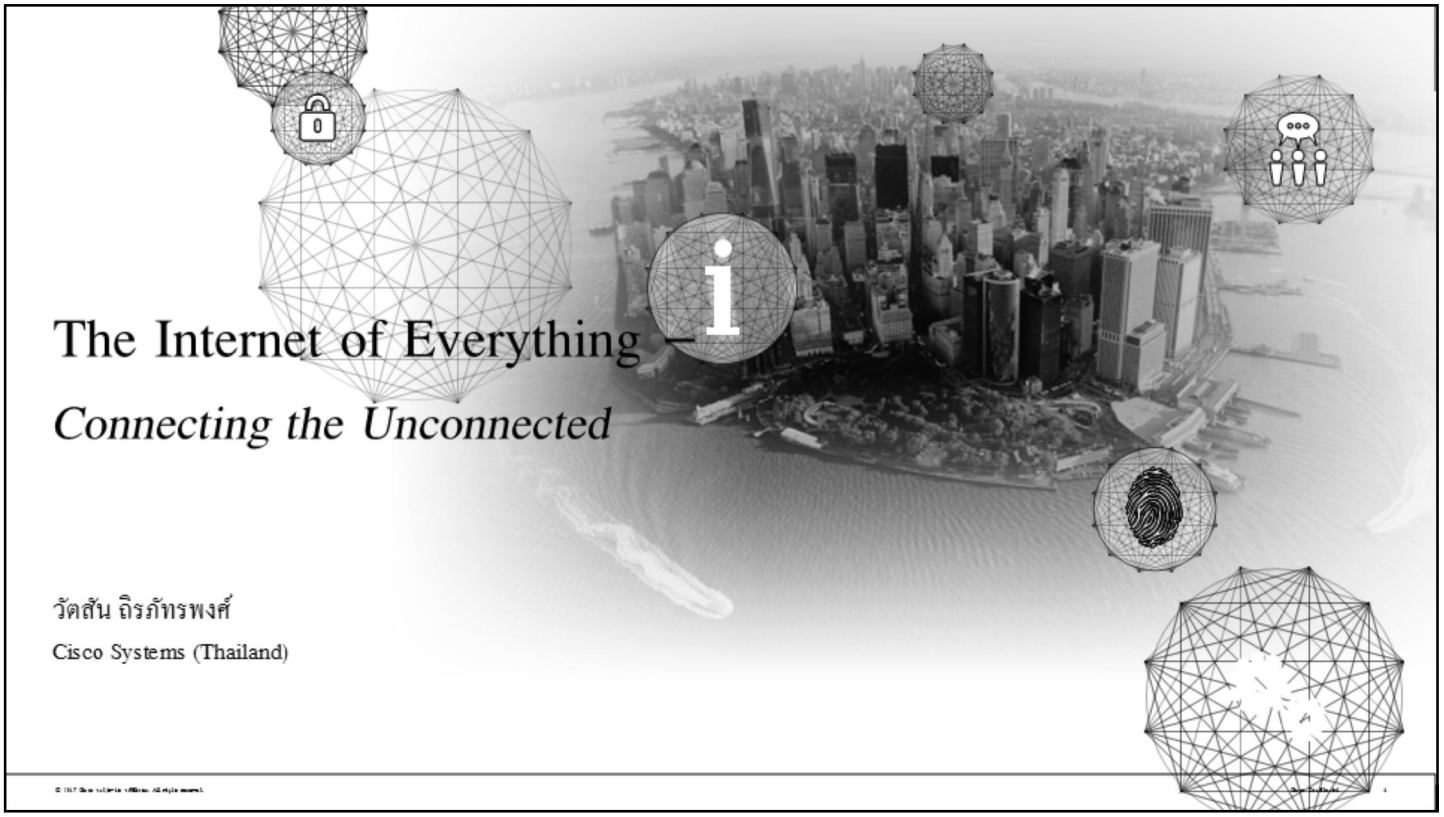
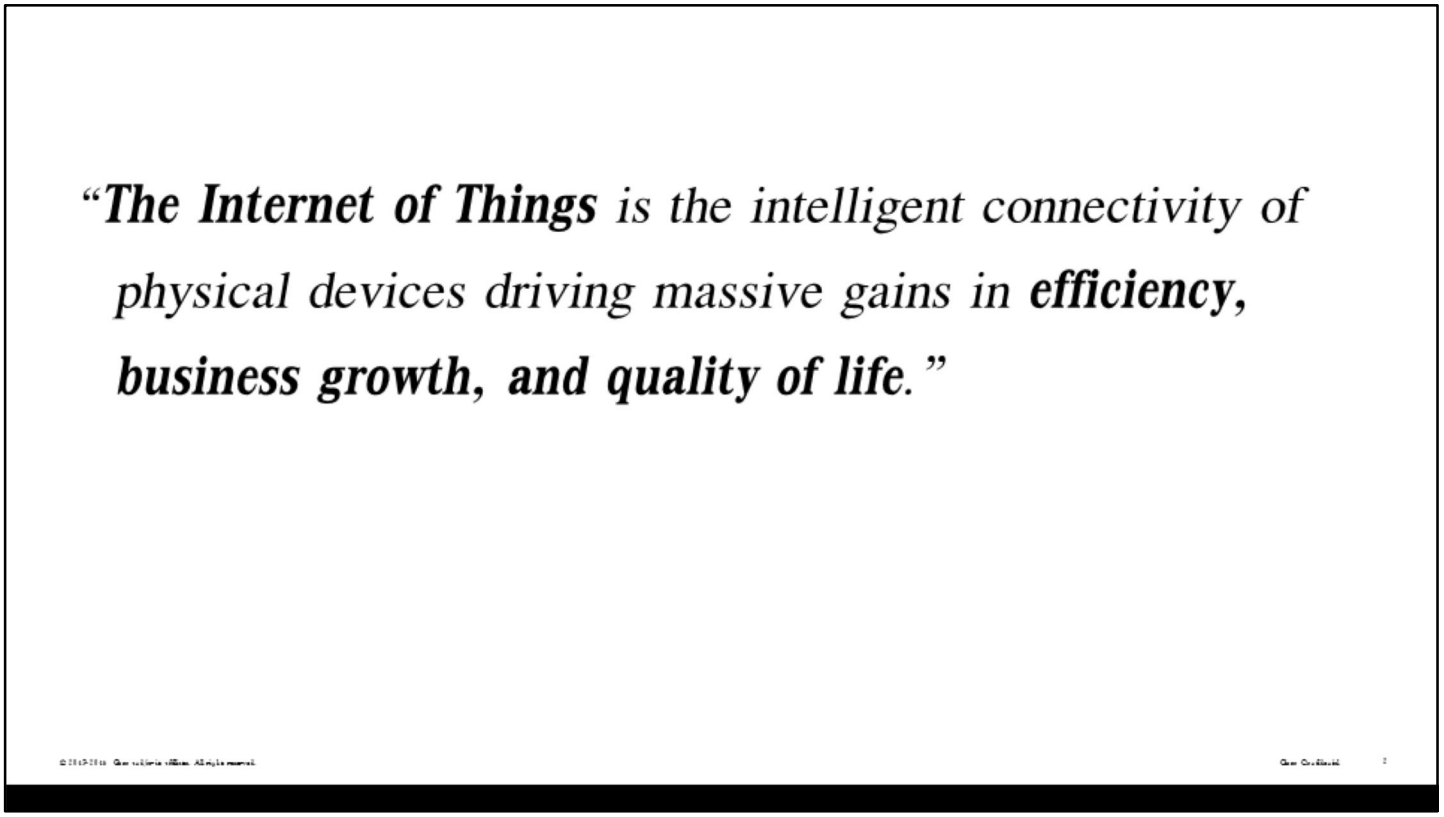


The Internet of Everything – i

Connecting the Unconnected

วัตสัน ถิรภัทรพงศ์

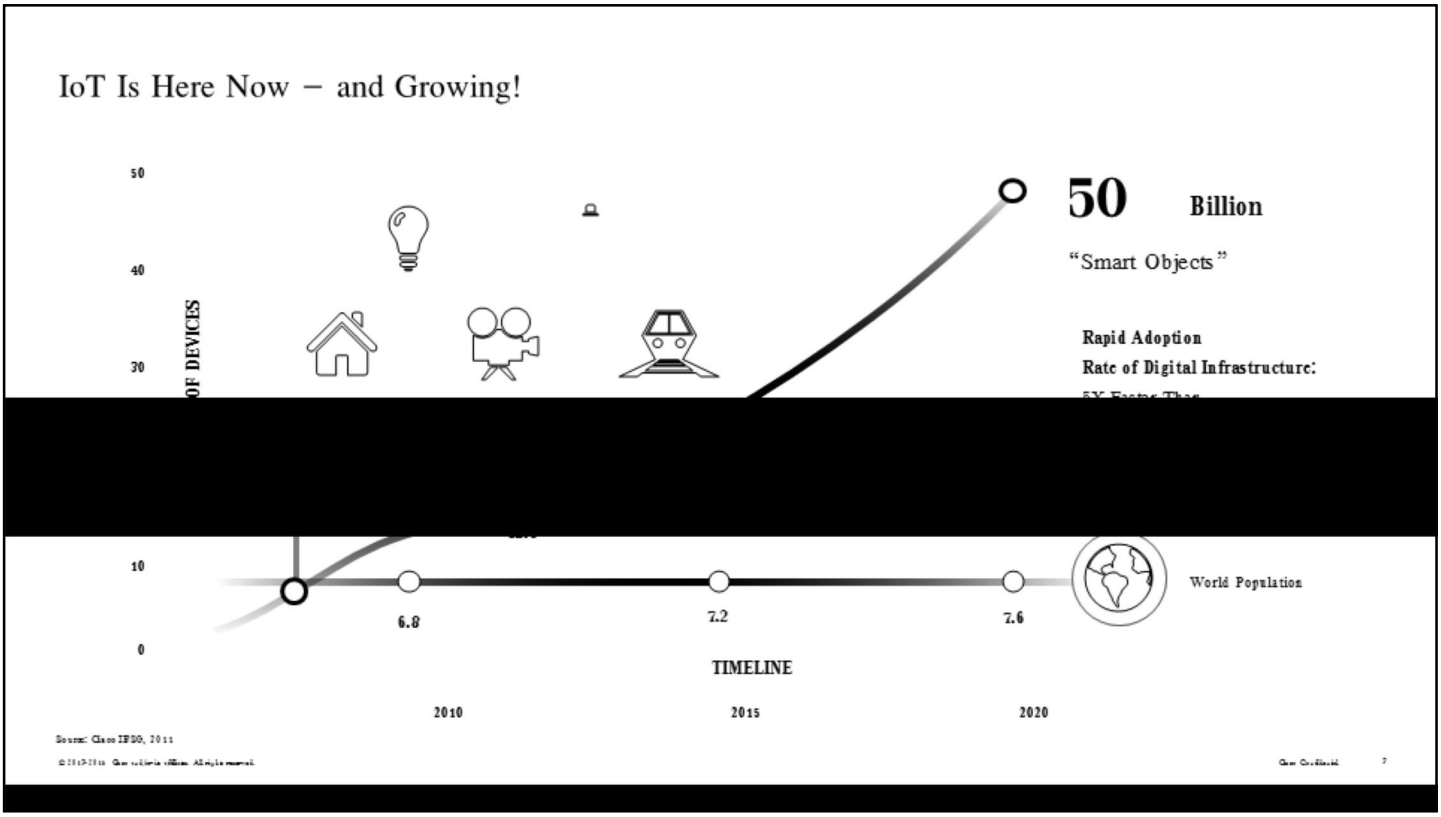
Cisco Systems (Thailand)



I want to take a moment to provide Cisco's definition of IoT, to ensure we're on the same page …

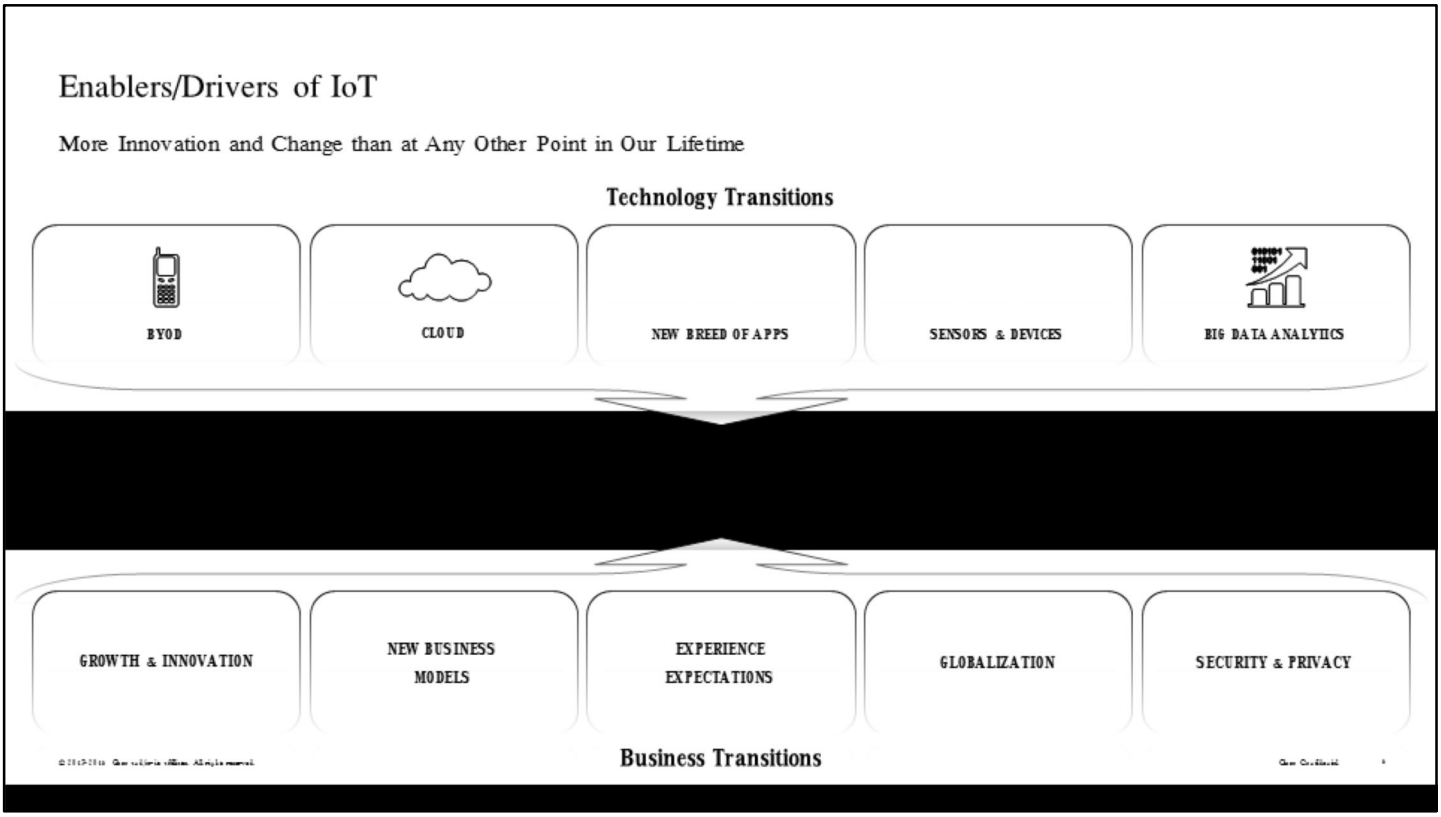
To put it more in context of what it means for your business and for your daily life, this highly distributed network of **connected smart objects** is capable of dynamically **generating, analyzing, and communicating intelligence** that can be used by businesses to **increase operational efficiency** and **power new business models**, and by individuals to **make life easier and more comfortable.**

... by connecting everyday objects and networking them together, we benefit from their ability to combine simple data to produce usable intelligence.



Sometime between 2009 and 2010, there was a point of inflexion, where the number of connected devices began outnumbering the planet's human population. And these aren't just laptops, mobile phones, and tablets – they also include sensors and everyday objects that were previously unconnected ... so IoT exists today in a very real way! More importantly, the gap is expected to widen exponentially over the next several years – with the number of sensors, objects, and other "things" exceeding 50 billion by the year 2020!

Adding all of these physical objects to IP networks imposes new and novel requirements on existing networking models. IT will need to deal with those requirements in relatively short order.



So how did we get here?

IoT is the result of a long line of technology and business transitions that have been taking place over the past several years.

- Five major technology transitions have been impacting companies, organizations, and consumers:
  - BYOD: The ability to access the network anytime, anywhere, using any device has resulted in massive gains in workforce productivity
  - Cloud: the shift to cloud computing has created new architectures, applications, control points, services and business models
  - New Breed of Applications: the fundamental shift from Client/Server to Mobile/Cloud has dramatically expanded the capabilities and accessibility of applications
  - Sensors and Devices: billions of previously unconnected objects are becoming connected, forming a network of sensors and other devices. While each of these "things" generate data, the fact that they are networked together enables that data to be combined with other data points to produce usable intelligence.
  - Big Data: the billions of devices are generating massive amounts of data which is now processed and analyzed to power real-time intelligence and rapid decision-making

- These transitions and other macroeconomic trends are impacting businesses such that organizations care about
  - Growth & Innovation: capitalizing on growth opportunities (open new markets, increase penetration, etc.) and increasing innovation & productivity to address these opportunities more efficiently and in a more agile manner
  - New Business Models: having / developing more flexible consumption models; capex-based → more opex-based models (e.g., adapting to mobile and cloud delivery / interaction, outcomes based, accelerating service creation)
  - Experience expectations: increasing employee and customer expectations with the proliferation of devices and Cloud services in the workplace ("anywhere, anytime" demand). In addition, organizations are looking for greater

linkages to drive business processes and business outcomes

- Globalization: global talent and a globally dispersed workforce, emerging market requirements and indigenous innovation
- Security & Privacy: increasing expectations from users around the world with security, regulation and compliance requirements (e.g., from malicious to competitive; cyber security, geo-political)

- In addition, IT budgets are shifting to the Line of Businesses. Together, this changing world results in a changing role of IT... to accommodate the technology transitions while dealing with the business implications we all face. However, THE NETWORK NEEDS TO BE AT THE CENTER

Connected Objects Generate Big Data

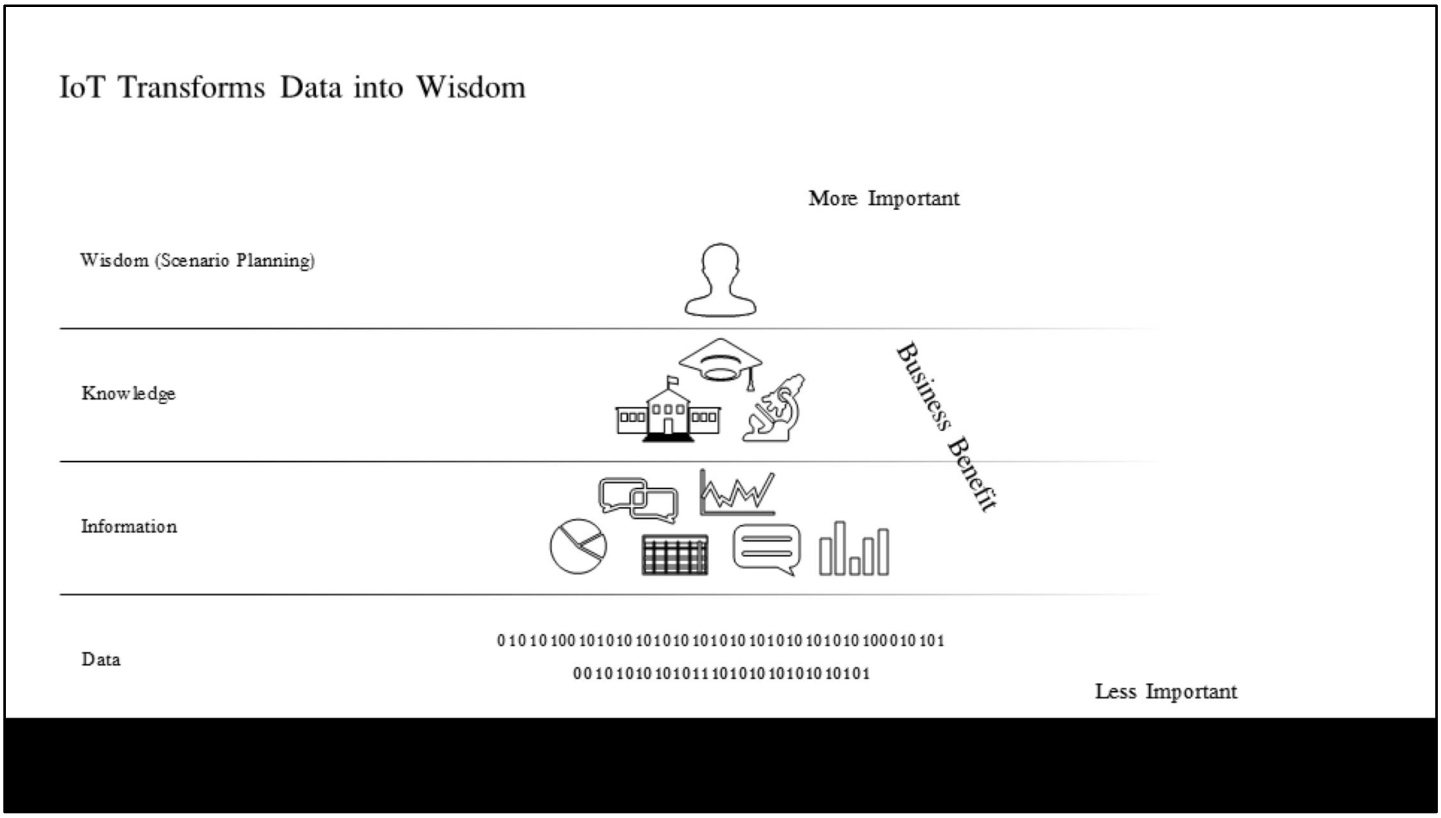
46 million smart meters in the U.S alone
1.1 billion data points (.5TB) per day

A single consumer packaged good manufacturing machine generates 1B data samples per day

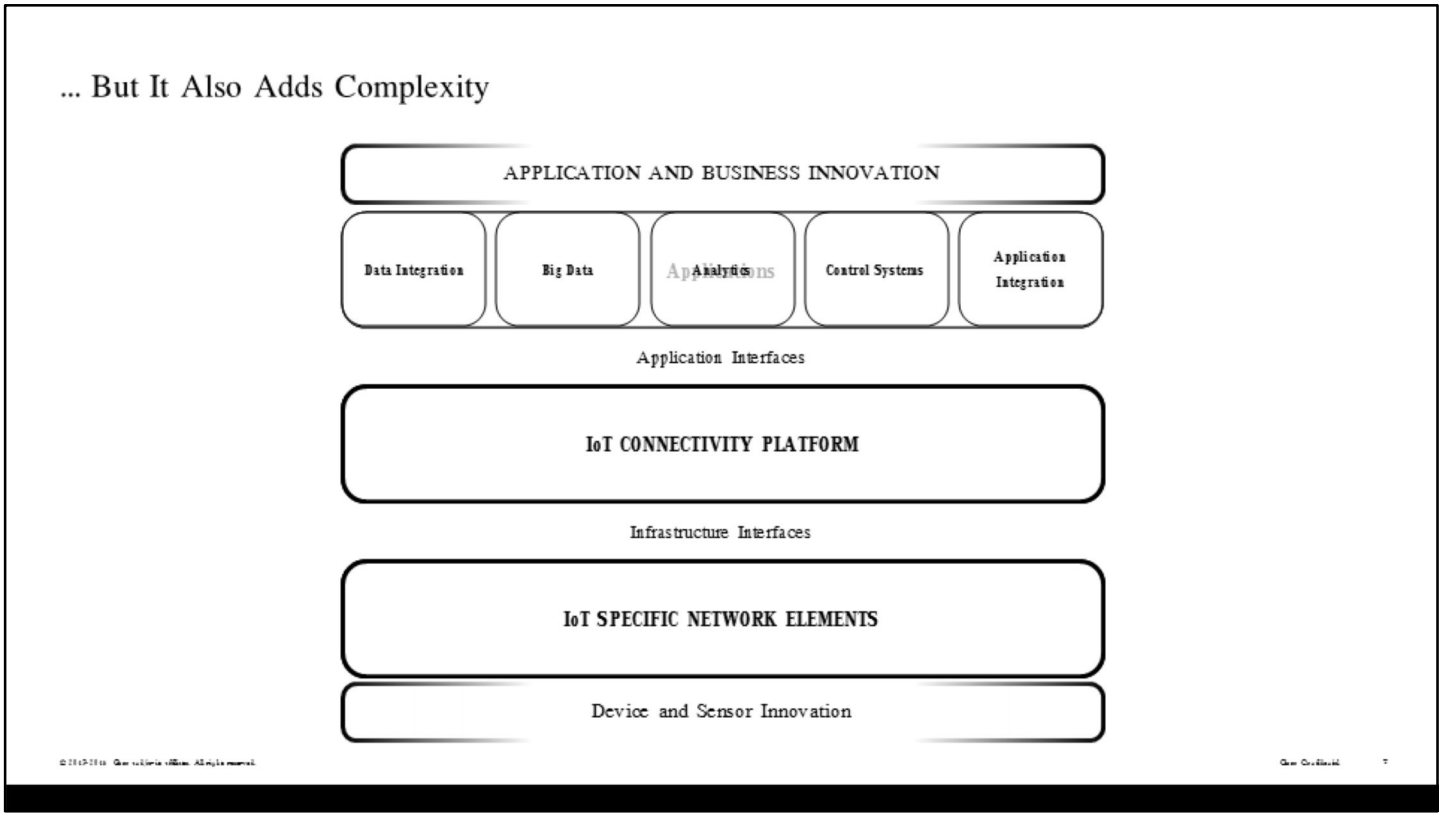
A large offshore field produces 0.75TB of data weekly
A large refinery generates 1TB of raw data per day

10TB of data for every 30 minutes of flight
With >25,000 flights per day, petabytes daily

In the past 2000 years, the world has generated a little more than 2 exabytes of data ... we now generate that amount *every day*. These objects are creating a data explosion, with data coming from billions of disparate devices, located all around the world. But unless they can work together, all of this data is siloed, and therefore relatively useless ...



The main benefit of IoT is derived from the connectivity of these billions of smart objects. While the data each of these individual items produces is of little value, IoT enables it to be processed and correlated with other inputs to produce relevant information; it can then be used in real-time as actionable knowledge by IoT-enabled applications; longer term, it can be used to gain deeper understandings for the purpose of developing proactive policies, processes, responses, and plans.



But in addition to these business benefits, IoT also adds additional complexity to your network. That's because IoT doesn't replace your existing network; rather, it supplements it, and relies on it in many ways.

Your existing network is comprised of a core infrastructure (switches, routers, and servers); a unified platform (not just the operating system, but a programmable SDN network is becoming increasingly important); and applications. Services are an inherent part of every level of the network, and security needs to be interwoven throughout to keep data and assets safe.

[ANIMATE x2]

IoT requires that connectivity tools be added to the platform, as well as some network elements such as smaller, more self-contained switches and routers for fields, plants, and other operational environments. These network elements are frequently deployed in challenging environments that include harsh weather conditions, significant amounts of vibration, etc., so they need to be ruggedized to function under these conditions.

[ANIMATE]

Now here's where it gets interesting ... one of the primary differences between your existing IT network and an IoT network is all of these additional devices, sensors, and other "smart objects". It's important to note that these objects are networked together, yet they're independent of your network – you don't own them; oftentimes can't see them; and you don't control them in any way, shape, or form. Yet they're sending petabytes of data through your network – data that's required by the applications to function properly.

[ANIMATE]

Another difference is in the applications, themselves. Unlike today's monolithic applications, where the main value is delivered locally from the application's code, IoT applications derive most of their value from the intelligence that is collected from, and distributed throughout, the network; the application itself is merely the method employed to access that intelligence.

[ANIMATE]

Which leads us to the other major infrastructure difference in an IoT network, which is required to communicate and process all of this intelligence ...

[ANIMATE]

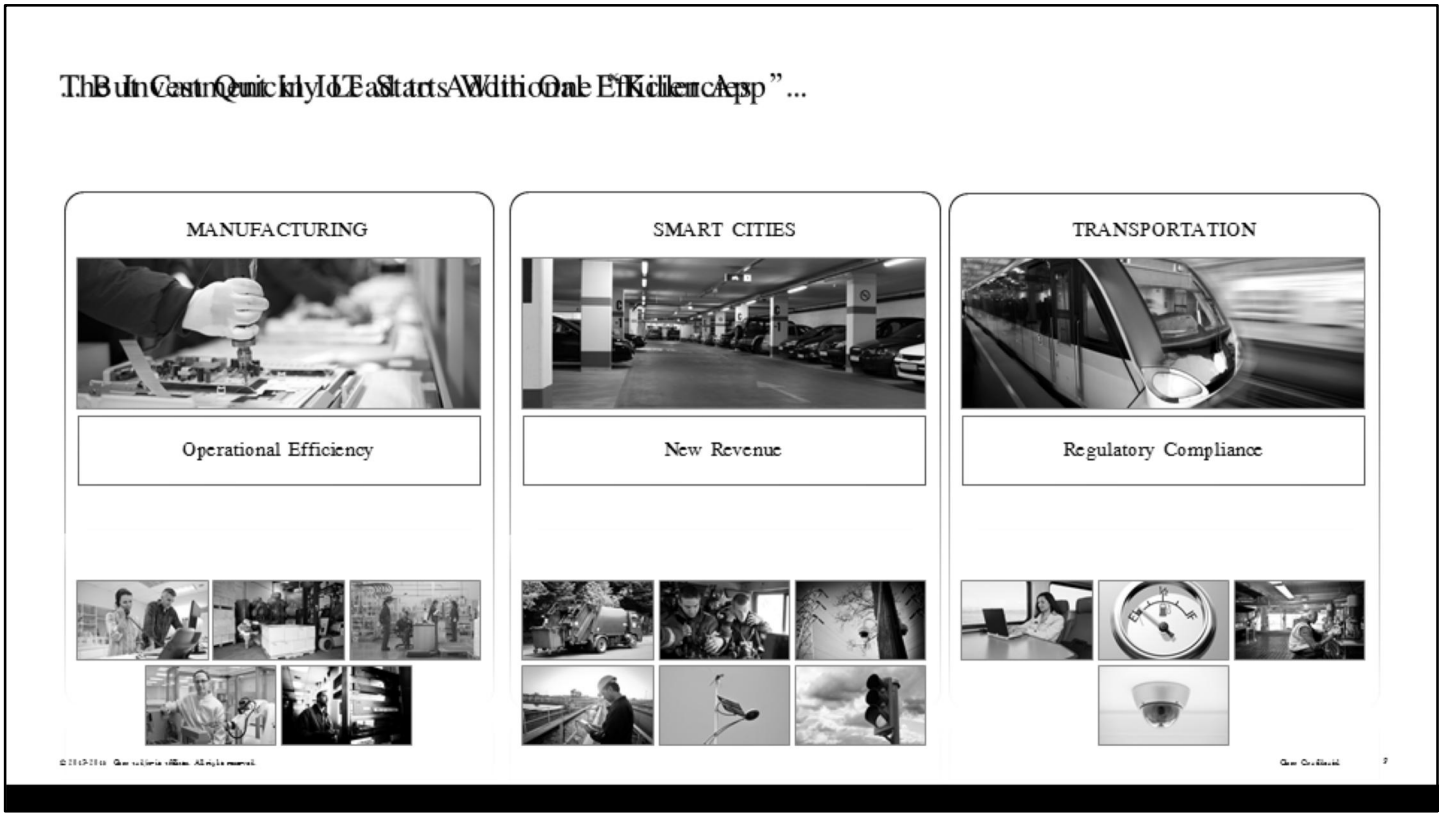
Of course, services will need to be expanded to cover the new capabilities ...

[ANIMATE]

And we'll need additional layers of security to enjoy the many business benefits of IoT while maintaining a high level of data privacy and protection.

[ANIMATE]

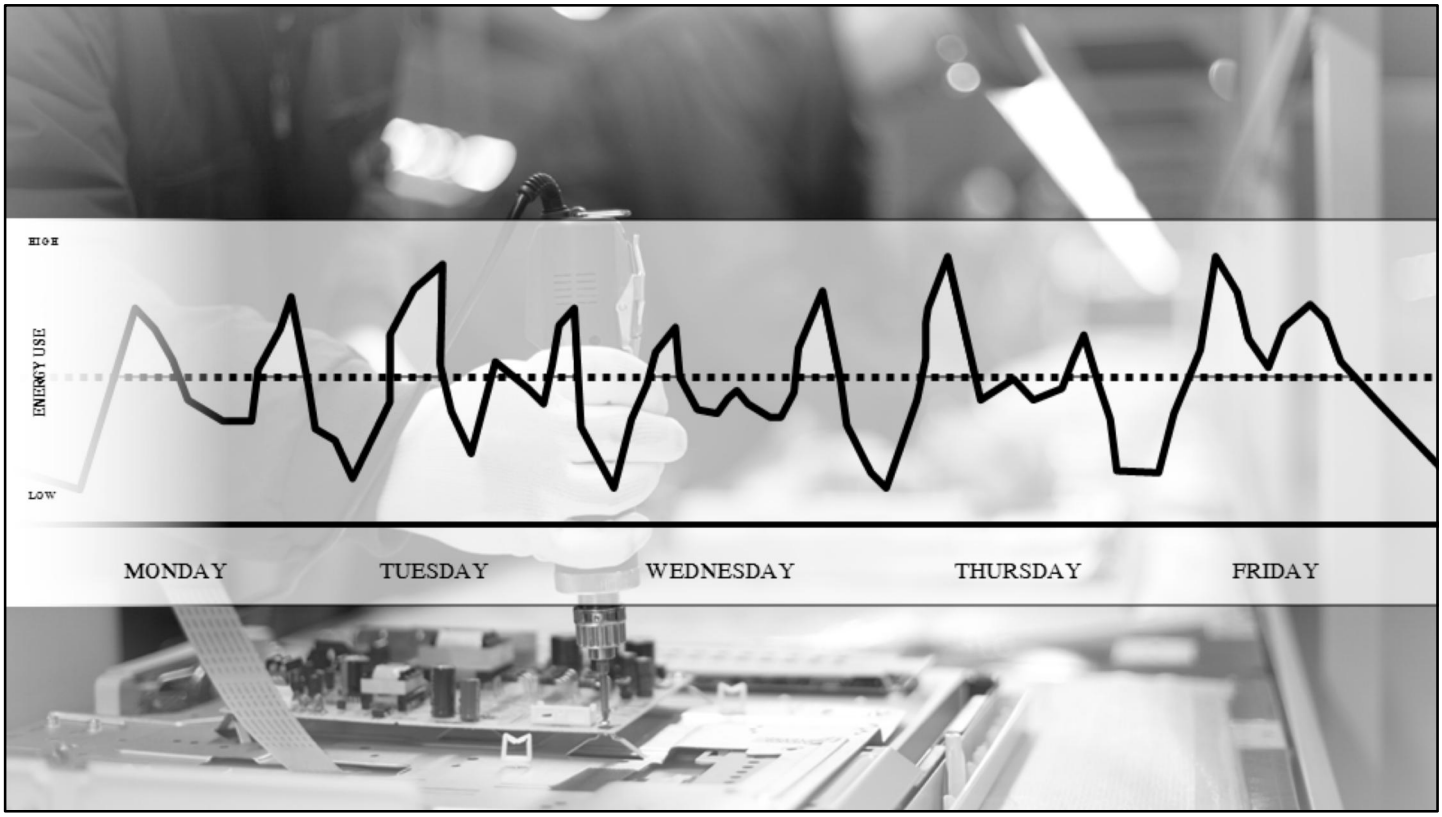
This is the area of the network Cisco serves. We'll continue providing core networking equipment, and are expanding to take a leadership role in providing the core infrastructure you'll need for successful IoT implementations.



IoT provides a wealth of intelligence that businesses can use for planning, management, policy, and decision-making to help them maximize productivity and efficiency while minimizing costs.

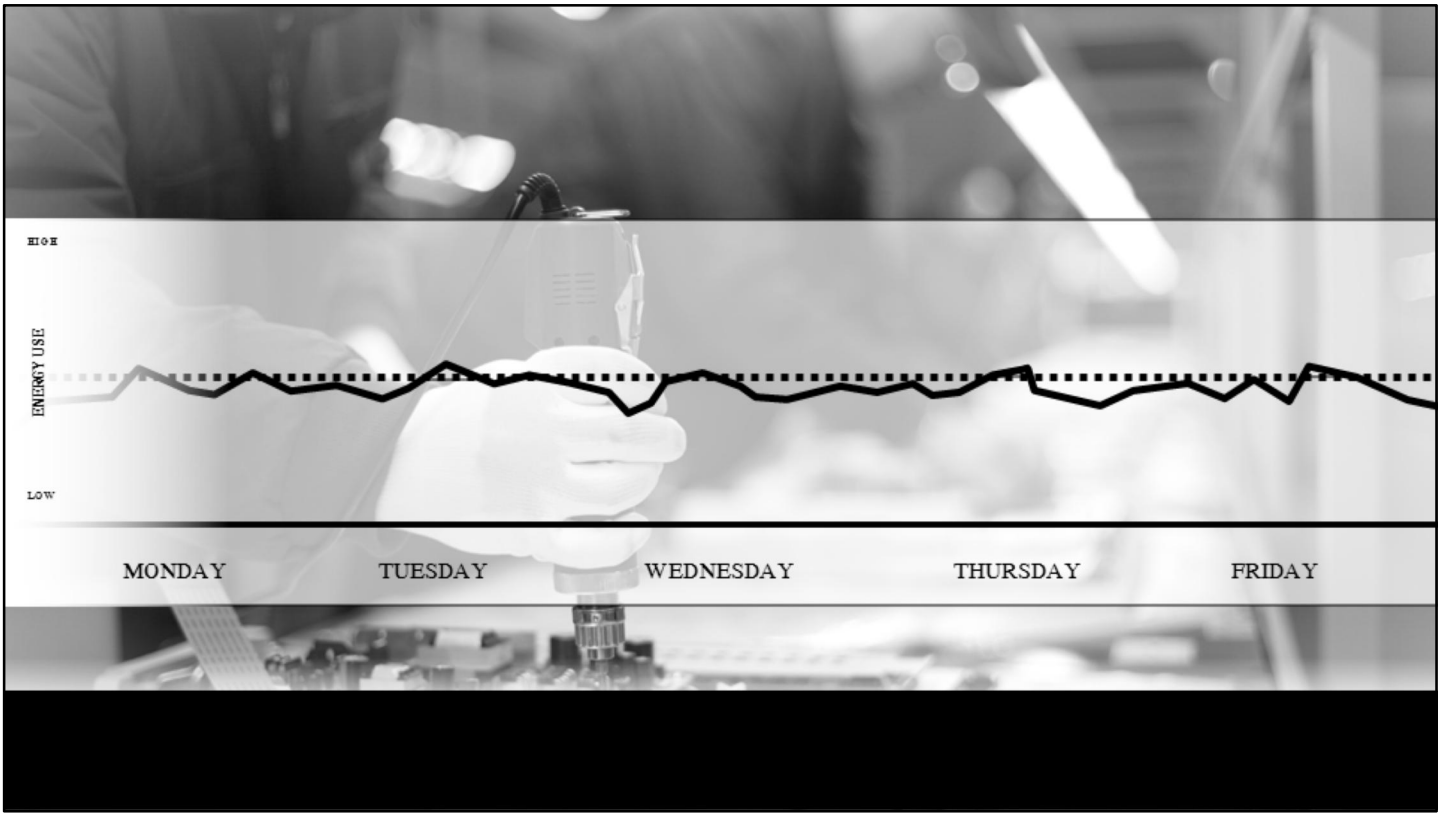
In most cases, the driver for embracing an IoT implementation will be one specific thing that the organization is trying to accomplish – and that becomes the "killer app" that proves the core value of thelarger technology. The beauty of IoT is that we're just beginning to scratch the surface of what's possible – once the killer app is developed and the infrastructure is therefore in place, the organization can find all sorts of new uses to better utilize the same infrastructure.

Consider these examples ... ***[ANIMATE]***



Manufacturing plants use a lot of energy and, when they go above a certain utilization rate, they're charged more per unit of energy. So if they can figure out how to even out their usage to avoid spikes, they can save money.

Right now, most manufacturers have a separate IT set-up and a separate network for the manufacturing plant versus headquarters. To shave those energy peaks you need to know a few things. First, you need to know what's going to be built when. That information comes from the "Master Execution Scheduler" which is kept on the proprietary manufacturing network. But you also want to know what's been committed to customers so you don't save money on energy yet drive away customers in the process. That information is in your ERP system on your corporate network. And then you want to know how changing the schedule might affect labor costs, so you don't lose all the money you saved on energy, making the whole exercise pointless. For that, you need information from your HR system, also on your corporate network. Then you need to analyze the information.



Once you've brought all the right systems together, you can build an application with thresholds and policies that alert operators to an approaching peak and show gaps in the schedule—times they could push the production load to. Or they can shift production to another plant with more capacity. But that requires adjusting supply chain, MRP, and the factory build plan to compensate without impacting customer commitments or desired inventory levels. Or they can check the power co-generation system to see if they can keep production high but use co-gen energy to avoid the peak.

But something interesting happens, once you've created your killer app....

Now you've built some new capabilities into your infrastructure that will enable lots of other applications. In the case of manufacturing, you can add things like predictive maintenance—which combines sensor data on equipment with historical averages in your database system to let you know *before* a part or machine breaks that it needs repair. This increases plant uptime—super valuable.

And you can implement more fine-grained traceability. This limits your downside if you have a product recall because you can track which products came from which production lines when and which components were used to make them, so you can target only those units that really need to be recalled.

Other applications include faster supply chain flows and mobile control rooms or wireless machines for greater flexibility on the factory floor.

So just that one killer app of peak shaving has been projected in one case to save 20-30% in energy costs in the first year is 20-30%. That's a huge number for manufacturers—and definitely worth investing in.

But beyond that, we've done some research that shows there is $1.95 trillion in potential *new* profits (from both cost savings/efficiencies and new business opportunitiess) over the next 10 years from implementing IoT just in manufacturing.

In the United States there is legislation requiring the railway industry to implement a traffic control system called Positive Train Control. This is to avoid terrible accidents like the one in Northwestern Spain in mid-2013. (The driver went too fast around a curve, and 79 people were killed)

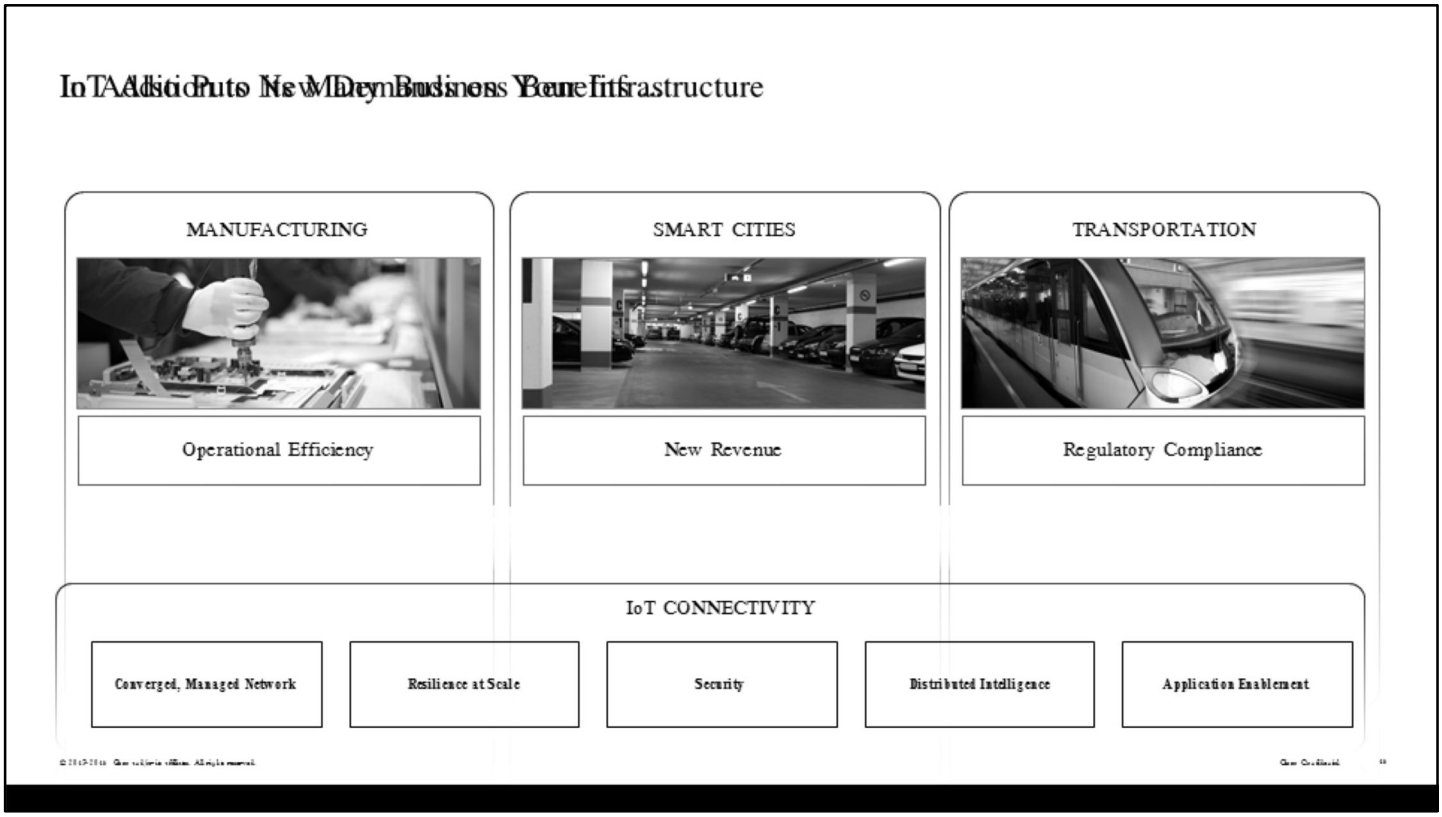
Along with increased safety, train operators get alerts that help them optimize routes based on track, traffic and other data. Other apps include predictive maintenance and wayside equipment tracking.

Cisco estimates that customers can use our PTC solution to save 1-2% in fuel costs through optimal throttling and braking data sent to engineers via a wireless tablet. Union Pacific in the US saved 4-6% in fuel costs with their system. They found that their best engineers use only two-thirds the fuel of their least efficient drivers. UP has put rewards in place to incent fuel-efficient practices (as well as serious talks with underperformers).

And the PTC infrastructure can also carry along passenger wi-fi and safety applications, as well.

Using Cisco's PTC solution, Connected Trackside for Passengers, railroads will deliver converged multi-services IP networks that can enable cost effective communication solutions for electrification that can double passenger capacity along the same track infrastructure.

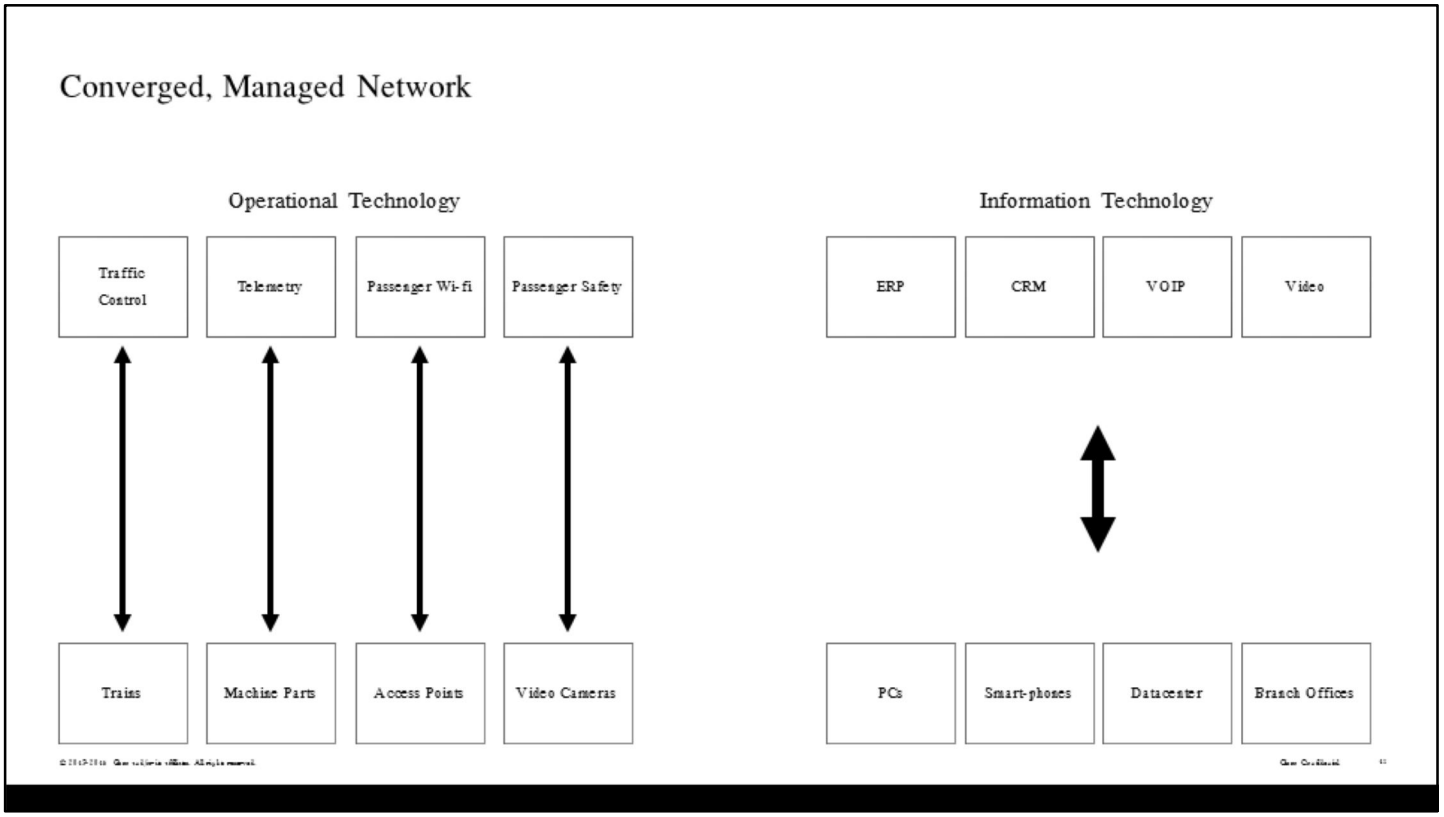
Rail operations costs represent 75 percent of total trail transport costs, or $184 billion per year. GE Transportation estimates that 2.5 percent of rail operations costs are the result of system inefficiencies. This amounts to $5.6 billion per year in potential savings. If only one percent savings can be achieved, the amount saved would be about $1.8 billion per year or about $27 billion over 15 years. Similar types of efficiencies appear possible in heavy duty trucking, transport fleets and marine vessels, meaning much larger transportation system benefits can likely be realized.
--GE report on Industrial Internet, Nov. 26, 2012, p.21
http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf



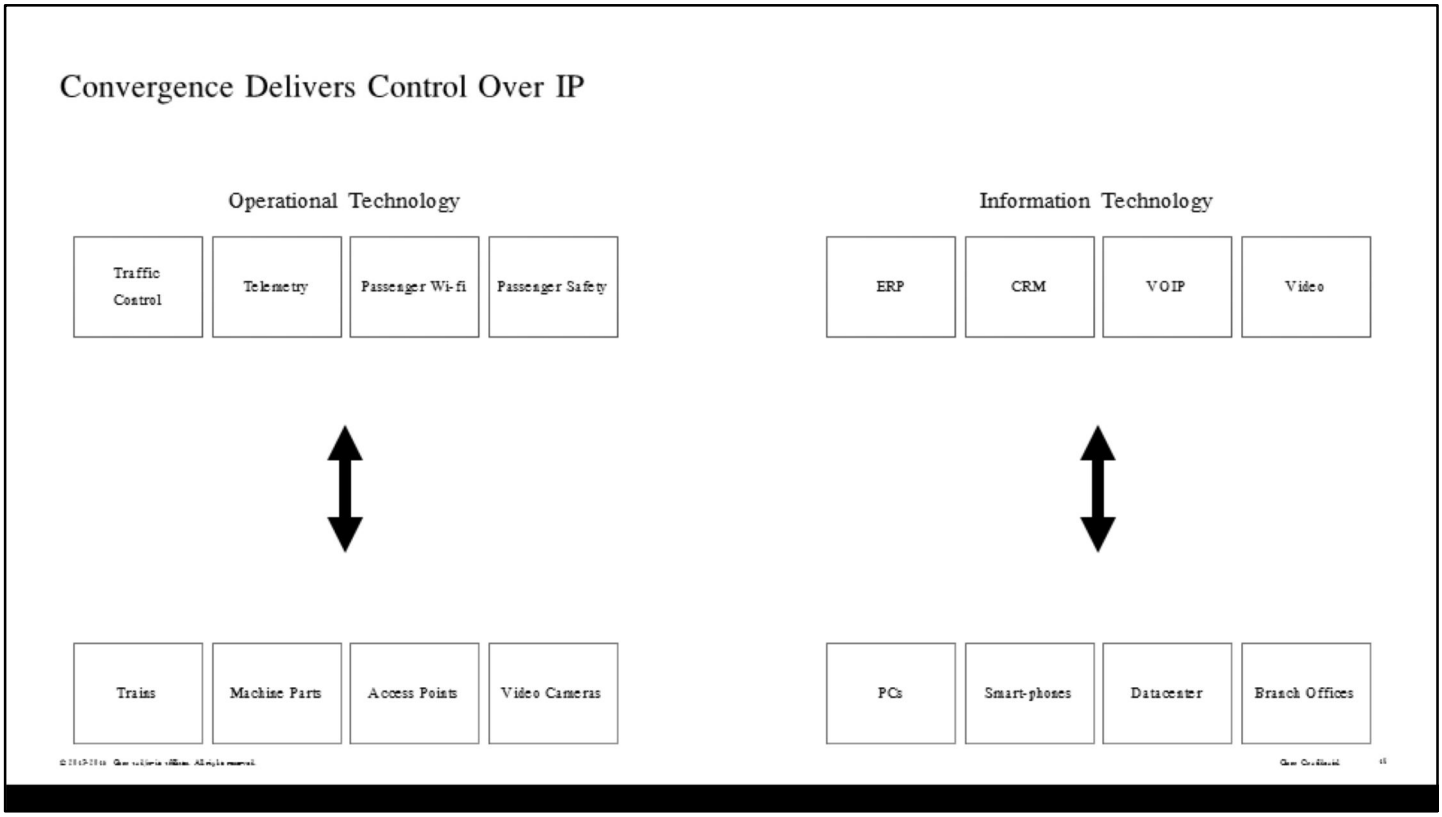
IoT is truly a "game-changer" for businesses. As we've discussed throughout this presentation, IoT can help you increase your business efficiency, reduce costs, enter new markets, and maximize your ROI ...

[ANIMATE SLIDE]

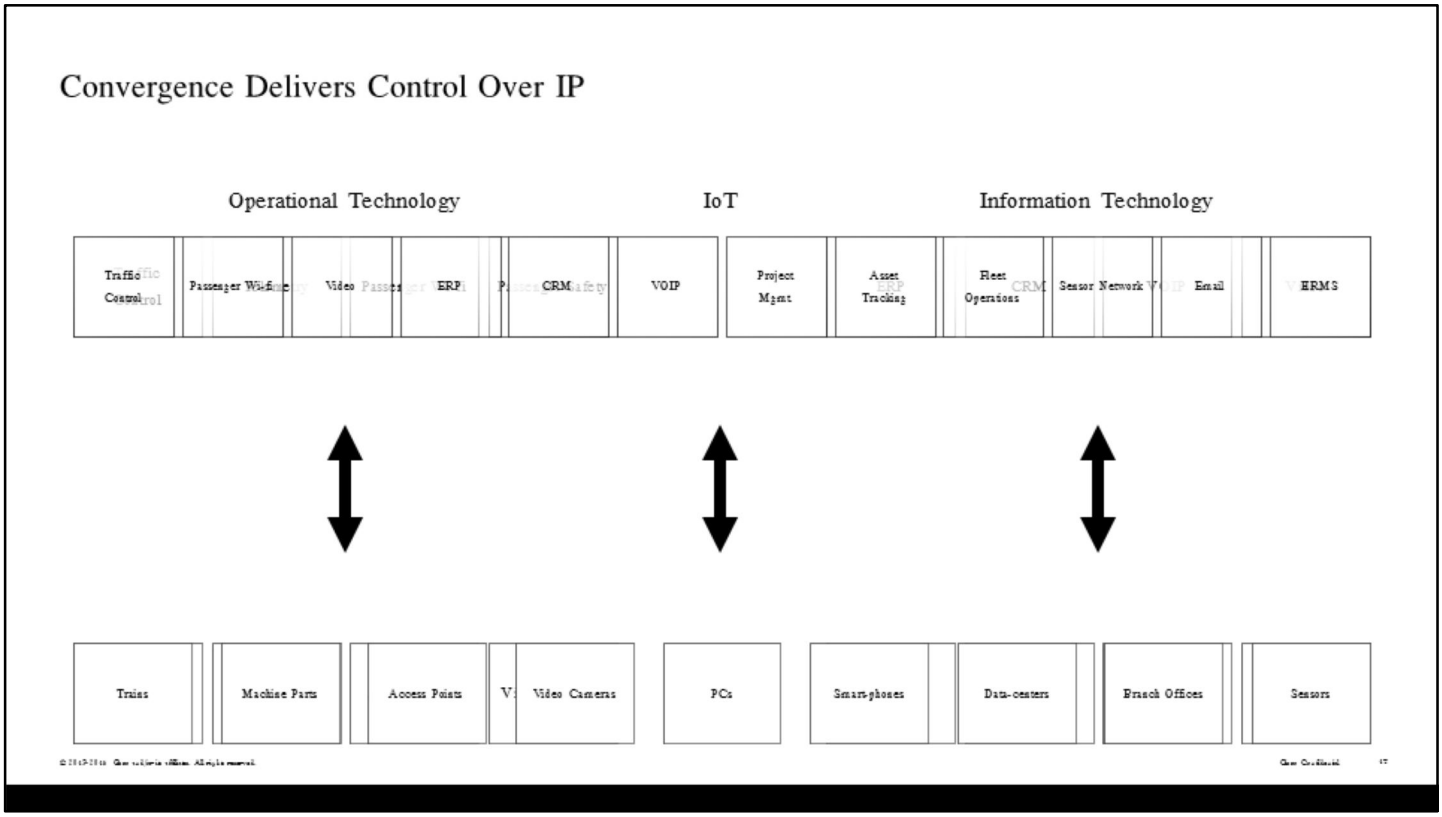
... but all of these benefits and capabilities come at a price. To take advantage of the benefits of IoT, we need to move beyond what only IT can provide; to successfully address these new needs, your network will have to evolve to include five new key capabilities.



Converging your network really has two dimensions. First, notice how IT networks are already converged, with visibility and management across multiple systems. In contrast, OT networks are typically siloed, with separate management for each component, and no ability to communicate or gain visibility from one to the next.

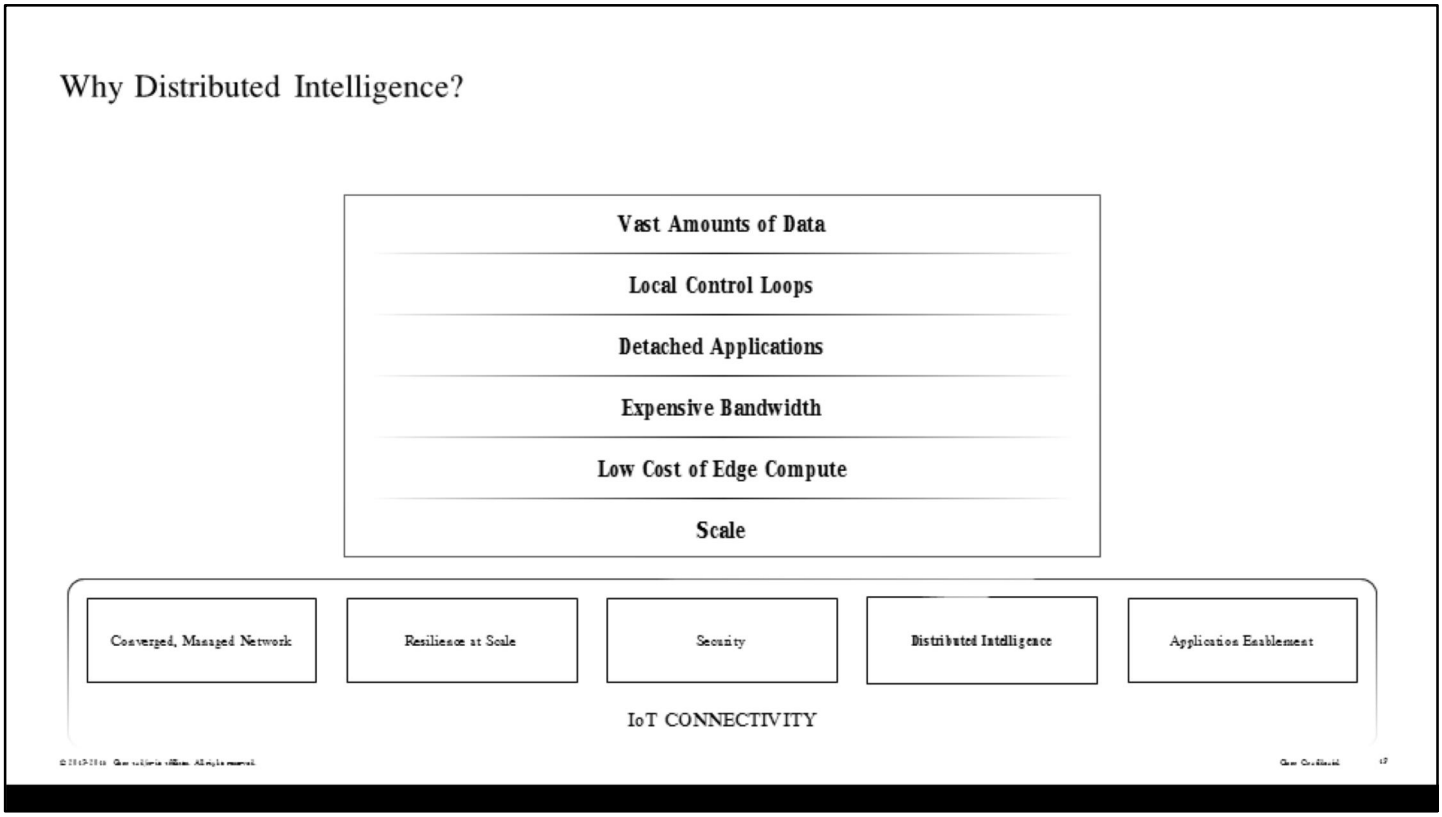


... so the first step is to bring OT networks in line with how IT networks are structured, helping OT achieve centralized visibility and control across the various systems – for a high level of business efficiency.



[ANIMATE]

But to truly reap the rewards of IoT, it's necessary to combine the IT and OT systems into one, to truly gain insights throughout the organization.

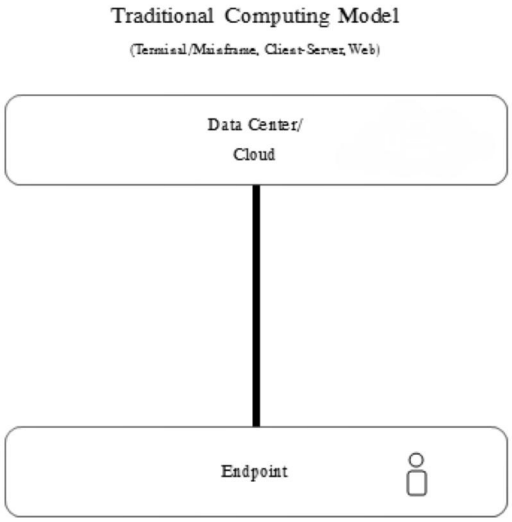


Another difference between IT and IoT is the speed at which decisions need to get made and acted upon. With IT, information, say financial data, comes in and gets analyzed over hours, days, weeks and months. In a mining operation, if someone's hand gets caught in a machine, you need to shut that machine down immediately. That requires sensor data to come in, be analyzed, a decision to be made and the machine to be shut down in milliseconds.

This can't involve a human being in the process because it's too slow, so you need closed-loop automation and real-time controls that draw on data analysis that is processed at the edge by an expert system that can decide to shut down the machine. Precise timing in the network is needed to make sure this happens immediately, not in five minutes. You simply can't have humans in a control center filtering all the data fast enough to make meaningful decisions.

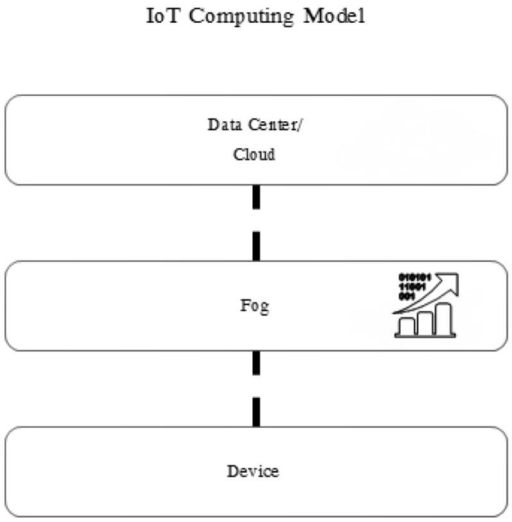
To achieve this speed, we need to push the compute capability closer to the source of the data, so data can be filtered and analyzed. Only when necessary does it filter up, in a more actionable form, to a human.

IoT Requires Distributed Computing



This is the traditional view of network computing. We have our data being produced down at the endpoint, then pushing that data up to the cloud to be correlated and analyzed. For existing, monolithic apps, this is just fine, since speed isn't absolutely essential. But the sheer amount of data generated by the billions of IoT devices can overwhelm existing networks, leading to unacceptable levels of latency.

IoT Requires Distributed Computing



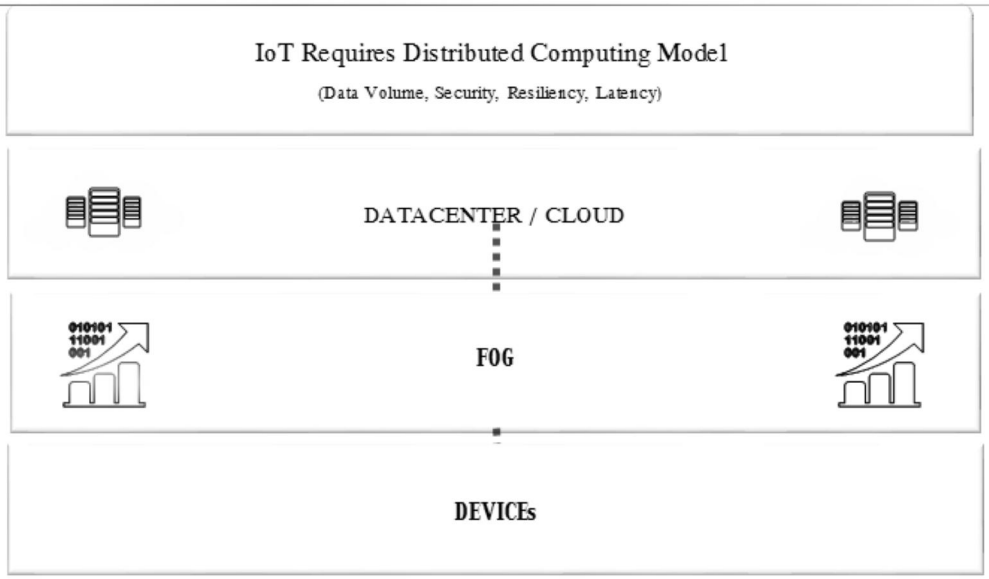
The main value of IoT is its ability to produce real-time intelligence. By placing compute capabilities at the edge where it's closest to the devices and applications, the data gets analyzed ***right there*** to minimize latency. This is edge computing model, placing compute and memory right into edge switches and routers, is what Cisco calls the "Fog" layer.

What is Fog Computing ?

Fog is an expansion of the cloud paradigm. It is similar to cloud but closer to the ground.

The Fog Computing architecture extends the cloud out into the physical world of things.

Fog Computing distributes selected computation, networking and storage functions closer to the edge.



We think that with IOT we need to introduce this new intermediate layer and this intermediate layer we have been calling fog.

It's close to the ground, it's close to the edge, it's for when you want to do some processing...you want to run control algorithms, you want to run some data optimization algorithms there to avoid having to backhaul everything because you just have to recognize that many of the device in this Internet of Things world are not perfectly connected.

They are intermittently connected
They are on battery power
They are going to be asleep most of the time
They might come into range every so often but then get out of range again.

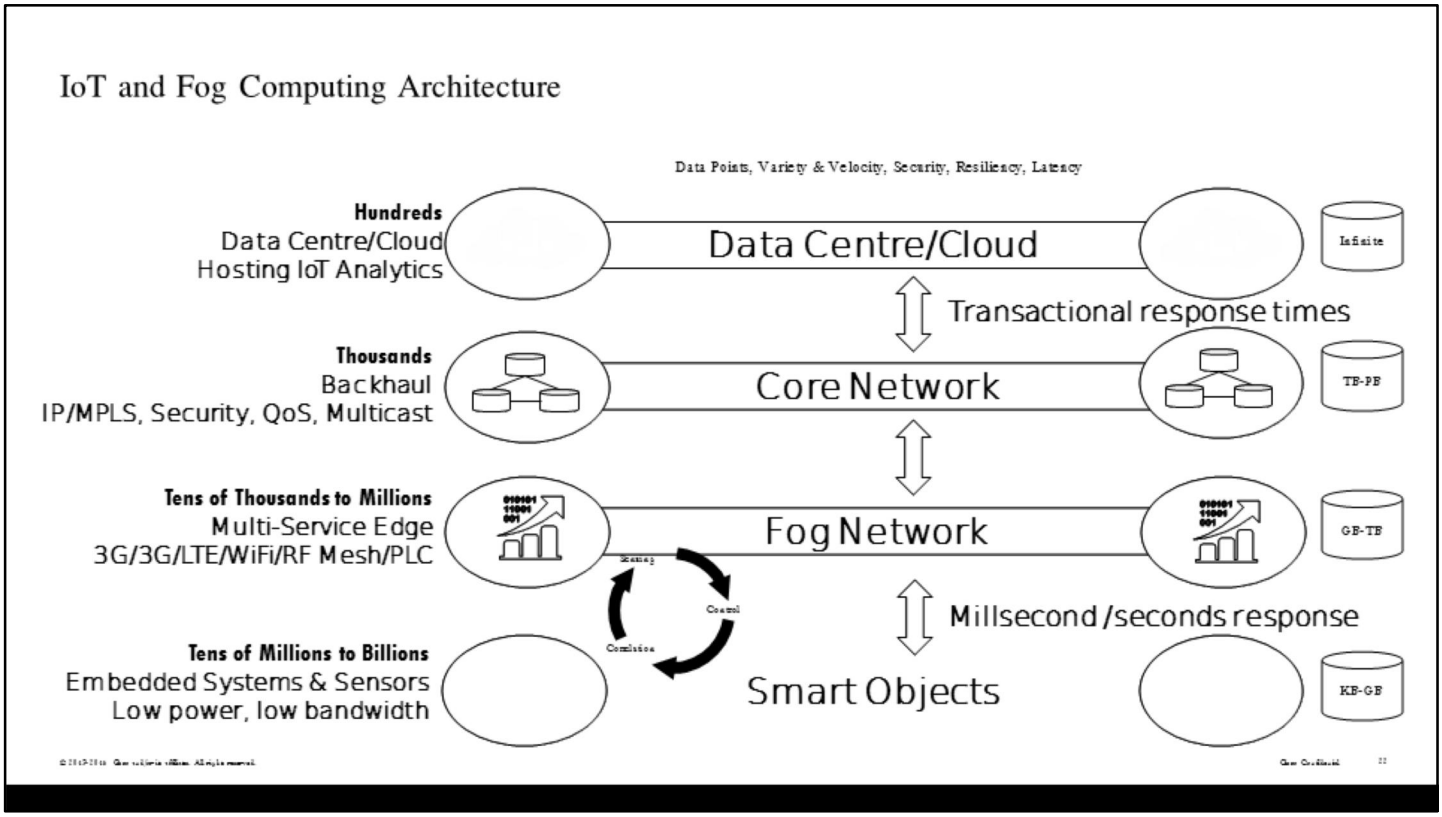
We have to cater to the idea that there is a place in the infrastructure that can act as a relay...as a data governor....some kind of intermediate layer.

Also if for nothing else, then just for scale.

If you think about it 50 billion objects...even a small utility with smart meters will see a dramatic uptick in the number of IP device that the IT department will now have to manage.

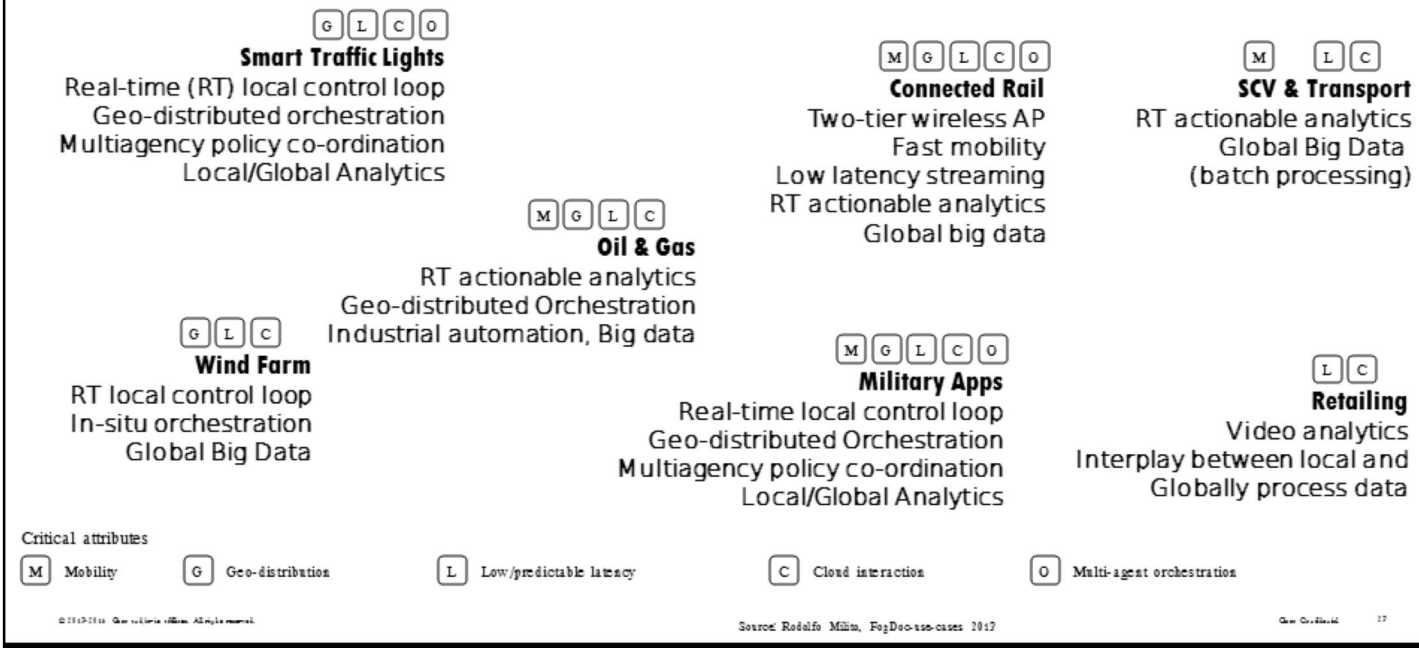
A three tier architecture is more scalable, more resilient and overcomes some of these problems.

A simple way to think of this "moving from always on to always ready".



- The IoT requires the introduction of an aggregation layer for computing and storage services we call Fog Computing
- The Fog Computing layer is context/location aware, close to the edge and can react to events in the IoT nework in sub-seconds
- The Fog layer provides a control loop capability, where devices can be monitored, controlled and analysed in real time (this is quite critical for SmartGrid components for example)

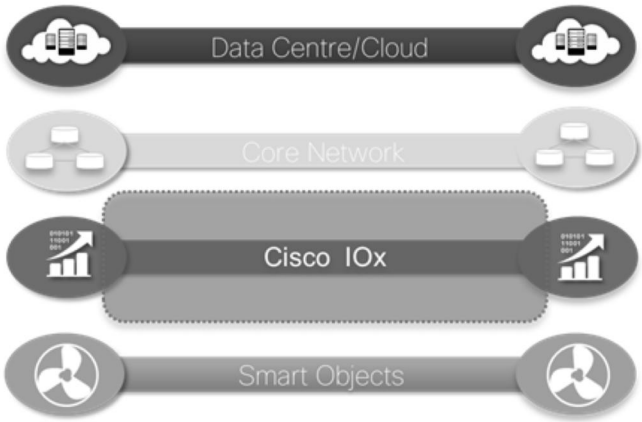
Fog Computing Example Use Cases



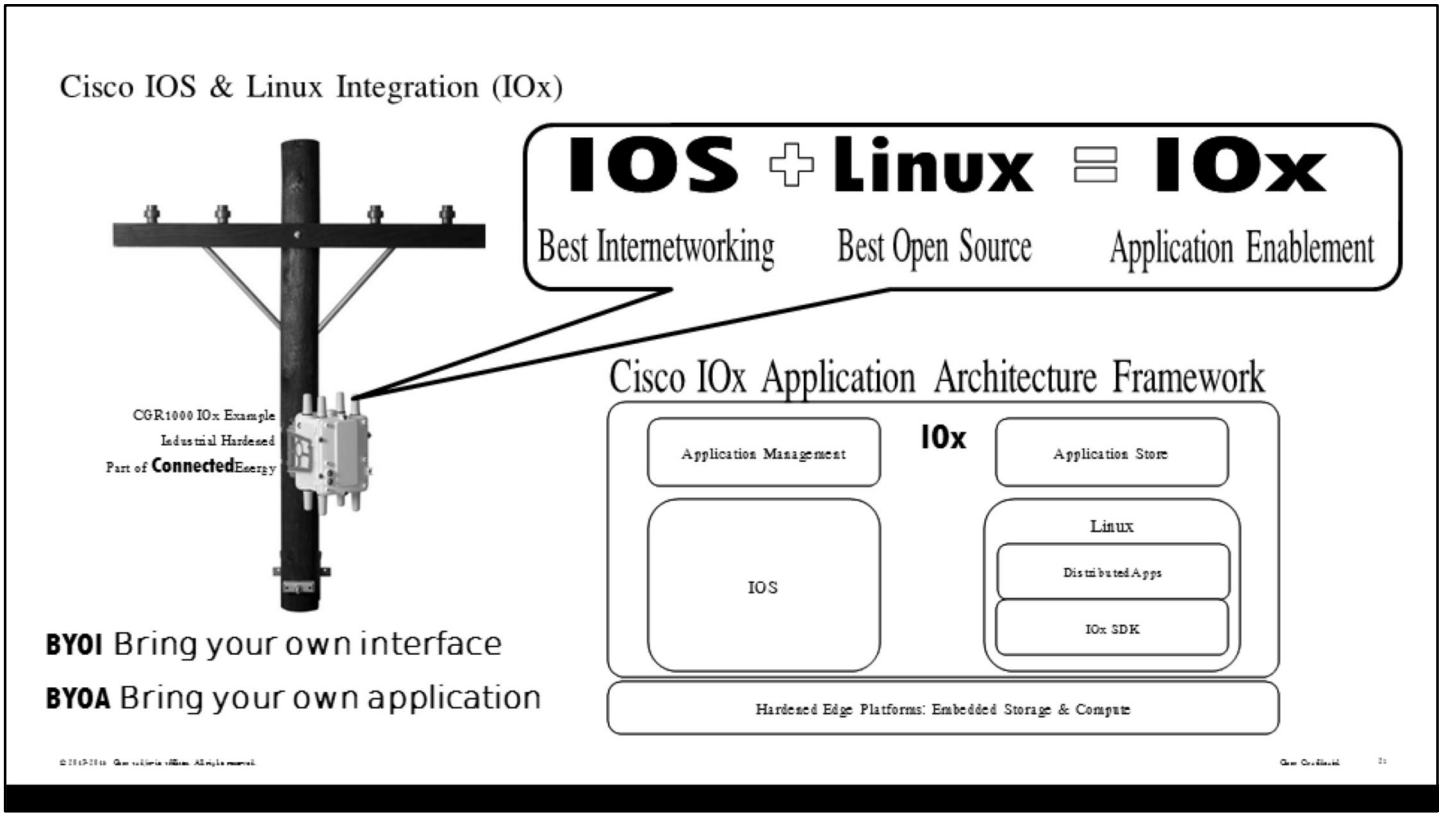
Source: Rodolfo Milito, FogDoc-use-cases-2015

Cisco IOx

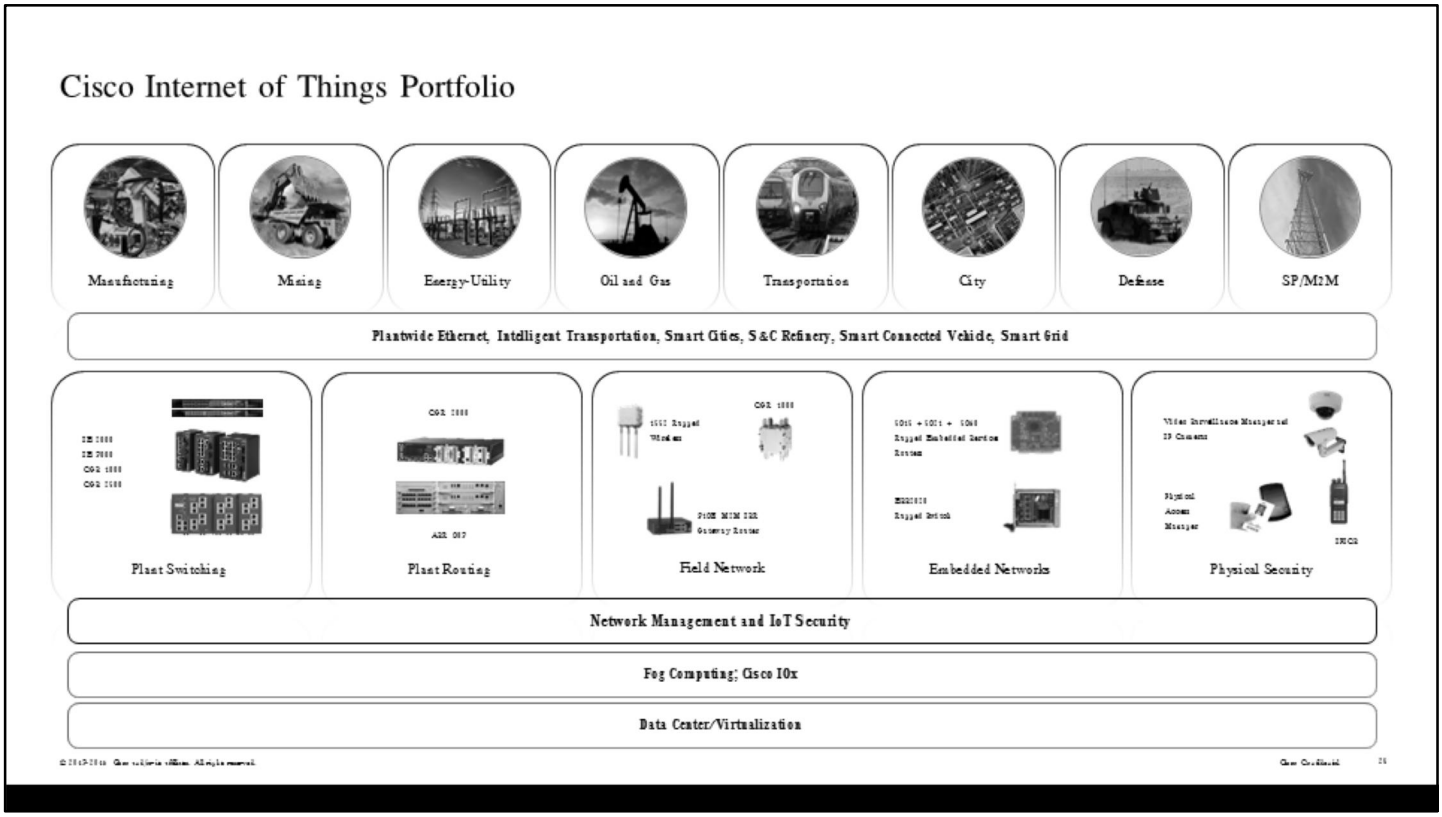
- Allows customer apps to execute on Cisco industrial network devices
  - Fosters innovation, agility and efficiency in operational technologies (OT)
- IOx integrates Cisco IOS™ with Linux (for customer apps)



- Cisco's architecture for fog computing, transforms the network edge into a distributed computing infrastructure for applications that take advantage of the billions of devices already connected in the Internet of Things (IoT).
- The new Cisco® IOx capability, customers from all segments and solution providers across industries will be able to develop, manage and run software applications directly on Cisco industrial networked-devices, including hardened routers, switches and IP video cameras.
- With applications closer to where actionable data is generated, customers can more easily manage the massive amount of data that is projected to come out of people, process and things in the Internet of Everything (IoE) – and derive more value from their existing networks.
- Companies will be able to become more innovative, agile and efficient in their operations as a result.



- Cisco IOx brings the open-source Linux operating system and industry-leading Cisco IOS® network operating system together in a single networked device, which allows applications to run and respond instantly to actionable data sensed in an IoE world.
- Enables developers to bring their own applications (BYOA) and connectivity interfaces (BYOI) at the edge of the network
- Help advance the deployment of IoE across different industries such as utilities, manufacturing and transportation.
- Cisco IOx capabilities will initially be available in Cisco industrial routers this spring. Cisco is working with industry leaders to collaborate and develop IOx-based solutions that will ease the deployment and support of the billions of connected devices in IoT.



Cisco offers a wide range of products and solutions to serve IoT use cases across multiple industries ...

Thank you.