ensure compatibility as well as stability of what we are trying to implement. But at the same time, we actually establish a baseline of the expected performance of certain applications over or between devices.

Now there's always the stage after testing and that is when you go into production and there's the need to do monitoring, to do performance management. And this is where the baseline that was established during testing is referenced against to determine whether there's fraudulent transactions or whether there's abnormal activities.

And I think what is truly lacking and something that we have not covered in today's discussion to enable the proliferation of internet of Things is we have an NOC for example to monitor the performance of network. Service providers and increasingly a lot security vendors have the SOC to monitor the security of the network and the applications. But do we have a IoT NOC or SOC equivalent to actually monitor the transactions and to baseline and reference them against the baseline that was established during the testing to ensure that there's actually no abnormal activities or fraudulent activities?

So I think that is something worth thinking about especially for companies in measurement and testing, whether we have the technology to actually enable IoT service providers to provide a SOC or NOC equivalent to actually now monitor IoT.

Nikhil Batra

So I think that SOC and NOC would be something, the standards that we were talking about all along.

Anthony Caruana - CSO, Australia

Anthony Caruana of the CSO magazine, Australia. Testing is broken. We can't possibly test billions of devices using the mechanisms we've used over the last 25 or 30 years. We just can't do it. We don't have enough people. And I take what you guys are saying about using big data analytics but we don't have enough people to do that. I think last stat I heard was we're going to be 16 million people short for analytics over the next two or three years.

That means you guys who are at the forefront of pushing the IoT and IoE world have to change the way you think about testing. What are you actually going to do? Like

I've heard lots of general stuff about testing, but tell me something really concrete that's going to make me feel a little bit more assured, because 99.999 is not good enough in a world with 10 billion devices plus because that's still hundreds of thousands of flawed devices.

Neil Holmquist

Well, from Spirent's perspective, there's a bunch of things that we're doing today. One of the biggest one is cellular connectivity. It's not billions of devices, you're getting down to the root level of my IoT pencil connected to the network because if I'm a manufacturer of this pencil, I'm not going to be testing the chip.

Anthony Caruana

[inaudible]

Neil Holmquist

Correct. So that testing of that connection is what we're doing today. We're working with those companies, building those modules, those chips and that they can connect to the Verizons, the Tatas, the Oranges of the world. So that's one aspect.

The other aspect is interoperability or standardisations. If I'm oneM2M standard, I can make sure it can work. So we're working on singularities making sure that these things work as specified. That's where we are today.

Anthony Caruana

[inaudible]. The world doesn't work that way because there are more interactions between devices and people than you even know happen.

Neil Holmquist

That's true. But from what we're, Spirent is doing and I'll let these guys and lady join in. But from what we're doing is on the machine to machine level and right now that industry is all about the old way. Because I have to communicate, I have to be able to take this guy and that guy and have them work. So that's where we are today.

And it's going to be stepping stones as it gets into the new world order, your wearables and the wider range of connectivity. But the mission-critical applications today are more on the automotive connected side and the machine to machine on the industrial side. That's where we are today.

Helen Wong

He didn't get the answer he wanted and I don't think there is an answer for you today.

Anthony Caruana

[inaudible] because I've heard this before. I'm looking for something new.

Chris Rezentes - Verizon

It's interesting we're hearing a lot about the testing we're talking about today and procedures, SLAs and things of that nature. I wonder would there ever be enough testing to feel safe getting into a driverless car. If you're the vendor creating that car, one would have to imagine then that you could have X amount of testing, but if you're going to be liable for something, a lost life for example, would it be safe to assume at least in the early years that we're going to see a lot of legal disclaimers from companies creating these devices that are going to say look, at your own risk, similar to going parachute diving somewhere or something like that.

It seems like that's going to be very common I think. I don't think that there would ever be enough testing as a company to make you feel good Yeah, 99.9 and we'll never get sued is probably -- would you guys -- would that be safe to --

Neil Holmquist

Well, I mean for me and I actually had this discussion with a colleague and I would feel safe if there was only self-driving vehicles on the road. The fact that there is a mix and the unpredictable human aspect is what scares me more than the autonomous car.

Amit Sinha Roy

And on the flip side, do we ask these questions when we get into an airliner, because it's all on software. And I think the captain and the co-pilot are just involved for a few minutes and then everything flies automatically. And there have been issues. There have been issues at air shows where brand new models of planes have crashed and then they've learnt from that and they've improved the software. But I think there's a lot of learnings over there that can perhaps be moved in transportation to the automatic cars and so on and so forth.

Nikhil Batra

So I think there's always going to be this question around the safety until and unless once we come up with these products and we, in a way come up with new standards. This is a whole learning process. We just need to adapt with the industry as a whole as we go forward with this. Any more questions?

From the floor

Hi. Neil, you have been telling about M2M standards. Can you tell a bit more about it?

Neil Holmquist

Apart from -- I'm not sure what you would want to know. So basically the way the machines can synchronise with one another. So just like BGP or OSPF in communicating and creating that communication channel and so that's one aspect. And the other aspect is the service layer on top, the software layer on top. Because

we don't want a bunch of companies building software and customised stacks underneath to do all the communication.

So OneM2M is that layer that handles all the communication between the devices so software can run on top of that on a common API if you will so that they can communicate. If you're asking me the detailed spec, I'd have to get back to you on that.

Nikhil Batra

Is there something particular that you're looking at?

From the floor

How would it work on different technologies and different software that's being used? Or I'll talk to you later about that.

Sherrie Huang - Analysys Mason

This is Sherrie Huang from Analysys Mason. So just now about the reliability question, it's quite interesting. When it comes to high reliability because there are billions of devices, there still can be some numbers of devices go wrong. But the things I think should be divided into two parts like mission critical or not so critical like watches or something. Like the laptop if it dies, then report it.

Then the other thing is about when it fails is there any back-up solution like fall back systems or like a parachute. So anything like that now available in the industry like a back-up solution or when something goes wrong, something can still support the function?

Amit Sinha Roy

I think there will always be these failsafe solutions built into these vehicles or whatever autonomous things we are talking about.

Helen Wong

I guess like you said depending on whether it's critical or non-critical. If you look at your smartphone now, if it dies on you, if you have got it backed up into the cloud in the Google, you can get your back up data, get a new device and get you up and going almost within minutes. So it really depends on the application and what you're using it for.

I guess in the Internet of Things because it's kind of a paradigm shift, it's so new, I think we -- yes, it's important the security and the reliability and the testing will happen. But consider it, even before the Internet of Things we're using millions of electronic devices for years, your laptop, your fridge, your TV, your phone. All those things can fail and can have adverse impact on how we run things.

But I guess we're so keen on getting things and data available instantaneously and it really depends on what the application is. I think the level of testing, the level of

standard and the level of how data is protected, it's not going to be one standard that we are be able to cover all of it. That would just be impossible. So there's got to be a lot of work between different parties to define that standard over time I believe. But do we back up data, do we make sure things can come back up? Yes, there are solutions today that can do that.

Nikhil Batra

Thanks a lot Helen. I think we've had a very insightful discussion, a very interesting discussion here around IoT. We are still moving towards IoT. We are not there yet. The industry is yet to decide (on a lot of things). But we see a lot of smart things happening around us and the best I can say is that we are in for a ride with IoT.

So thanks a lot to the panel and the audience for this discussion. Thank you.

[End]