NETEVENTS

EMEA IT SPOTLIGHT

DRAFT

Conference Debate Session V - They're Everywhere! Managing the Incredible Explosion of IoT and IIoT Devices

Chair: Kevin Restivo

Research Manager, European Enterprise Mobility, IDC

Panellists:

Jan Guldentops	Director, BA Test Labs
Peter Galvin	Chief Strategy and Marketing Officer, nCipher Security
Philip Griffiths	Head of EMEA Partnerships, NetFoundry
Professor Martin Curley	Director of the Digital Academy and Open Innovation. The Health Service Executive
Michael Kagan	Chief Technology Officer, Mellanox Technologies

Kevin Restivo

I'll make a few remarks, set the stage for our IoT discussion by framing the market. That's what we do IDC. We size, forecast markets, describe the drivers and inhibitors. I'll do that in exactly one slide. I'll use a lot less slides than the other presenters and hopefully set the stage for everybody to help you understand why we at IDC believe IoT is one of the fastest growing markets or collection of technologies as I'll describe in a moment relative to the ICT spectrum.

Here's what I mean. For the vendors in the room, the bar graph and the growth rates are basically what you would hope to see and what you'd expect to see intuitively given the discussion and the promise of IoT and the fact that it's very early days. But it begs the question first and foremost, what do I mean or what does IDC mean by the internet of things? Natural question because of what I said previously. That is a vast collection of technologies. What I mean by that is a network of uniquely identifiable endpoints, hence the word things that everybody uses, that autonomously connect bidirectionally using IP, IP connectivity to be more specific. The ecosystem is really a complex mix of technologies and services that involve a lot of what we discussed over the last day and a half. So that's server, storage, analytics, IT services, security and a range of other technologies that I won't limit the definition to but essentially a wide span of the ICT spectrum.

That largest portion of spending, given my description of IoT last year, the last historical period we've measured, is really in the device category, so about 30 per cent or just under 30 per cent is on the devices themselves. The spanning is quite fragmented given the range of technologies we're trying to measure and the fact it's early days, so the groundwork is very much being laid as we'll talk a little bit about. Device is services, software spanning across the board fairly evenly distributed.

Over the forecast period we're expecting a lot more spanning to happen on, as you can imagine, the actual platform analytics as people try to derive the benefits of IoT so that operational data that can really improve processes and essentially the results of the operations they're trying to derive from IoT. When you think about the spanning, this is a worldwide forecast. The bulk of it is happening right now. It's happening nearly half, 45 per cent, in Asia-Pacific. The Americas are the second-largest group of continents, if you will, followed by EMEA, the region we're in right now. However, EMEA we expect to grow the fastest as it plays catchup over our forecast period.

That's our take on IoT. Why is it growing so fast? If you look to the right of the slide the key drivers - this is not a laundry list or a comprehensive list and I'd love to get everybody's input on this including the panel's as to what's actually driving IoT from a deployment perspective - it's essentially a collection of drivers. First and foremost the proliferation of the internet-connected devices and things. What that means is people are trying to gain that data and insight into business operations. The initial value of IoT is going to be realised in the operational improvements made using that IoT-generated data. That's one big driver.

But also complexity. You might look at that as an inhibitor but it's actually a driver because of spending first and foremost because people need to spend on multiple software layers to make everything sing together. So, that hardware, the services, the connectivity landscape includes a large array of vendors, as you might imagine, given our definition. So, those phones that you have before you, the enterprise computing devices, they run on a very limited set of operating systems and networks over TCP/IP, whereas IoT - we discussed this earlier this morning - run on a vast array to say the least of operating systems and protocols that make it, there's that word again, complex. That complexity is again driving a lot of spending.

Nevertheless, enterprises are ready to deploy IoT for the benefits I've already mentioned, the gains that can be had from that. They're ready to act with IT projects. It's a strategic directive for many organisations as our global decision-maker survey will reveal to you. If you want to look online there is a free webcast and a free download you might want to check out as well. I can send you the link. But the efficiencies of differentiation and the feedback loops that can be generated from the products and services is really the benefits the enterprises see and they're ready to deploy and invest in IoT solutions across the technology stack.

There are implications to that too that we will discuss. First and foremost among the major implications to the downside - like every other benefit in life there's a flipside to that and security is one of them. There are impacts to each of these assumptions and downsides too.

Going to the point about security concerns, year over year despite that enterprise readiness it is really the greatest inhibitor we see at IDC to IoT deployment and adoptions. Those vast quantities of data and content that are being created for connected things mean there's a whole range of issues around compliance, governance, privacy issues - essentially risk and governance. So, despite the promise of IoT there is definitely downward pressure as a result of the security implications.

As much as technology is involved in IoT we're still talking about people and people and processes, that feedback loop that everyone has become so familiar with over the years, technology, people and processes. The people part of it is also an inhibitor. What I mean by that is that lack of coordination between operations and IT is very much an inhibitor to deployment as well. That means close collaboration between IT and operational departments is necessary and yet it doesn't happen. Everyone wants to protect their fiefdoms or they're simply not able or willing to cooperation, and so the lines of business driving demand for IoT don't necessary synch, if you will, with IT. So, IT is often left behind during the project planning and budgeting and the piloting. That lack of coordination again is an inhibitor. It can really stall the successful deployment of IoT initiatives as far as the impact goes in a timely manner and the procurement processes as well.

With that, let's get into the weeds and talk about the various issues around IoT and what we see in the field. That's the birds'-eye view of the market, if you will, the way we see it. So IT market heading in the right direction. Are there any other key drivers or inhibitors? Like I said off the top, it's not a massive laundry list of drivers and inhibitors. You're in the field. Any other key drivers that you see taking IoT deployments forward? I'll open out to any of the…

Peter Galvin

Personally I think the IoT market is broken into a few segments. Some of the things we were talking about earlier - you have either the consumer segment which is growing rapidly, doesn't have a lot of security focus on it and people are trying to drive a lot of devices, and then you have more of the industrial IoT side which is probably a little more thoughtful. Then you have that quasi - period in between where we're seeing a

lot of interest in things like medical devices that have a much higher regulation but are still at the end in many cases either used by consumers or used by medical staff. So, you're seeing some of those pieces get into the marketplace, but I think on the consumer side it's being driven because there aren't any security concerns, there aren't any - I mean, there are security concerns; they're just not being addressed

Jan Guldentops

It's more difficult than that. It's such a wide range of devices. We're going from very small sensors for use, for instance, in parking spaces which are there for 10 years which have a battery, which send one piece of data a day, to complex plc-like industrial [unclear] stuff with 200 sensors controlling $2 million devices. It all has its impact especially on security because the battery is the limiting factor for the first one.

So, maybe we should try to cut up this broad term and put it into certain categories. I think we're going to talk mostly about industrial. Consumer is…

Kevin Restivo

We don't have any consumer IoT here so I think we can safely limit that discussion.

Jan Guldentops

It's a very broad market and that has its impact on security. We all forget that. It's like cloud all over again. I was inventing some of them right here and I came up with - somebody said the internet of shit. I came up with IOBSD, internet of badly secured devices.

Philip Griffiths

I think security is the biggest thing holding back IoT or consistently comes up in surveys as what's holding things back from going further. But it's interesting because some organisations do see that and are, therefore, looking at, how do I solve it? In fact, pulling together a few of the things you had on your slide, I'm working on an engagement at the moment where a Fortune 10 company is rolling out an IoT solution. They're not involving IT because they want to move as quickly as possible. But the partner we're working with, who's an ISV, came to us and said, we need to make sure the solution is very secure so that when IT do come along we can say, this is more secure than your corporate network so there's nothing for you to worry about, and at the same time we don't want to have to manage 50,000 VPNs so we're going to use your solution because it automates that secure connectivity.

They realise they have that issue and are, therefore, looking to deploy a solution which really gives them a rapid return on investment which is driving that first thing of how to make the business change. It's all well and good connecting things but unless you're driving the business, a return on investment and a reduction to bottom line or an increase in top line it doesn't matter.

Kevin Restivo

Great. So, business benefits, let's not deploy technology for technology's sake, operational improvements - that's what I'm hearing from the panel so far. Martin, you're champing at the bit. What benefits do you see from IoT from the people you're talking to in your experience?

Martin Curley

I've just moved into the healthcare sector from Intel and I think there's a massive opportunity for IoT - the amount of unconnected devices and the amazing benefits that will come, the consumerisation of IT that we saw over the last decade or so - we're going to see the consumerisation of healthcare. Eric Topol, a renowned American cardiologist has written a book called *The Patient Will See You Now*, and we will now have patients routinely showing up to their cardiologist or to their nephrologist with much better information than the consultants themselves have. The Apple Watch with its ECG is already an FDA-regulated device. It can detect atrial fibrillation. It could be lifesaving.

But I think one of the huge opportunities is the internet of you. We will all be instrumented and all our vital signs, and we will come with better capabilities than you can get in the acute or community-based hospitals. As an example, in Irish hospitals the vital signs monitors are not connected to the network. A small Irish company called SyncroPhi have developed a solution to automatically connect and collect and display vital signs. What they found as they were doing their trials in the Galway Clinic, which is probably the top private hospital in Ireland, was that over 50 per cent of the early warning scores that were computed for patients by handwritten notes from nurses were incorrect. This is the key predictor that nurses use to determine if a patient is deteriorating, and the current manual system over the 50 per cent of the scores were wrong.

There are so many opportunities. Another small Irish IoT company called [Reever] is developing a technology to track pieces of equipment in the ward. One of the key issues is there's so much time spent by nurses and doctors looking for equipment that somebody else has borrowed. They've developed a smart solution that RFID-enabled tracks where the equipment is in the wards. I can probably give you 10 other examples.

I think the biggest untapped market is going to be healthcare, and the big paradigm that's coming is that patients will show up with better data than their consultants have and their doctors have. That interaction, the patient will become part, because of the internet of things, of the medical production process. It's going to be hugely exciting and I think it can absolutely lead to a scenario where we can add several new years of life to the average person's lifespan because we have proactive and pre-emptive interventions we can make based on, like, the Apple Watch detecting atrial fibrillation. That's absolutely a lifesaver.

Kevin Restivo

Let's hear about some other use cases and potential benefits. Philip…

Philip Griffiths

Very quickly because that was all very positive and I need to be a bit negative, because last year there was a Wipro survey about cyber security. It was saying how healthcare is now the most attacked industry. It literally gets I think 40 per cent of all attacks because medical data is twice as valuable in terms of where hackers are attacking than financial data because they're able to use it to abstract more value, to the point that when they did the survey in last year, the year before, an average hospital had 40,000 exposed endpoints of how you could get access to the network and, therefore, compromise systems. If we're connecting all these other things in just a - hey, throw it on the wi-fi, it's going to become crazy in a way that could impact people's lives.

It's all well and good to see the benefits - and I really believe they are there - but we have to make sure that we're doing security by design as early as possible within the manufacturing process so that things aren't being connected which are putting people's lives at risk.

Kevin Restivo

I want to delve into IoT security but at the risk of running - IoT security panel - I'd love to hear more about use cases and benefits potential.

Peter Galvin

A couple of interesting use cases we've run into - we are a security company so they do tie into security - the things we've seen like smart meter programs where you have smart meters. Those are IoT devices. They're providing information back to central systems. They're providing a bunch of data. That's been a project that's been going on for a long time in the UK. Recently we've done some work with a company that's doing surgical robot. As you can imagine you have doctors and you have surgical centres. They're in different places so you want to be able to provide a hip replacement or a knee operation and be able to walk into a hospital that doesn't have the doctor present but you can then download that information about that patient and about that code to that surgical robot.

We're seeing a ton of interest in automation. There's a lot of talk about autonomous cars, but really what we're seeing is autonomy is more in the industrial area. If you think of big giant harvesters that are out in the mid-west doing wheat, there's nobody in those. They're all remotely controlled. They're considered an IoT device and they continue - they're giving telemetry data and also data about - what's the soil like? What's the content like? How fast are they [go through]? There's all this data collection going on as well as effort going on.

Recently an energy company in Australia is moving to doing the same thing. They're automating all their mining equipment. So, now again where they have mines hundreds of miles away from any civilisation and they used to have to transport people to those mines and feed them and do a whole bunch of stuff, now they can do that all remotely. There's a lot of innovation going on in a lot of different sections of IoT. There are certainly a huge amount of benefits.

Jan Guldentops

It's the same thing with the smart cities project. You have speed cameras these days. I know that's not a popular thing. The average speed camera collects a lot of data you can use to send tickets, which are basically indirect taxes, but you can also use it to do policy. You can see how fast people drive combined with other technologies. Cool stuff. You have parking systems in which you can give people, for instance, 25 minutes of parking based on a sensor. You can monitor that and you can display that. There's quite a lot of stuff to do.

Philip Griffiths

I personally believe - smart city is one thing that's been talked about for many years. There is stuff happening there but it's not as much as the marketing would tell you because governments find it difficult to say, how am I going to make money from that? Whereas a manufacturing plant…

Jan Guldentops

There's European money.

Philip Griffiths

Yes, there is.

Jan Guldentops

There is European money for it so every city is doing it.

Philip Griffiths

On the other hand, a manufacturing plant or global business can say - we're working on one at the moment where they're going to be installing thousands of cameras in their manufacturing plants to reduce defects and, therefore, increase their return on investment on the production process which will be billions in terms of their spend - unfortunately that's not on us - but which will have return on investment in months because it's really saving that much on their production process.

Where it gets into the very interesting bit is a lot of people - particularly from the sales and company perspective - everyone was trying to see, how do I position myself in IoT? How can I sell into it? But you don't do it just by saying, here's my product. All the opportunities we're working on IoT are where we're bringing together an ecosystem of different technology providers to provide a full turnkey stack for the end company so they can just go, okay, I can pay for that as a service rather than I have to assemble it all myself, which means playing nicely with other partners but it's fundamental to IoT because otherwise it's far too complex to pull together as one business.

Peter Galvin

One last thought is, we forget about the gains from information. If you think of all these IoT devices, whether they're censors or parking meters or health devices, there's so

much data that's being transmitted, and as you anonymise that data organisations, especially in healthcare, are learning a ton about patients that they wouldn't have learned before.

It does give some great scientific strides and really can help people, because before you'd have to go do a medical trial. As long as people are willing to give you the data, now you can have some really genuine insights into the way people are living and also if they're having issues. So, I think from a medical standpoint there's a lot of opportunity there to more rapidly help people with some of these devices.

Michael Kagan

Jan talked about policies. The point is there is feedback. Something happens that we all talk about data collection. Now, somebody makes a decision based on this data, and because we are talking about machines the decisions will be formalised. Once these algorithms, formulisations become known it can have very interesting implications on our lives.

I can give you an example [unclear] discussions that if I'm building the algorithm for a self-driving car I need to take into consideration the fact that if I have two bicyclists in front of me and an accident is unavoidable, how do I choose which one to hit? Of course you try to avoid it but if it's unavoidable, how do you choose which one to hit? One of the options can be, we'll probably hit the one that wears a helmet because he has a higher chance to survive. Once this algorithm becomes known nobody is going to wear helmets anymore because you're going to be hit by the car if you wear a helmet, and the result may be tragic out of these things.

You can go on and on, but once we make the decision, which is the policy is one of the examples of the decision based on the data, we need to figure out how to understand the implications of these things happening.

Kevin Restivo

That's not a bad segue. So, implications, using that word. Jan and Philip, you were champing at the bit to talk about IoT security. We have a few minutes left, so let's talk about the realities of IoT. It was Joe yesterday that talked about internet-connected kettles taking down Hargreaves Lansdown in the UK or something like that, so there are real security problems given the diversity of operating systems that I mentioned. There's a lack of security right now.

Jan Guldentops

Can I give you an example? I would like to be the devil's advocate a little. Security is in my opinion at this time not holding back IoT because it is an issue but not in the minds of a lot of people that are implementing it. I'll give you an example. A certain brand of speed cameras runs a Debian 6 operating system that hasn’t been patched since I think 2010, 201, I don't know by heart. So, it takes me around three and a half minutes to become root on that system.

They cannot patch it. I talked to the guys and they said, we cannot patch it because we need to validate the system and every change we make the speed camera is not valid anymore. But still there are around 400 AMPR cameras in Belgium that are using it. So, it's not really a concern. The only way it's going to become a concern - and it's unfortunate we don't have a legal guy here - is when it becomes a liability.

In the medical we have that already because GDPR says you have to be careful with people's data. So, you can be fined up to four per cent, but for all the other ones, if you're hacked it's probably *force majeure* and you're not going to be liable for the damages. Once that starts coming up we're going to do security, but up to that moment it's not a concern really.

Philip Griffiths

Devil's advocate to devil's advocate - I do fundamentally agree with that. This is where - to circle back to what we were discussing earlier - commercial IoT, people care less about the data. A speed camera, it's maybe not important data. On the other hand of the scale when you're talking critical infrastructure, when you're talking things that can impact people's lives, I think it is holding back in that people are not looking to connect things.

They may find a way to connect things by merging the industrial network with the IT network which then creates an attack - most of the attacks we've seen have been some sort of phishing campaign turning into malware, laterally moving from the IT network into the OT network because someone didn't think about security enough and then blowing up a billion dollar [molten] steel facility or something as happened in Germany a few years ago, where because of that people are looking at, how do we manage to get benefits from this digital transformation from IoT but without compromising the security of our systems?

That's where it's been held back, where people are not - if you speak to manufacturing companies they're all saying, how do I bring the cloud on to my premise? I literally have no external connection. That's why Azure Stack is popular in disconnected [node] which is a heinously expensive way to consume Azure because you pay for it twice, but that's how they're doing it and that's where it's being held back.

If we create that secure connectivity with software-defined perimeters, zero trust, all these things, then you can get the benefits of both worlds so that you can move towards having the benefits and the light at the end of the tunnel.

Peter Galvin

I do think depending on industry - I think security in IoT is like other things. The best thing to do is, everything would be secure but there's also the - how easy is something to use? It goes back to, can my mom get into her email? You could make it super secure. You could have really difficult passwords. You could have multifactor authentication. So, it really depends on, how important is that? And making sure there's a certain level of usability. I think the same thing is true in IoT whether they're consumer devices or industrial devices.

Jan Guldentops

It should be easier in IoT because you don't have a lot of human interaction.

Peter Galvin

From a security standpoint?

Jan Guldentops

You just put the device. Or am I wrong?

Philip Griffiths

Most IoT should be machine to machine.

Peter Galvin

But I think there's also policy associated with that.

Jan Guldentops

That's typical. The installer, the guy who develops it, they don't have the skillset. They don't even think about security. They're not paid to do security; they're paid to deliver the product as soon as possible.

Kevin Restivo

As we said earlier, the incentives are sometimes misaligned about how to do that. A lot of times that becomes a - oh, we didn't think about it; it's now a secondary consideration about…

Jan Guldentops

We have to bolt something on.

Kevin Restivo

Martin, you had a comment.

Martin Curley

I agree with Jan in that the IoT industry is carrying barely along. What it's going to take unfortunately is some sort of catastrophe to raise the awareness that security really is a massive issue. Similar to the Boeing 727 Max with the angle of attack sensor with a faulty - that is an internet of things device, but I think for the industry of things industry that also is one of these road to Damascus moments that software resilience and software validation has to be done in a much more thorough way than it has been.

There's the software resilience and functional resilience as well as the security issue. I think it will be something like another Stuxnet incident that will occur and there'll be big trouble and then it will make people sit up and say, we can't continue on this path; we've got to take security very seriously.

Kevin Restivo

If any organisation is interested in IT I'll cap off with saying this - and we're going to open the question to the field - we absolutely see security as top reason why organisations don't deploy IoT. That said, we haven't taken any questions for the panel.

Audience Q&A

Davey Winder

Davey Winder, *Forbes*, *Sunday Times*, et cetera. Martin, really to you. You've just spoken about it will take a catastrophe. We've already got catastrophes happening especially in health. For example, recently security researchers did a proof of concept in a [pen] test in a live hospital where they introduced malware into the software for CT and MRI scanners and managed to change the data that was coming out of cancer scans.

They removed cancerous nodes from scans and they added cancerous nodes to scans. Three consultant radiologists were unable to identify which ones they'd adjusted, manipulated. This is people's lives we're talking about. When are - especially in healthcare but generally speaking - people going to take this seriously and realise that the catastrophe is now? This is life-threatening stuff.

Martin Curley

It's a great question. Obviously they were seriously evil and sick people that did that.

Davey Winder

It was security researchers who were proving the concepts. They were showing you how dangerous these IoT devices are.

Martin Curley

I missed the start of your preamble. We had a ransomware attack a couple of months ago and it took the entire senior leadership of the IT team to work for a week to fix the issue and do all the backups and restores. I think the particular issue in healthcare, there's a systematic problem in that the relative IT intensity is very low compared to - financial services are spending about 15 per cent of their revenue on IT whereas in healthcare typically it's about 3 per cent of the overall spend. It's just such a paradox because healthcare is the most information-intensive industry in the world.

The problem I think is down to under-resourcing. Particularly in my own organisation the IT intensity is about one per cent. There's barely enough staff to just get the systems functional never mind thinking about security. I'm certainly going to look for more detail on that and bring that back to my own organisation to make a case for increased funding in security.

That clearly is a catastrophe waiting to happen. In the hands of the wrong people it could be catastrophic. I don't have an answer. I acknowledge it's a problem. I think there's systematic underfunding in healthcare.

Jan Guldentops

Can I pick into that? It's one of the best innovations within the security industry in the last couple of years how we created bug bounties. There are a number of companies running bug bounties, so you can get a community of people who like to get into your system but not break it, who do it as an intellectual challenge. So, they can report their problems, earn sometimes a living with it.

It's something we should start using also in IoT. If you're a company developing a device and you want to put it on the market, hire one of those bug bounty companies and get some people to play with it, to break it. You're going to be happy that you know there's a security problem in it before you roll it out to 10,000 people.

Philip Griffiths

To your question, what we need is a high-profile incident that everyone sees. Recently I've been twittering about Triton, which is a type of malware that's being used to infect industrial control systems which are literally put in place to stop a runaway chain of events from causing catastrophic incidents.

There was an incident last year in Saudi Arabia where there was an execution of this malware. If there wasn't an incorrect syntax issue in their code it would have caused an explosion that would have killed at least hundreds of people in that site. Recently they found this same malware on other industrial control systems in manufacturing businesses around the world. I personally see Triton could be that malware that creates that news article where people say, people are actually being hurt by this now and we need to take it much more seriously.

Davey Winder

On the bug bounties, that's good. I'm all for dealing with the [defsec oops] issue, but in healthcare in particular but across industrial IoT it's the legacy problem that is the real problem and bug bounties aren't going to solve that, because those devices are already there. They can't be patched or it's inefficient to patch them, it's too costly to patch them. How do you deal with this legacy problem?

Philip Griffiths

That legacy issue you need to solve with a secure greenfield overlay. In fact, Jan and I were talking last evening because he's working with this company with the speed cameras who are - we can't patch our operating system. So, we're thinking, how do we throw NetFoundry on there in order to secure that so that someone can't get into it? They've still got that underlying flaw but you at least layer over a more secure solution on that so you make it much harder for someone to get access to that and root password it.

Jan Guldentops

It's the problem of the embedded XPs in medical devices. There are masses around. These devices are bought for 20, 25 years. You invent a way of shielding them off. You don't have a choice. It's something you can do and you can do that with something like NetFoundry. You can put a Citrix front-end in front of it or [in a ring] [unclear]. There's a lot of stuff you can do but you cannot fix the fundamental problem.

Davey Winder

Which begs the question, why isn't it being done?

Michael Kagan

I think there are two - legacy, whatever, done is done. Moving forward I think we need to really identify and understand the interfaces between different blocks and not mix too many things together. The example I was using in my presentation about the segregation of the infrastructure computing and application computing enables you to pitch or update these two tiers absolutely independently. With the various devices or architectures that we are developing moving forward we need to keep this in mind. Don't tie things too much together so you can update them and manage them and provision them independently.

Philip Griffiths

To your question, why hasn't it been done, most people don't know that it's possible. I was at Hannover Messe a few weeks ago. Last year at IoT Solutions World Congress, when I talk to people around silicon [to] trust security using zero-trust software-defined perimeters based upon getting hardware certificates and other roots of trust, they go, wow, I can do that? That's awesome. How can I use that to secure my brownfield system? But they just don't know it exists.

Jan Guldentops

It's a management problem. It's basically a CEO or a director of a company - the general director of a company should know how security works. From a simple quality PDCA approach, plan-do-check-act approach they should be able to know they have to plan it, do it by design, check it, have security operations. I've been doing these talks for 25 years, I guess. It's still not here. We could use my old presentations still, I guess.

Steve Broadhead

Steve Broadhead, broadband Testing and all the other things and pieces. IoT as a concept for me frankly is ludicrous in the sense that you'd have kettles and lifesaving machines and industrial billion dollar - sharing the same network? What is that about? What is wrong with some proprietary technology that is 110 per cent secure?

Jan Guldentops

But that's security by obscurity. If you make it proprietary it doesn't mean you cannot reverse-engineer it.

Steve Broadhead

But there are benefits to having properly designed independent systems to control stuff, unless you're Boeing obviously in which case you don’t need security anyway because they just build in automatic failures. It's just a silly concept, it really is.

Kevin Restivo

We're running behind schedule now so I think we'll cap it off with that comment. Thank you, panellists.

[end]