Deepa Kundur: Fall Alumni Networking Reception 2015

Professor **Farid Najm**: Good evening, and thank you for being here. My name is Farid Najm and I am a professor in the Electrical and Computer Engineering Department, and Department Chair at this point. It is really a pleasure to welcome you back to our annual Fall Alumni Networking event. This is probably our 3rd or 4th year that we've had this event. I enjoy this event, it is a chance to meet Alumni and see what you all are doing. It is also a chance to network and I find that Alumni enjoy networking with each other so that's always great to see. We've been doing some exciting things on this end, just to briefly update you. If you attended last year you may have heard me speak about our Energy Systems lab renovation. This is a long process - it is a 3 stage process. We've done stage one was in 2014, stage two in 2015 and next summer hopefully we will finish stage three. We basically renovated the whole lab. If you remember the lab, the power labs, in the Galbraith basement, there is a back room that produces all the voltage supplies for the whole lab and that was circa 1950. So we have renovated that stuff now and it's up to code, thank God [laughter]. But that was the first step, we completely renovated the back room, it looks clean and modern and safe. And then the second phase was to redo the wiring, so we pulled the wires out of the conduits and wired all the new supplies to all the workstations and we had custom-made terminals and display units at the workstations. Now there are no more exposed plugs, you don't see metal, so again we are very happy with that. Between phase one and phase two, this was probably a 1.5 million dollar project and now we are going into phase three which is to renovate the experiments and the equipment. So we are going to focus on modern smart grid technology which mixes power and communications, hence our topic for tonight. So, it is my pleasure to introduce Professor Deepa Kundur. Deepa is an ECE professor and Director of the Centre for Power and Information in the Department. She also serves as Associate Chair for the Division of Engineering Science. Deepa is a native of Toronto, she got her Bachelors, Masters and PhD all here from this Department. She taught here for a couple of years and then she went to Texas A&M, where she enjoyed the BBQ, I assume [laughter]. She was there for 10 years in which time she participated in a lot of the work that has been going in the states on power systems and power systems security, helped define standards, etc . And we were lucky to have her come back to Toronto, about 3 years ago. So she is now back here as a professor in the department. Deepa's interests include cyber security, signal processing and complex dynamical networks. She will tell us what these are, I think. She is an author of over 150 journal and conference articles. She is a recognized authority on cyber security, and has appeared as an expert speaker on TV at as well as radio and print media. She is currently an Associate Editor of the IEEE transactions on Information and Forensics Security. She's been the recipient of several best paper awards and teaching awards at both U of T and Texas A&M. She is a fellow of the IEEE. Please join me in welcoming Deepa Kundur.

Deepa Kundur: Thank you very much. It is a pleasure to be here. And as Farid mentioned I am a triple alumnus of the Department so it actually has a lot of meaning for me to be here at an Alumni Reception for ECE. Farid mentioned I have been a faculty member twice, with a 10 year gap in the middle. I'm not sure if some of the alumni here were taught by me between the period of 1999 and 2002. There we go – at least one person. I recognize you – wonderful! Probability? Signals and Systems? Yes, wonderful. Please come up to me after the talk, I'd love to talk to you after if I've taught you before. So as Farid mentioned I am Associate Chair of

Engineering Science, and what I'm very proud of, and has been possible due to the support of Professor Najm and the Department, is we're establishing a Centre for Power and Information. And basically my talk is going to talk about what my work and research within this Centre really involves. And it really looks at a number of different things. For example, my work looks at cybersecurity issues, looking at the integration of renewable energy, making this emerging power grid more efficient, reliable, higher capacity. So we have a number of core faculty from different areas and departments. It's not just the Energy Systems Group, although they are very important. We have members from the Computer Engineering Group as well as the Communications Group as well. We also have a very nice web page that Marit, who is our Senior Communications Officer, has put together for the Centre, so if you're interested there is more information on the web page about that.

Now, I was really excited to give a talk but I was a little apprehensive because I noticed that the Department tagline for this, it said "Come back to Skule for a stress free lecture and networking reception". Now the stress free part concerned me because I'm in the business of stressing people out to motivate my work. So it's sort of an area where you are essentially defending yourself, trying to think like an attacker to defend yourself, and you somewhat have to be in a semi-state of paranoia to be able to do good work. How am I going to address this sort of challenge and I thought well this is really a high class problem trying to cyber secure something and it's because we have systems that are emerging that have advanced instrumentation, that are interconnected and that have intelligence. And a lot of this really stems from having amazing ideas technically and also have amazing ideas in terms of applications and what we can do in the future in terms of society. One of the end results of a lot of the ideas is this whole smart movement, this intelligent technology movement is this paradigm of smart city we're looking at. And smart cities really are defined as "using information and communication technologies (ICT) to enhance quality and performance of urban services, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens." So this is really a utopia we're envisioning where we're harnessing technology to make things better. And a large part of this really is the infrastructure, and what I'm going to focus on today is the energy infrastructure, the power delivery infrastructure which we call the smart grid. The smart grid if we look at in a more detailed way has a number of different components. There was motivation to this movement and the movement has started, it's international, China is a leader, the United States is a leader, Canada is a leader as well. And we're really looking at taking the existing power delivery network and enhancing it. Basically enhancing it by making it more consumer-centric and I'll talk a little bit more about what that means. Making it more reliable – it is reliable now but as we start moving towards adding renewable energy sources like photovoltaics and wind, reliability becomes an issue. We're also looking at making it more efficient. Energy needs are increasing. More and more we are a generation that makes use of our portable devices, our digital devices. So we're living in this digital world and everything has to be powered up. So our capacity needs are going up and so efficiency needs are very important. Economics are also important, making things accessible economically to people, and sustainability which is a big thing, reducing our carbon footprint.

So what does it mean this smart grid? You can think of it in very simple terms. We can think of it basically as a system where you marry two things – information and communication

technologies with the electricity network. And why do you do that? Well it really allows this bi-directional information transfer and bi-directional energy transfer. That opens up a host of possibilities on how to harness this information and how to harness the fact that you can now sell, not just consume, energy as consumers. So there is a more formal definition and we're all engineers so you can probably value the fact that 20 of us got in a room basically for 4 hours and we finally came up with a definition (still debated to this day) of what the smart grid is. I was part of a task force known as the North American Reliability Corporation (NERC). It is in charge of regulating a number of things – the reliability practices as well as the cyber security practices of utilities in North America. So we all got together and we realized that this was a definition that we were all somewhat comfortable with. The smart grid is the "integration of real-time monitoring, advanced sensing and communications, utilizing analytics and control, enabling the dynamic flow of both energy and information to accommodate existing and new forms of supply, delivery, and use in a secure and reliable manner and this is from generation source to end-user." So if you look at this definition, it's quite dense and basically what we say, especially in the IEEE, you are probably aware that we have here a power and energy society, and what we basically say this definition says is that everybody's in smart grid. It doesn't matter what type of computer or electrical engineer you are, you probably have knowledge that will contribute to what we need to know to move towards this advanced smart grid. So what that really means is that you can basically look at our traditional system which involved bulk generation - that bulk generation, which is geographically separated from where it is consumed, at the consumer end. That energy is transmitted through a transmission system and it is done at a high voltage to be able to reduce loss and make it more efficient, then through a sub-station it is converted to a distribution component where the energy is made more accessible and in a form that consumers can actually make use of. So this is our traditional system. But when we start integrating information and communication technologies it opens up a host of possibilities. We have markets, so we can do advanced things in terms of the markets, the economics, pricing of energy. Operations becomes more advanced because we have more information, more timely information, and other people, other stakeholders can be part of the smart grid and they can sell and buy energy as they couldn't before. And it's opened up a number of applications – there's smart metering which I think has probably touched everybody in this room - which leads essentially to home automation.

So now your smart meter is the home's connection to the utility and that is the portal into your home and helps you regulate how your appliances are working and helps you reduce your energy costs. Billing and real-time pricing is another advantage of this. And also this whole idea of advanced monitoring of the operations of the system to make it more reliable and efficient. So, the smart grid vision, everyone's got a vision for it, ranging from the European Union to IBM, for example. And so when I first embarked on this research I thought where do you start, everyone's sort of got a different definition. Two things are clear that stand out in almost everyone's vision and the first is that the smart grid has to be participatory and open. It's about making it possible for people to produce energy and sell it back to the grid, make it possible for people to use the energy they produce and all second it's about making it more consumer-centric. And that is to be able to provide choice for consumers in terms of their energy needs – what they want to buy, who they want to buy from and to empower them with knowledge so they can make effective decisions for their home. So if we see these two things, Open and Consumer

Centric, what does that mean, this is why you need information. You need information about the right thing to the right party at the right time. So we need: telemetry – sensing; communication – so basically moving this information around quickly to where it needs to be; computation – to be able to use this information and; control – to be able to regulate the whole the system, because the overall goal of the system is power delivery and it operates if there's balance. And by balance we mean if that supply and demand match. So this lead us to cyber-enablement, which is why we call it a smart grid. Now the interesting thing is anytime you cyber enable something, security issues arise because we start to depend on information, computation, essentially computers, so we have to be very careful as to what the effects of cyber- attacks can be on these systems. So there are many motivations to protect the grid. First of all because we're dependent on these information systems in a growing way there's increased opportunity. There's increased motivation as well, that makes people want to hack into these systems. Also, people are now buying and selling energy from their homes. So, there's motivation having to do with energy theft. Everyone's got a smart meter, some people may think, wouldn't it be nice if their usage ended up on somebody else's smart meter bill rather than their own. So there are all sorts of motivations. Of course there's public welfare, this is a critical infrastructure, so safety is always an issue. And it also makes business sense. The interesting thing is for anyone who manufactures smart grid devices they have to have security. Basically for the utility to be compliant, the functionality of a lot of these services and devices has to include security. So to be able to produce a smart grid device you need to be able to include security, so it makes business sense as well.

So if you look at securing a system, where do you start? The nice thing is this is not the first system that has been cyber-enabled. And there's been a multitude of systems before that. For ex., commerce became e-commerce so it provided the greater consumer and vendor-centricity. So it has created new business models. We don't have to go physically into a store, we can buy online, we can do banking any time of the day. The entertainment industry has seen this as well. We have cyber-enabled so now we have a digital entertainment movement. So business models have changed. For ex., you can buy a single song instead of an entire album now. And even friendship. Social networking allows us to connect with people whom we couldn't before, because of their geographic location. So all of these things have been fantastic and cyber-enabled and we see that security has been an issue. In terms of commerce, impersonation has become a bigger issue because you can do it remotely now, off of a computer, you don't have to go and sign something because everything is digital. Entertainment – piracy – theft of content became an issue. And friendship, there are issues of privacy we hear about in the media every day. So from securing these systems we learned many things. What worked and what didn't work. We can think of them in terms of three things. Cyber security should be part of the system design. And this is good. Because right now we're at the stage where we are moving and cyber-enabling the power grid. So designing in security is very important, it's critical in fact. Cyber security is a support service that should not hinder usability. In a lot of ways we depend on people to make use of the cyber security techniques that we have integrated into the system. And the more useable we can make it the more we can guarantee that people will make use of them. Often people get frustrated with cyber security techniques that just are not very user friendly. And so it's funny, people find ways to circumvent that. Cyber security is also a process, so unfortunately there is no one technology we can develop that will completely secure a system forever. This is a

situation where you have technology constantly changing, the threat landscape is constantly changing. And because it's a very dynamic environment, it's really important that cyber security be continually re-visited. Now what makes this problem different is what we call the Cyber-Physical Interface. So in the other applications, the e-commerce, the social networking, the digital entertainment, there was a little bit of a cyber-physical interface. So by physical we mean the real world, there was the human with a computer basically. But what makes the smart grid different is that the cyber-physical interface is distributed. It's complex, it's highly connected, so you have not just information connecting, computers connecting, it's not an information system that is connected, you have the physical system that is connected, and by physical we mean the actual power delivery system, the transmission lines, the transformers. So you have a strong physical coupling that's involved, which are governed by the laws of physics. And, you have a lot of collaboration going on. Everything has to remain tightly in balance with supply and consumption matching.

So what's interesting is, any time we increase the complexity of something, we increase the number of flaws. When we add connectivity, we unfortunately also increase connectivity, access to the flaws. And when we start collaborating, so we give people accessibility to share resources, it becomes possible to exploit flaws that we didn't before. Now with all those three things, at the interface of those three things, if we have all three things, it's defined as a vulnerability, in security terms. So this system will have vulnerabilities just because of the nature of it. So this moves into the area that we call cyber-physical systems. And for many of you if you know the whole digital movement it started with the computer, and then computers had to be networked. There was the whole internet generation. And then in terms of, we started with the whole smart environments, the whole sensor networks. Now we're seeing a movement towards cyber-physical systems. What they're defined as is a tight integration and coordination of the cyber and physical components. And we've always had this but it's at a much higher degree and a much more integrated scale. And really the advantage is it's supposed to improve our adaptability, our autonomy, our efficiency, our functionality, reliability, safety and usability. And depending on the type of system you're looking at, some of these characteristics would be more important than others. Examples of cyber physical systems are, of course the smart grid, robotic systems, medical systems, so it's really an emerging scenario. And of course anything having to do with a smart city where you're dependent on communication and information technologies. So if we look at securing these systems we have to look it at from two different perspectives, there is the information system, which sort of acts as a central nervous system. We need to look at cyber security of that. And if we look at the definition of cyber security it's concerned with securing the safety of computers and computer systems in a networked environment. And you break it down into three services you generally have to provide – confidentiality, integrity and availability. Now if we look at what security means in a physical context and those of you who are power engineers may be very familiar with the definition of power systems security. It is defined as the degree of risk in a power system's ability to survive imminent disturbances without interruption to customer service. So it's a very different definition that incorporates the objective of the application. And from the perspective of the power grid, availability is most important, availability of power. The fact that information doesn't have integrity and confidentiality doesn't matter in the situation that it doesn't affect availability, that's the ultimate goal.

So we're moving into this area where cyber security has to have a more comprehensive definition. So we're starting to look at what we call cyber-physical security that integrates both of these definitions. And what it involves is employing strategies at both the cyber system and physical system, so this would be our communication and information system, as well as our physical system, so we're looking at our traditional power system components. Our generators, our transmission lines, our transformers and employing strategies in both those domains to be able to provide security, reliability and resilience. So what's interesting is what combines all of this is a risk analysis framework and as engineers we are always interested in risk because we're often designing systems in order to accommodate the appropriate levels of risk. Risk as we all know is the product of the likelihood of an unwanted event and the impact of an unwanted event. And we can even break down likelihood into terms of the likelihood of threats times the likelihood of those threats exploiting vulnerabilities times the impact. And what a utility would want to do is estimate all these quantities and actually manage their systems such that unwanted risks are driven down. You would want to get out this region where risk is high and go into a lower region. Now the problem is, it's unknown at this stage, because the system is new and constantly evolving, what the impacts of a lot of these unwanted events, especially if they're related to cyber-attacks, are. So there are really some fundamental R&D questions as well as fundamental questions we have as engineers, those who are working in power industry, with respect to this field. First of all, we really need to know, what are the electrical system impacts of a cyber-attack? We still don't know because we're integrating these components and to be able to understand how it affects the grid, requires an entire system perspective. Second, how should security resources be prioritized for the greatest advantage? Cyber securing a system, especially one that's evolving, the legacy components are monumental.

So utilities really need to know, where is it best to put their money for the best outcome and what cyber physical mechanisms enable greater resilience? Thinking about what we should be concerned with. If you talk to an electrical utility, most of the engineers say they are concerned with about three things. Information that has to do with their telemetry systems. So they're concerned with attacks on information accuracy, so they don't want false information going in to the system and affecting how the system operates, because decisions are made on this data. They're concerned with attacks on access control, so a lot of devices in the grid allow re-configuration, so allow energy flow to change for the purpose of balancing supply and demand. So now that these are being automated and cyber enabled, there are problems with the system, if hacked into, being able to reconfigure automatically. And that can have profoundly dangerous effects on the grid that it couldn't before. Because before, that weakness may have existed but access to that weakness because things were not automated and connected to the internet, were not an issue. And also we're concerned with timely delivery. When you start depending on information, that information needs to be where it is on time and so there's issues with we want to avoid denial of information and delayed information.

So I won't go into technical details but I'll talk a little bit about what my group is doing in this area and it's really motivated by the vulnerabilities we see existing in the system. Before we can secure the system we need to know what vulnerabilities exist. And really it comes about, as I mentioned before, because it is a complex system that is connected and collaborative, so we have flaws, access to the flaws and ability to exploit them. So we have vulnerabilities. So how do we

start? It's important with a system that is so interconnected, as we have in the smart grid, where you've got the cyber world as well as the power delivery, the physical world, to be able to see what the couplings are in the system to see where cascading failures can occur. So modeling is very important and there's many ways to model a system. So what we try to do is take a holistic view. This is what the industry is doing, attempting to look at both the power delivery system and the information system and their dependencies together. And this is called cyber-physical modeling. And so if we wanted a nice model it would have to be: simulation-friendly, design-friendly, visualization-friendly, it should enable vulnerability analysis, it should give this idea that the grid can heal itself. So we need models that will help us design a better grid. So there's many types of models. The power industry has been using dynamical systems models for many years. The computing industry has been using graph-based models for many years. So what we essentially do through our collaborations with various partners and our peer research projects is we look at combining these tools in a very effective way. And there's different ways to do that. You can come out with a number of different tools that you can use. So the dynamical systems have the advantage that they model physics very well. In fact, ODE's are usually the result of an exceptional model and we deal with utilities where they spend 20 years coming up with fantastic high order ordinary differential equation models. Graphs are a very compact, convenient way to represent relationships. And we have a lot of relationships that need to be represented in this system. So if we can combine them, it really results in a lot of interesting things.

So I'll just talk briefly about some projects that we're working on. We talked about securing these systems, so I'll talk a little bit later about cyber security issues. But one of the first things we have to do is if we can protect the system, and use technologies like cryptography, and that involves encryption, digital signatures, we can protect and prevent attacks of the information system. Unfortunately as we all know, those systems can be broken into, the protection mechanisms can be broken into. Because the threat landscape is constantly changing, technology is constantly changing. And so it's possible, then, if someone breaks in, we need to detect and react to this. And to be able to do that in sufficient time, we need the system to be resilient. And by resilient we mean that the system has to be able to bounce back and gracefully degrade during the face of an attack so that we can detect what's going on and try to recover from it rapidly. So resilience really has to do with making the system still operate in the face of a very severe disturbance of some sort, especially a cyber-attack. So we look at strategies to use control and control is interesting because it takes information, it makes decisions on it and aims to regulate the system to be able to get that supply and consumption balance going on. And so we use all sorts of models based on flocking theory, and game theory to be able to do this very effectively. So for example, here, we utilize storage devices. So we're talking about the importance of storage often, so renewables are important, but renewables create a lot of intermittence from the system. Storage helps add more regulation into the system, inertia into the system, so we're looking at how to do that more effectively. We're also looking at, should we distribute this, do we keep it centralized, what kind of strategies are most effective in this context. So we do various studies to see what ultimately makes things more resilient in the face of a cyber-attack. Because if things are centralized you have better situational awareness, you can make better decisions, but you have a single point of failure. If they're distributed, you are more robust to cyber-attack and there is a trade-off there that we try and find. Also, we look at strategies, what's the minimum amount of an information system we need to make use of that

will make the system fairly resilient and efficient. Because every time we add a sensor to the system, it is important that it provides information for decision making. But, it's a point of cyber-attack. So at some point you keep adding sensors to the system, they start to become liabilities. Because you don't need any more information, they will just become redundant, but they become a potential vulnerability in a system because they can be cyber-attacked. So we look at strategies to figure out at what point, instead of harnessing the information system, can we harness the robustness of the physical power delivery system itself.

Another interesting area looks at micro-grids. Micro grids are basically systems that tend to be stand alone, they could connect to the main power grid, but they can also operate in stand-alone mode and they have renewable resources or distributed generation and loads that are very local. And the idea here is that they can operate either full, or at a partial capacity, by themselves. And this provides a lot of resilience especially if something happens to the main grid. And there's a lot of activity in looking at micro grids, especially, not just in urban areas of course we have access to the main grid, but they're looking at them in a variety of places especially when the main grid may not be available. So we're looking at networks of micro-grids and how to connect them for overall resilience and make them robust to cyber-attack. Another thing we're looking at is if you look at cyber security, we're trying to take a balanced approach, looking at the cyber system and the physical system, we could just look at advancement of the cyber system. For those of you who are in the communications area, there is this new field called software defined networking that's emerging. And industry is very much embracing this idea. And the idea of software defined networking is it provides you, essentially, you know the decision making and routing of information, as well as the actual process of routing are separated, so you can do it more effectively. And there are very effective ways to use this paradigm to be able to use this paradigm to be able to make information more reliably transferred in a smart grid operations environment. So we're looking at those strategies and seeing what kinds of paradigms are better for smart grid. Because in a simple, normal telecom situation you need information flow to be fast and reliable. In a smart grid it is very different. You need information to flow in different directions and there has to be synchronization involved. Because decisions and control has to occur in a very synchronized way. So different parts of the grid have to make related decisions. So networks like this allow you to have fast, reliable and synchronized communications.

There are other applications that need to be secured. We can call it demand response. Many of you may be familiar with this – this gives your appliances the ability to turn on or off pending on the price of energy at a certain point. Again, you're starting to depend on information and these systems need to be secured. As well as we have a photovoltaic cell. At what point is it acceptable to dispatch, for the utility to dispatch that particular source of energy into the grid, so that you can sell energy and make use of it. And also we're looking at homomorphic encryption. The interesting thing is we all hear about the cloud. And the idea with the cloud is you basically make your information responsibility someone else's problem. And they can do it very well because they are providing these information services and they can do it in a much more cost-effective way because they have many people who need those resources and so it's a situation where they can balance a the needs of a number of different utilities or organizations and be able to offer either application services, or computation services at a very cost-effective price. The thing with utilities is that they're very concerned with going to the cloud. There's a lot of

economic advantages but when you're dealing with utilities they have a lot of private information. For example, consumption information. Anything coming out of the smart meter is now highly granular. So basically you can look at meter readings from a household and learn a lot of different things. You could learn how many refrigerators they have; you can probably estimate how many people live in the home. So, because this information really can be very revealing, and it's very different from the old meters that would have an aggregate result at the end of the month, you could tell a little but not a lot. Because of the granularity of the information we're now using, privacy issues arise. So utilities are scared to go the cloud. One strategy is, everything is encrypted all the time. So it's encrypted at the meter and if it goes to the cloud, it's still encrypted and nobody can really get access to that information. The problem is utilities and cloud providers need to do things with that information. So there's ways to suit your encryption so that you can process and do those interesting things in the encrypted domain. And that's called homomorphic encryption. So we're working on that with London Hydro. And of course, simulation. Many of you may be involved in simulation. So the last thing we're looking at is simulating the communication grid, the power grid, the control and simultaneously trying to get a very nice understanding of how the three operate together. So thank you very much (applause).

Farid: Deepa this was great. We have time for a few questions, if folks have questions.

Audience member #1: Given that the power network is already heavily connected over distances and all the components, why would you use the internet at all for the command and control systems and not just build a private one?

Deepa: So, they're not as connected as they'd like to be. You're absolutely right. That's why in the beginning I said it is a smarter grid. Today it is smart; it does have some communication capability. But, for the type of sensors – they want to move towards these very expensive phasomeasurement units that will look at providing voltage, current readings, phaso, so magnitude as well as phase information of the voltage and the current and you're looking at something in the order of 200 samples per second. So you tend to need high speed communications for this. Also for a lot of the applications – of course, we hear a lot in the media about using the smart meter data but there are also applications that arise from using the telemetry data using these phasomeasurement units. How you could do advanced control because of the higher granularity, you have the sensors and you're able to connect them in multiple distributed locations. So to answer your question, you're absolutely right, it's connected today but they need even more connectivity to be able to achieve what they want. Especially when you start integrating renewables.

Audience #1: They already own most of the rights of way. Just running a fiber line over the same rights of way over there, you can get as much connectivity as you need. Why expose yourself to the internet when you could just as easily….

Deepa: Oh I see, the internet was an example. So, the thing is, you're right, there is a lot of fiber that occurs. At some point you have to get wireless, utilities for example, at a substation prefer wireless. The reason is that it is cheaper and simpler. You are right, there may be fibers along the transmission system because it is convenient and it has been previously deployed, but at

some point you are going to avoid that medium and you could even have fiber be compromised as well. But at some point it will become wireless and so that really pertains to systems that have to do with operations. Like Scata, the fiber and the wireless. You start to see internet when you get to the smart metering part of the system. The whole part of the smart meter is in some sense, consumer centricity. So when you want to connect to the consumer, you have to give them internet access. So these systems start to be connected to the internet at that point especially.

Audience #2 : One of the core problems I see right now is all this conservation. The utilities don`t really like it because it reduces their revenues. So I think right now I see they are working on more smart metering, washing machines turn off at certain times, etc., etc., but the core problem is that they can't afford to have their revenues drop. It feels to me that we're probably 10-15 years away before we're going to see it in practice.

Deepa: You're right, the economics is a long term type of thing. So the benefits will be seen in the long run and that's why you have the government trying to provide incentives to utilities and consumers. There is that initial investment that has to occur. But ultimately, you can think of it in this way, these technologies not only make it cheaper for the consumer, but ultimately aim to make it cheaper to generate and transmit and distribute energy. And you can think of it in a very simple way, the demand response makes it cheaper for the utility because the power plant has to be generally designed to be able to handle peak load. When I was in Texas it was Aug. 15th, we knew, it was the worst month of the year, everyone's air conditioning is up and you had to buy energy from Mexico. So we have similar problems in Ontario, as well, but with applications like Demand Response, the idea ultimately is to benefit the utility. So you do motivate consumers, economically, to turn off their appliances, but you do it for the purpose of making that peak go down. So you have a typical peak and you try and flatten that usage. So ultimately, running their systems becomes effective. Because as the need to generate increases, there is a certain point at which it now becomes a loss to be able to serve consumers. So that's the ultimate holistic goal.