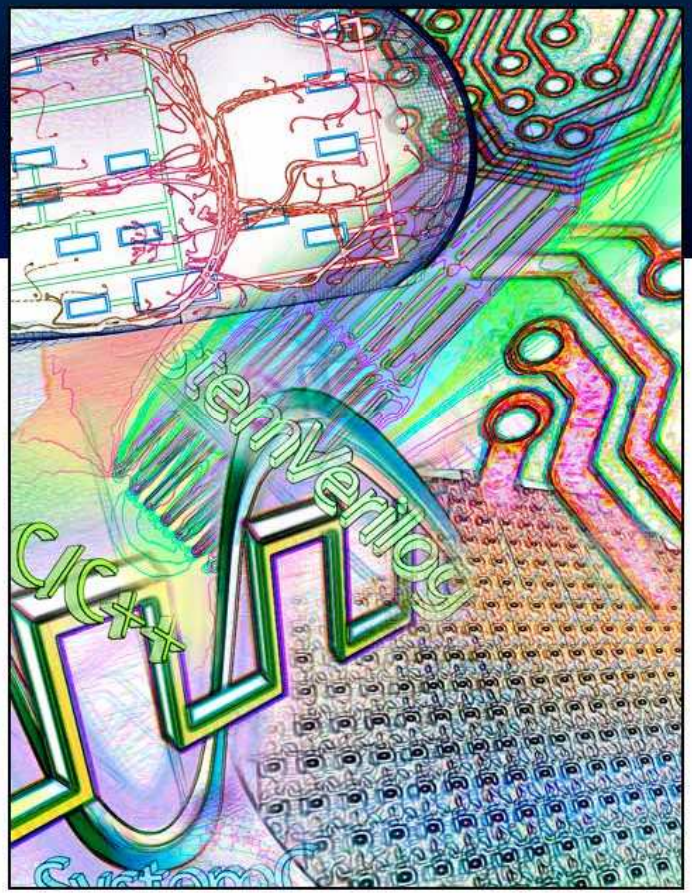


Convergence of silicon, Sensors, Mobility, and Cloud as Driving Forces in System Design Evolution

Serge Leef

VP, New Ventures, Mentor Graphics

April 21, 2016, Monterey, CA

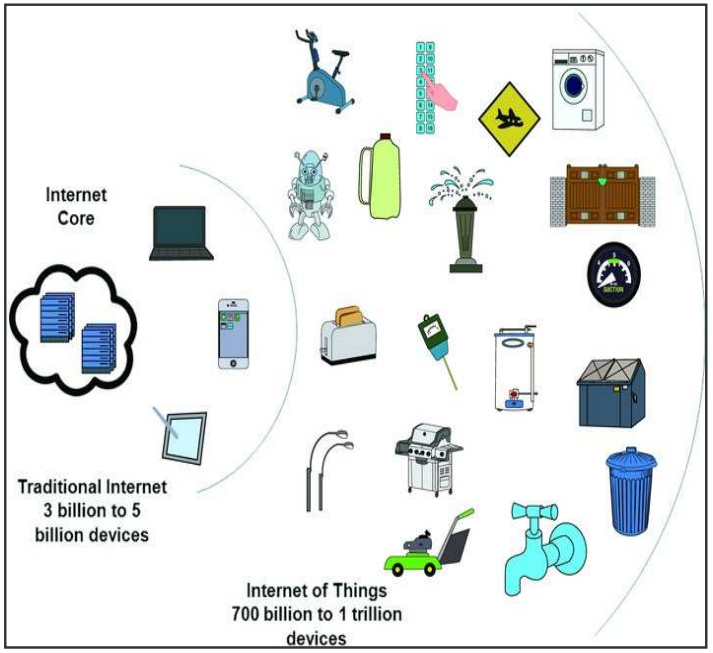
Mentor Graphics®

Outline

- Driving forces behind IoT
- Metamorphosis of embedded systems
- Domain driven end-to-end applications
- IOT Enablement tools and technologies
- Security implications of a large attack surface

IoT: Emergence of Intelligent Systems

- Intelligent Systems / **Internet of Things**
  - 75B Devices will be connected by 2020 (Morgan Stanley)
  - Execute native or cloud-based applications
  - Data collection & analytics
  - Explosive growth potential
- Internet of Things
  - Uniquely identified "things"
  - Machine-to-machine communication
  - Cloud infrastructure
  - Cyber-physical systems
- Edge-node design
  - Electronics, Controls, Software
  - Multi-physics, Communications

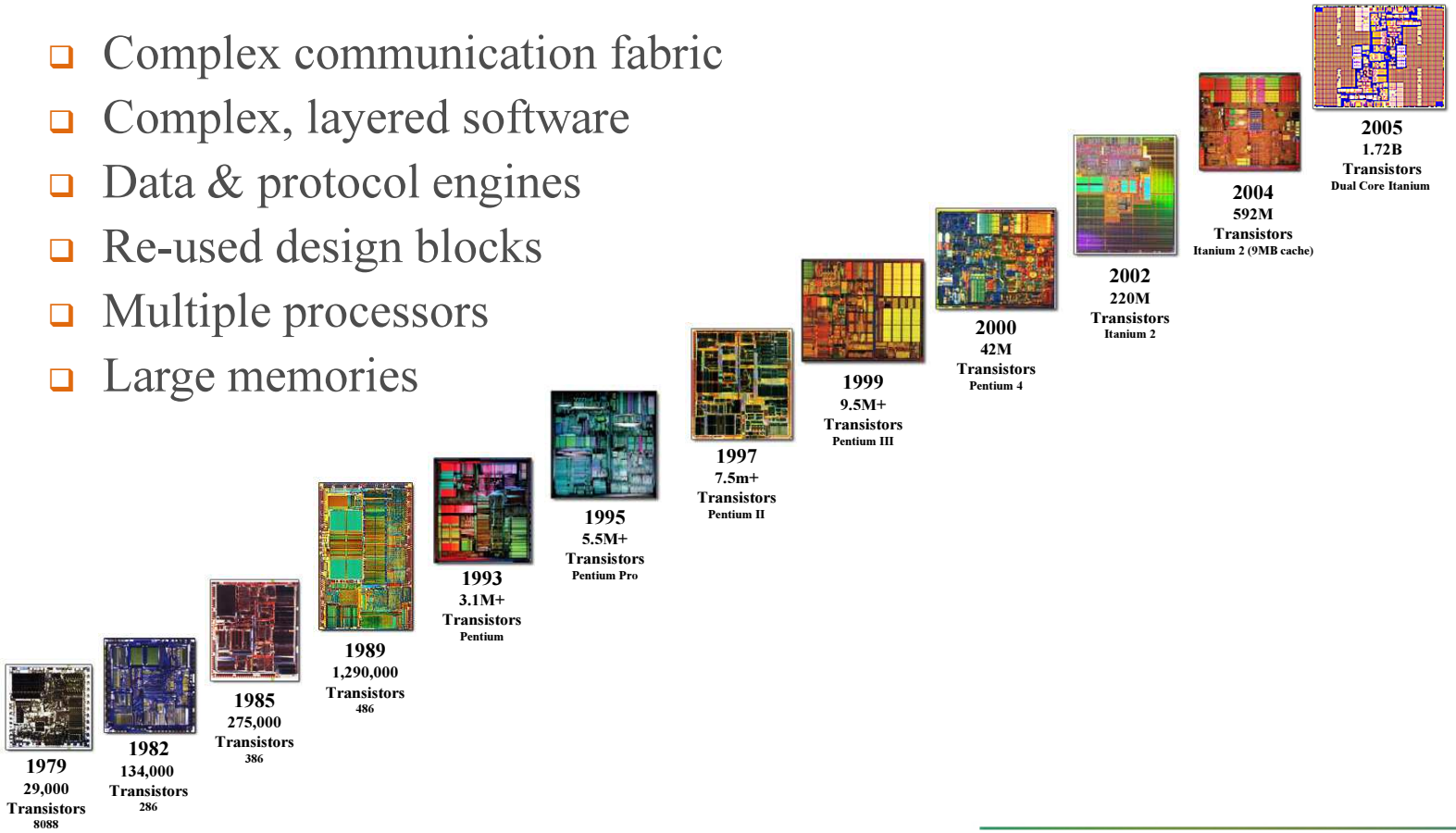


* "Rethinking the Internet of Things: A Scalable Approach to Connecting Everything", Francis daCosta

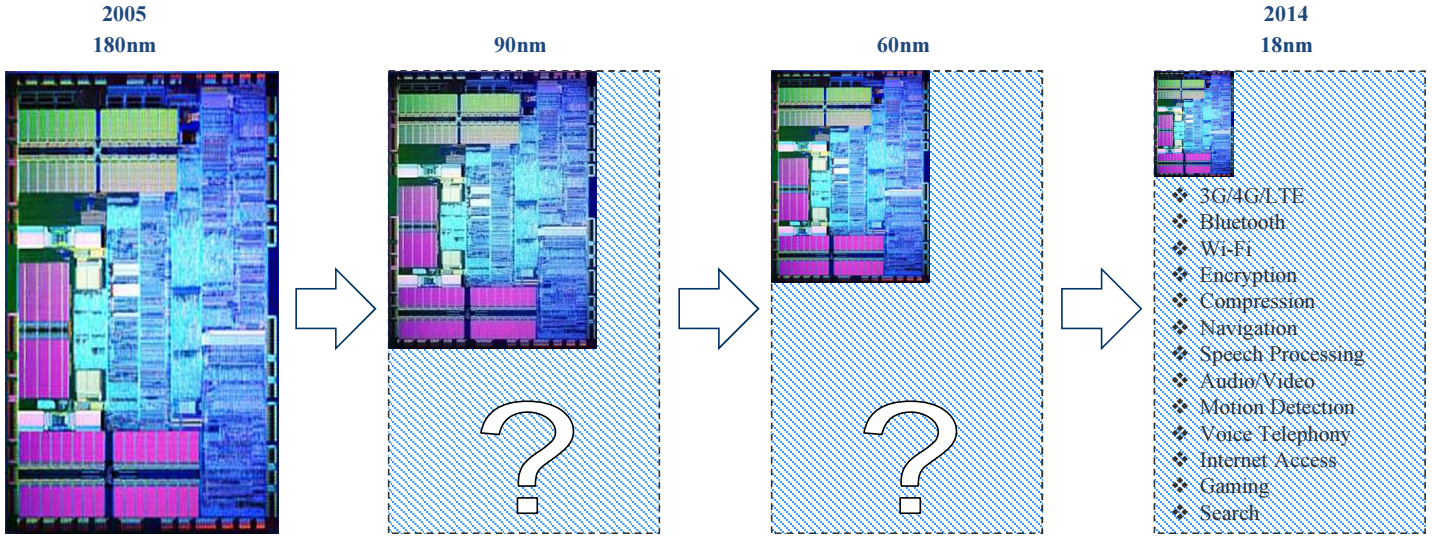
DRIVING FORCES BEHIND IOT

Growth in processor complexity & size

- Complex communication fabric
- Complex, layered software
- Data & protocol engines
- Re-used design blocks
- Multiple processors
- Large memories



What happened since 2005?

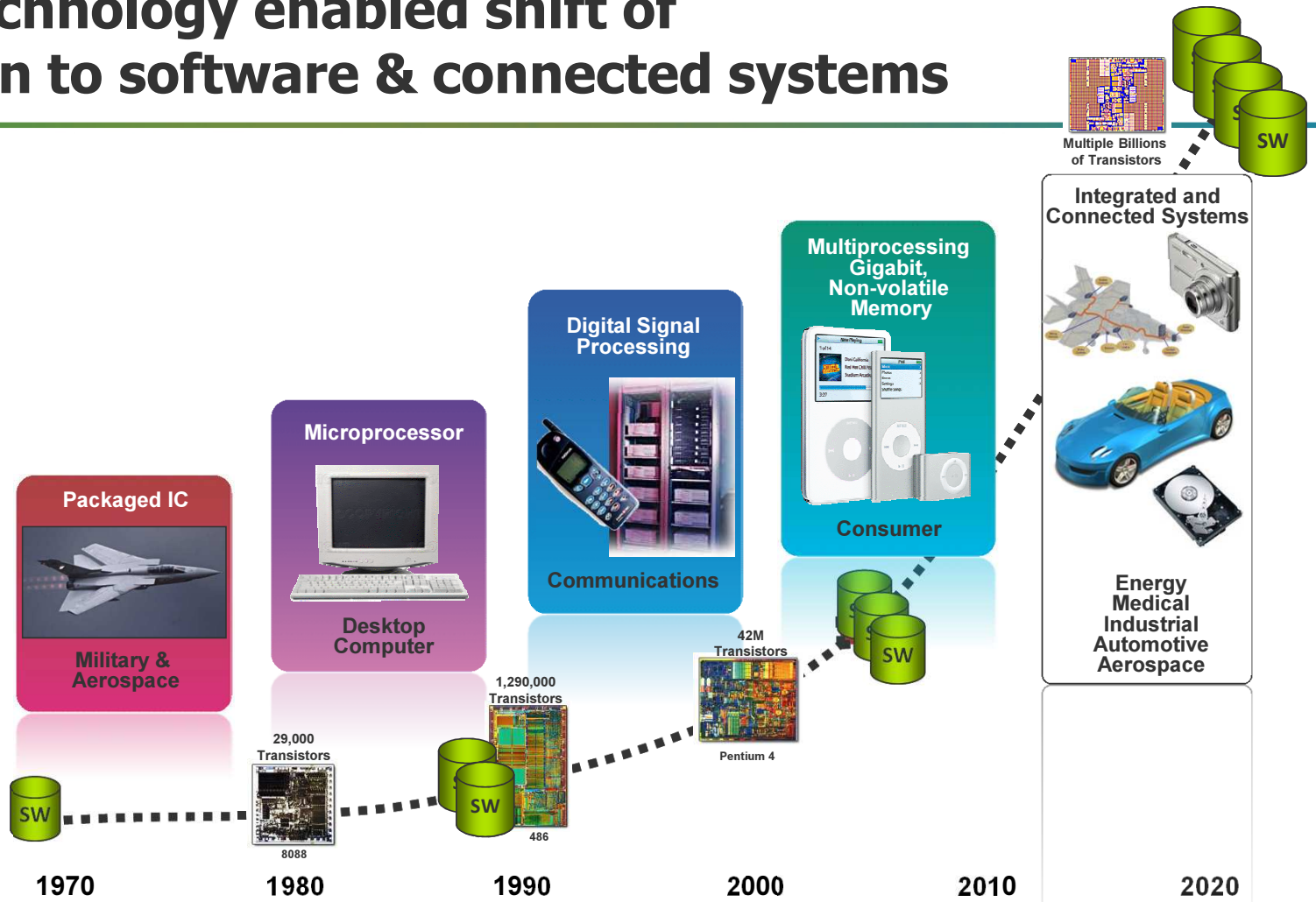


"We are running out of ideas on what else to put on the chip, so we are staying at ~20M gates for now…"

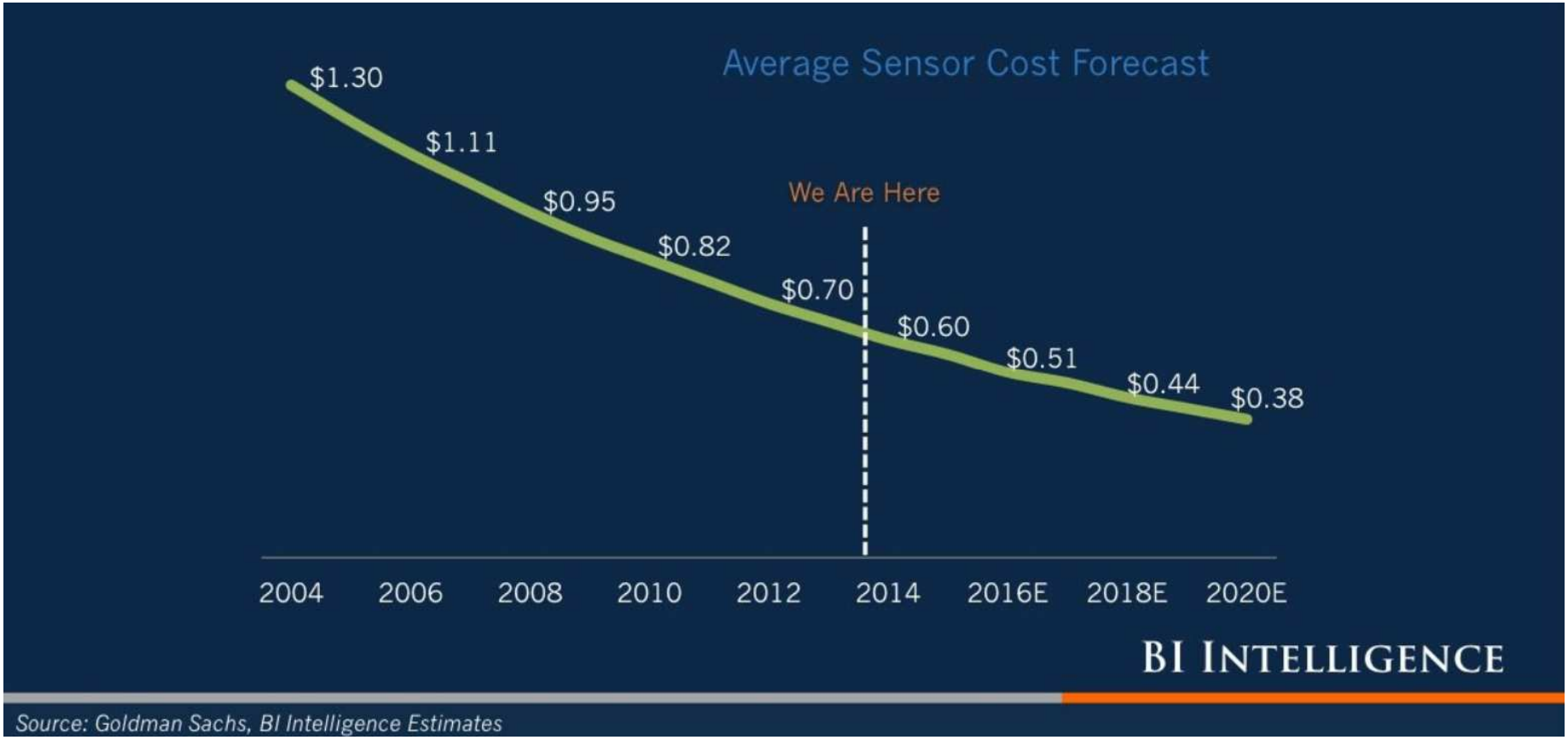
a cell phone company executive in 2005

- Since 2005 we found many more features that are needed

Silicon technology enabled shift of innovation to software & connected systems

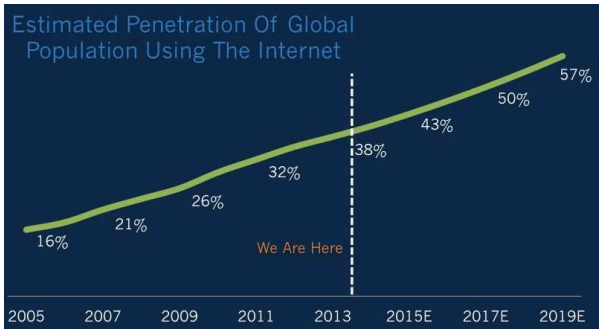


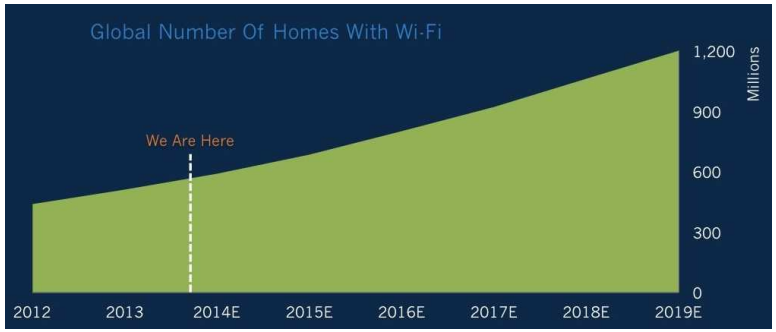
…Meanwhile cost of sensors has declined



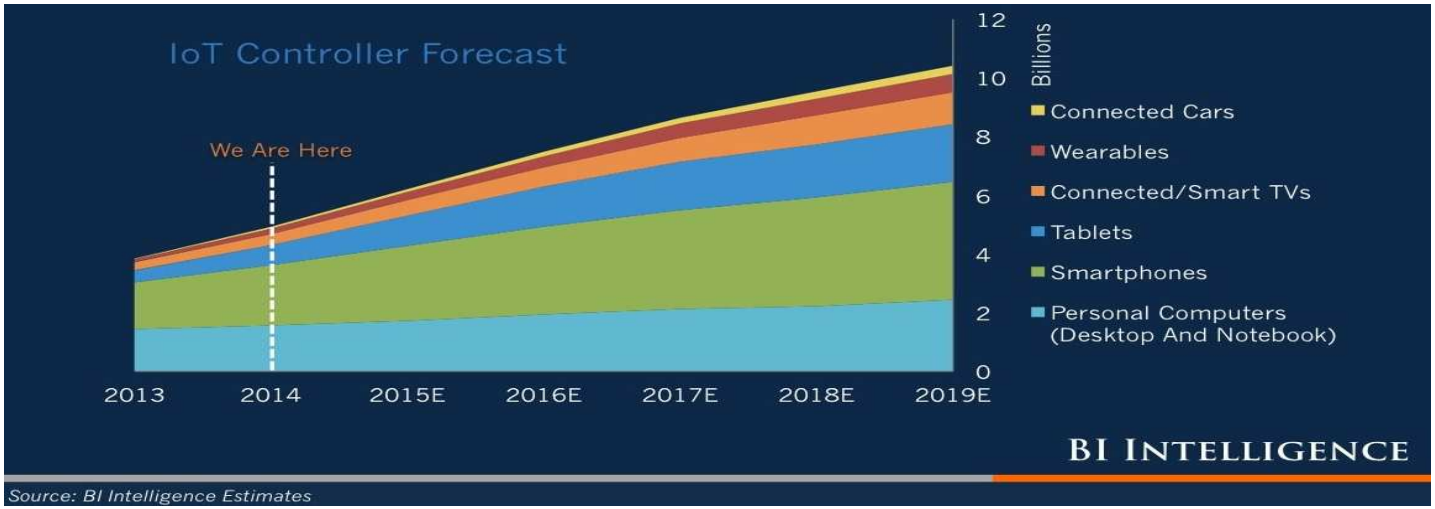
Source: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?op=1

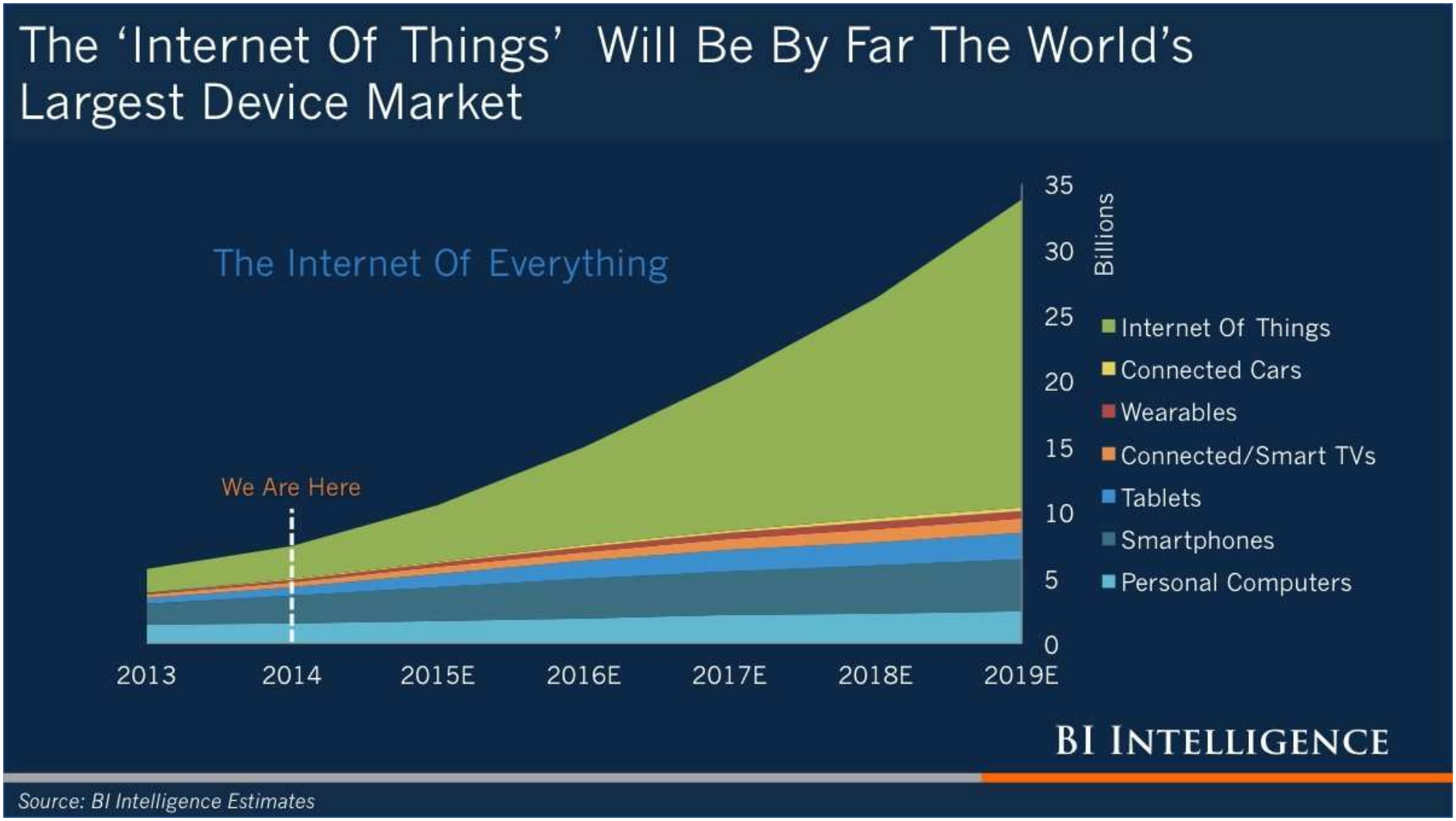
…And internet connectivity exploded





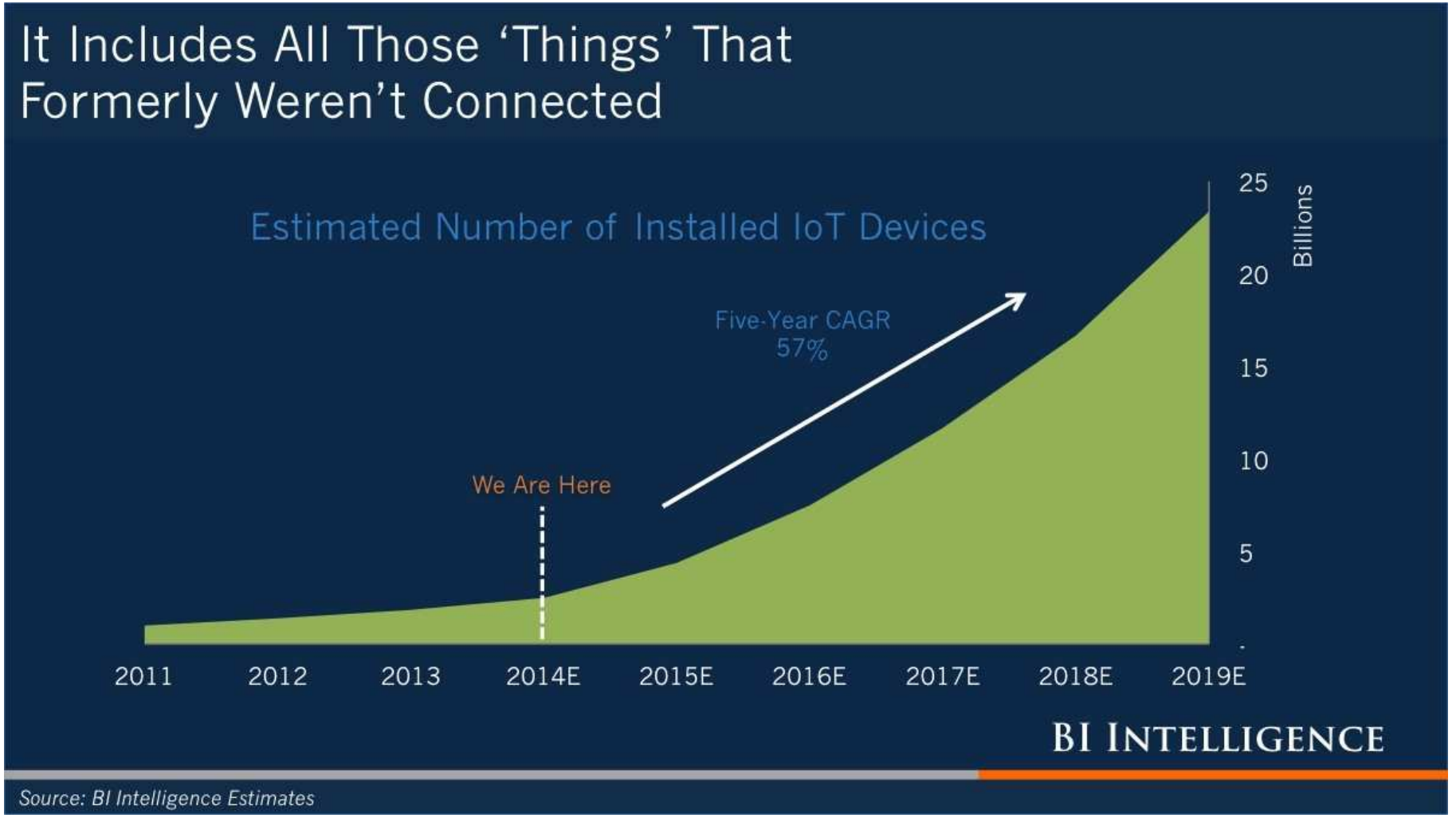
Source: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?op=1





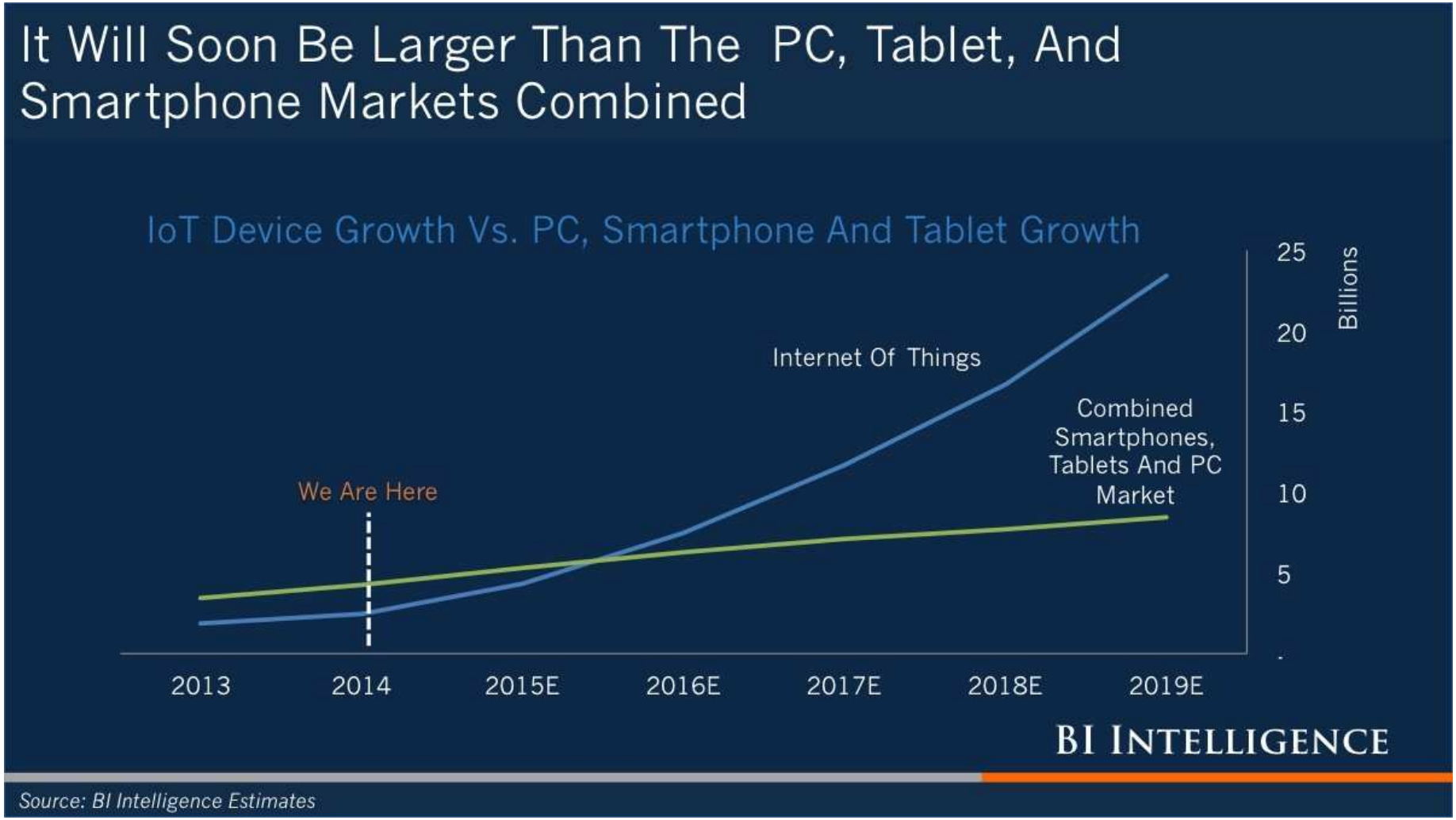
 Source: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?op=1

It Includes All Those 'Things' That Formerly Weren't Connected



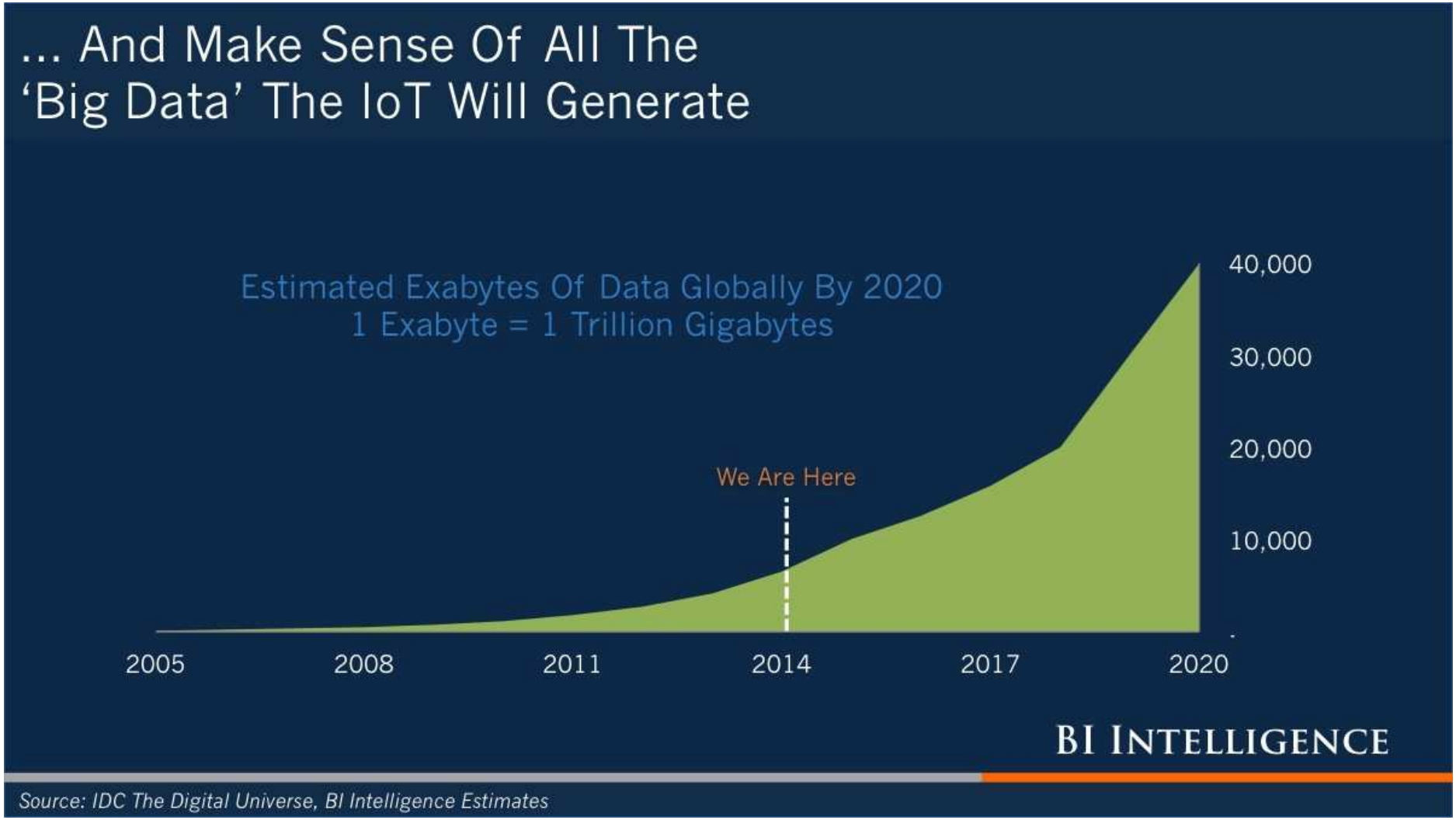
Source: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?op=1

It Will Soon Be Larger Than The PC, Tablet, And Smartphone Markets Combined



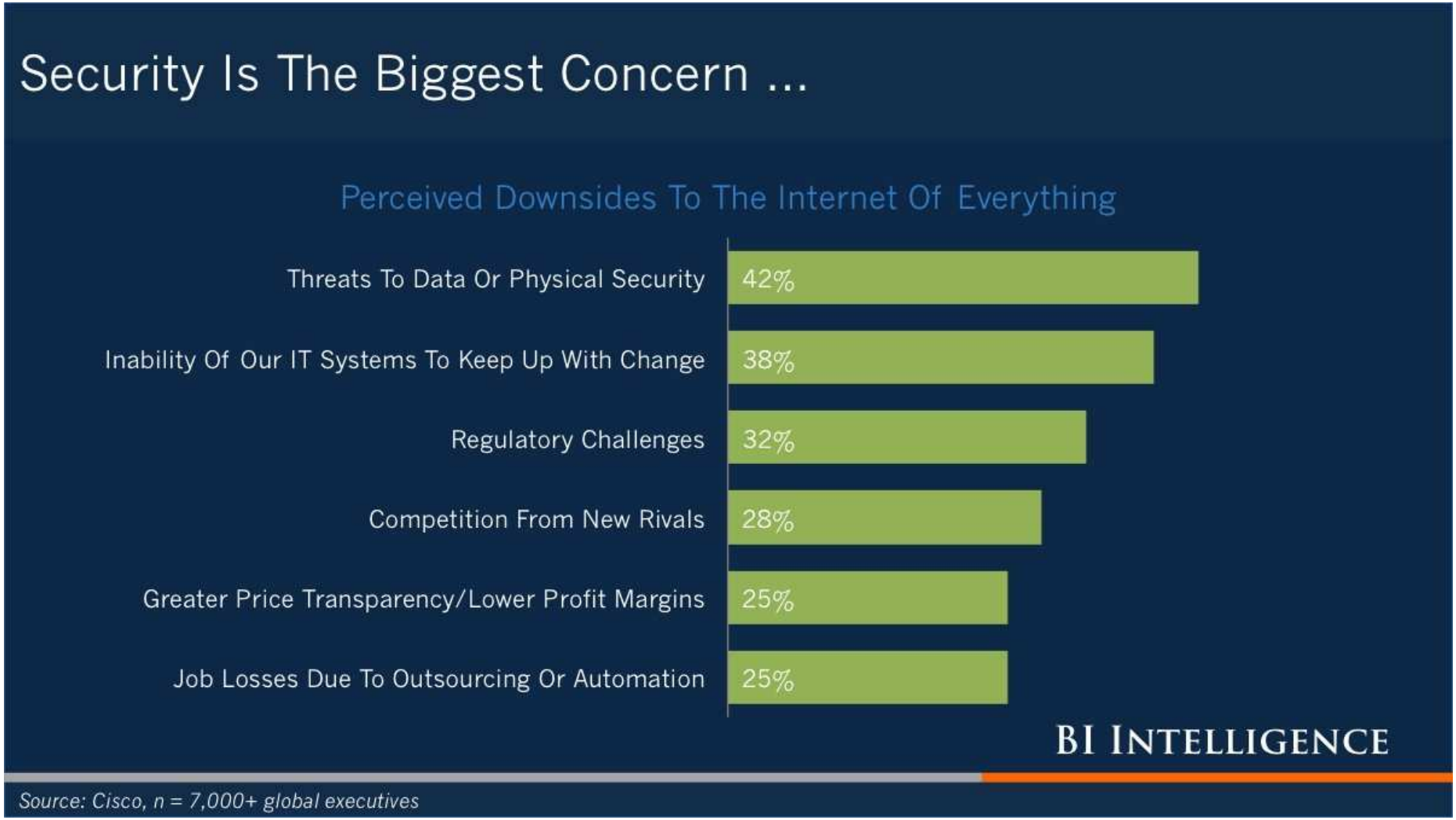
Source: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?op=1

… And Make Sense Of All The 'Big Data' The IoT Will Generate



 Source: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?op=1

Security Is The Biggest Concern ...



 Source: http://uk.businessinsider.com/internet-of-everything-2015-bi-2014-12?op=1

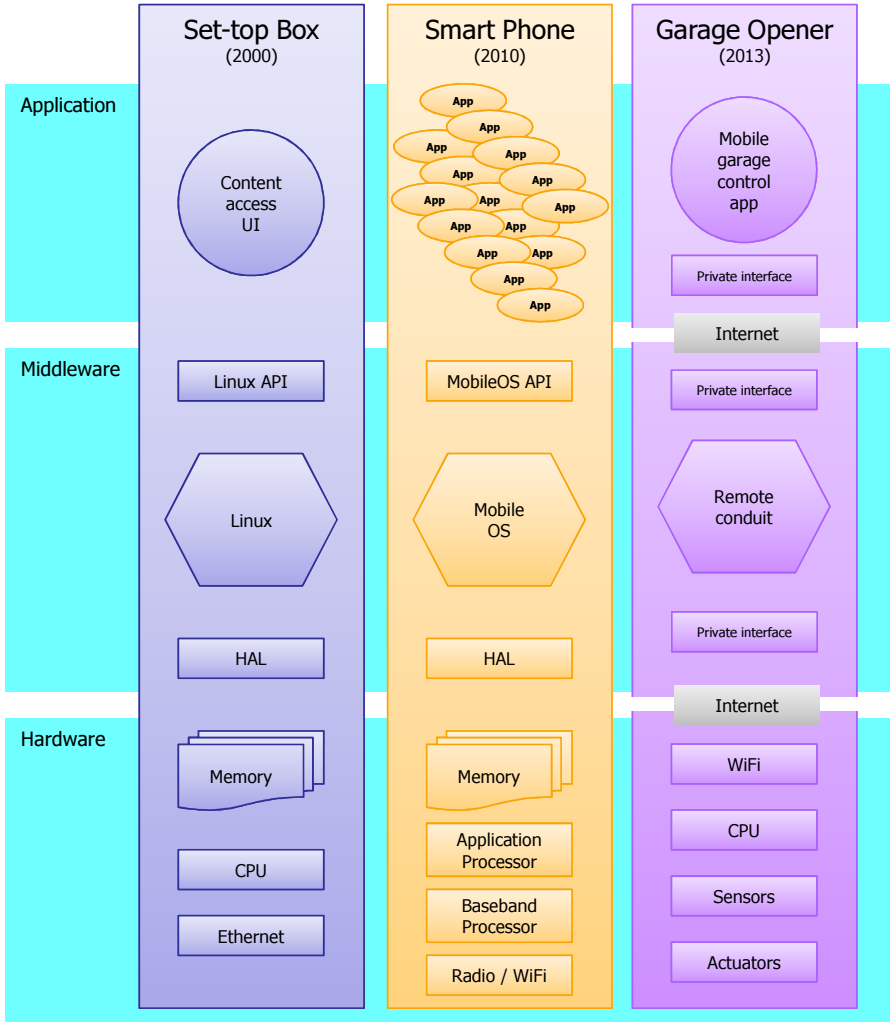
METAMORPHOSIS OF EMBEDDED SYSTEMS

What is IoT?

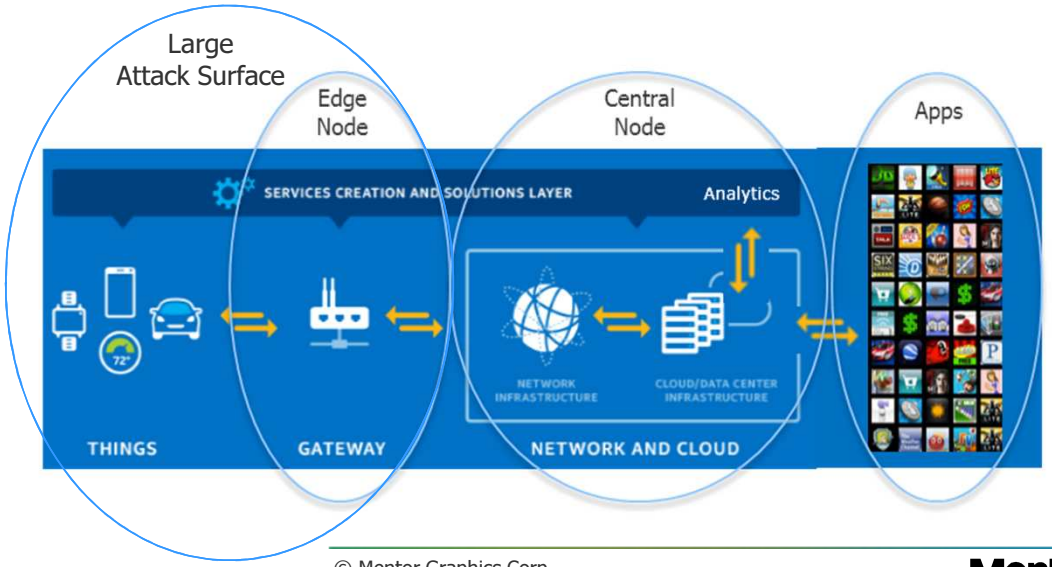
- **Internet** connected general purpose computers
- **Internet of Things** connects everyday objects to **Internet**

- Everyday objects have to be re-designed to include **computers**
  - Standalone TV becomes a "Smart TV" by connecting to Internet and offering on-demand content, shopping, browsing, e-commerce
  - Standalone Garage Door Opener becomes smart by connecting to your smart phone over Internet

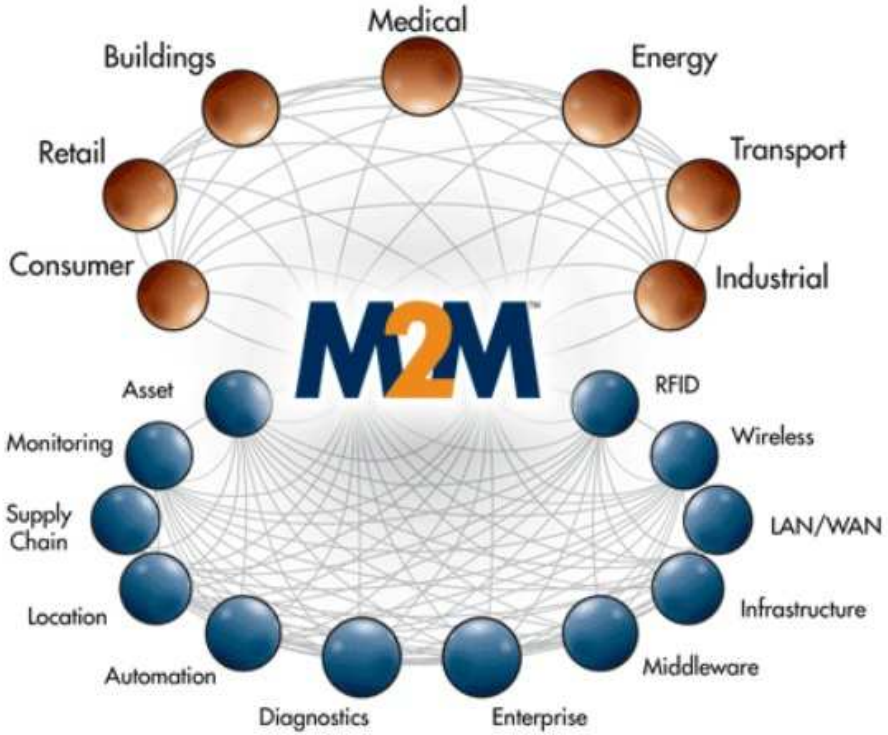
Transformation of Embedded Systems into IoT world

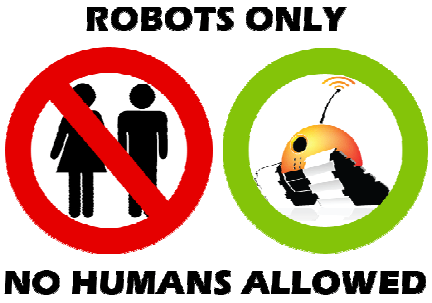


- Definition of embedded system is changing, it's morphing into a connected IoT end node



Next Generation:
Objects interact without human facilitation





Next-Next Generation?

Internet of Things: Computing in 2015 - 2020

Humans are still part of the picture…

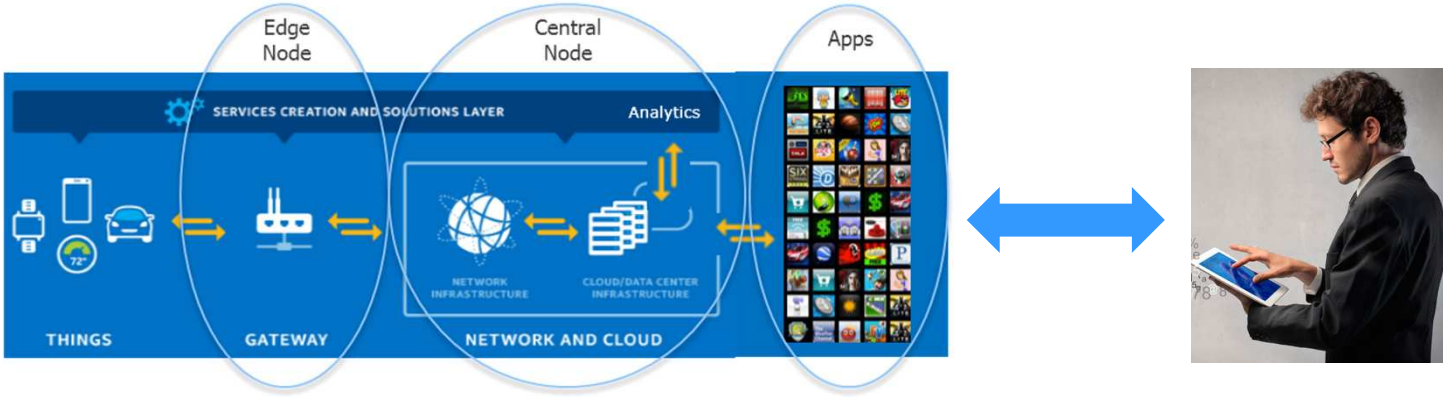
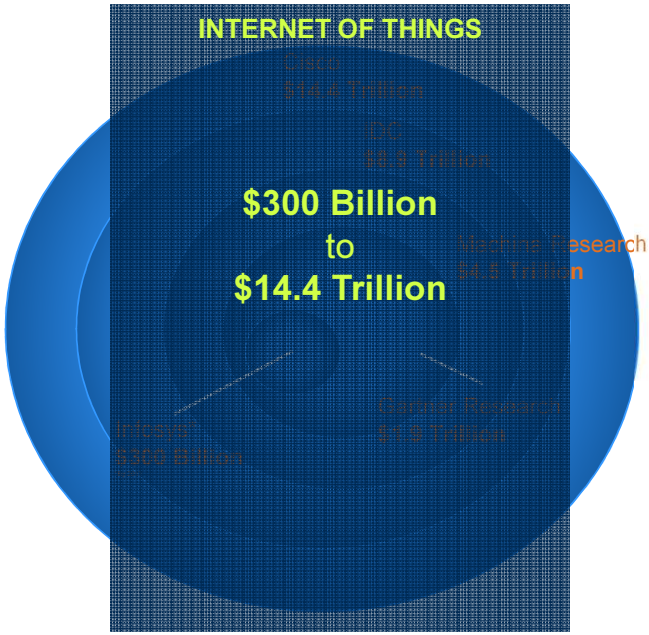
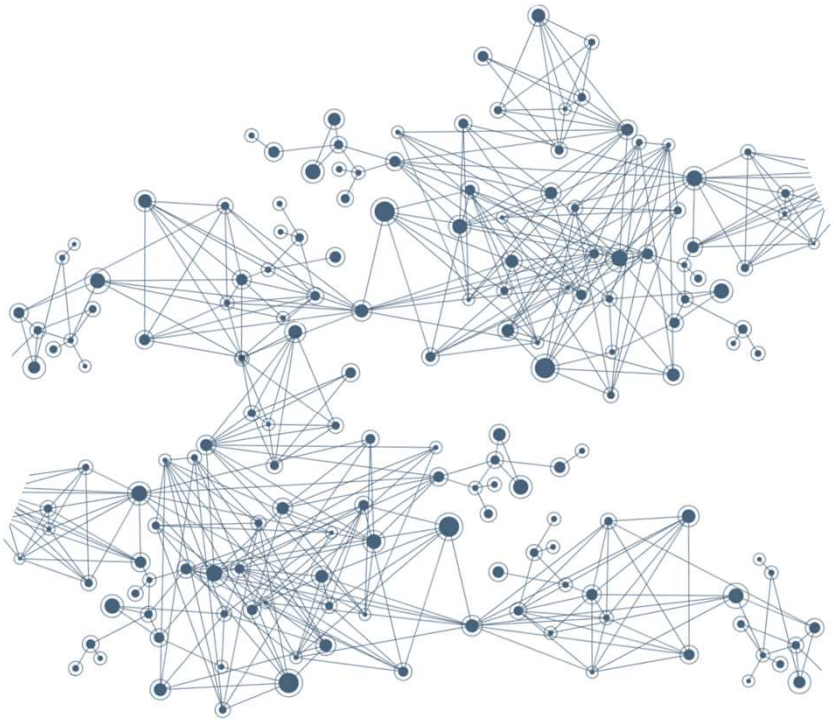


*Image uses elements from Intel Corp web site

DOMAIN DRIVEN
END-TO-END APPLICATIONS

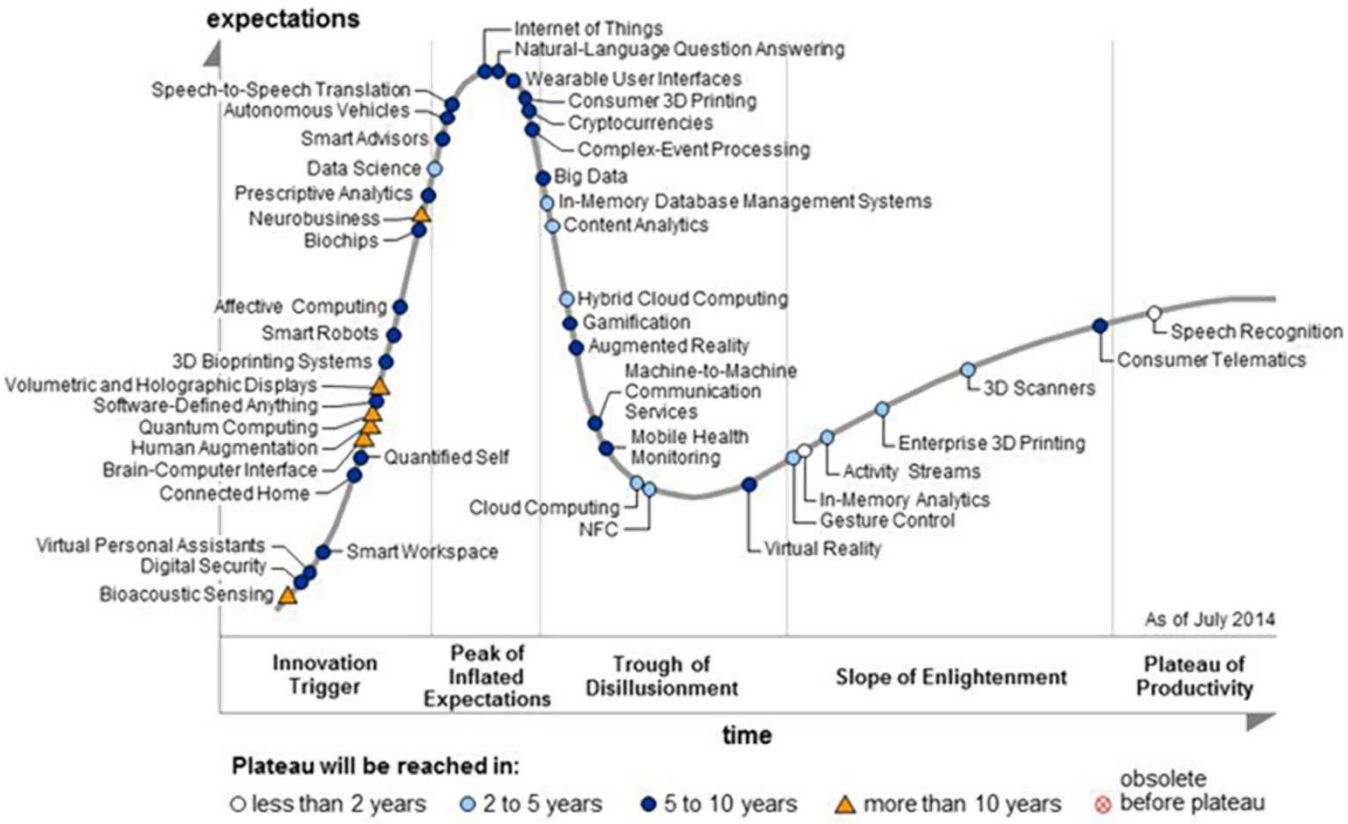
IoT Projected Market Size Generates Excitement





HYPE IN 2015 AROUND THE INTERNET OF THINGS (IOT)

Source: Gartner (August 2014)

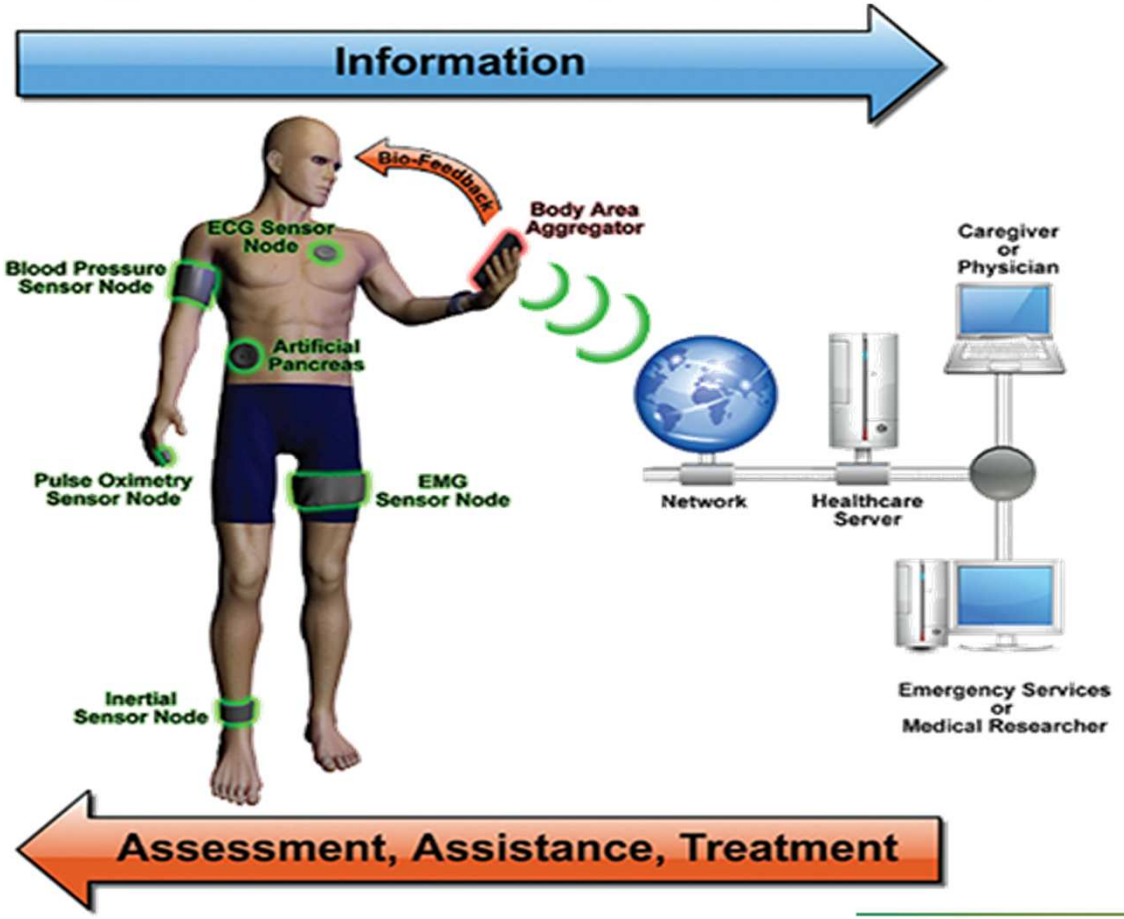


- …But
  - — IoT is not a singular homogeneous thing
  - — It's an enabler for numerous vertical applications…
- …Where
  - — Domain expertise

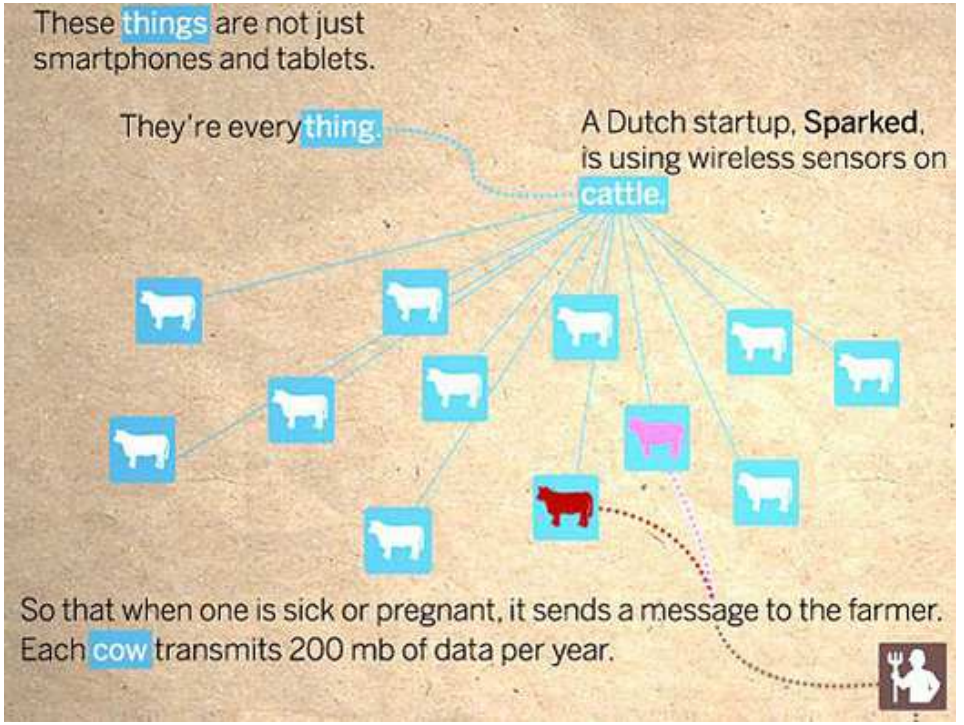
meets

  - — Mobility, Sensors
  - — Limitless storage
  - — Infinite compute power
  - — Pervasive internet access

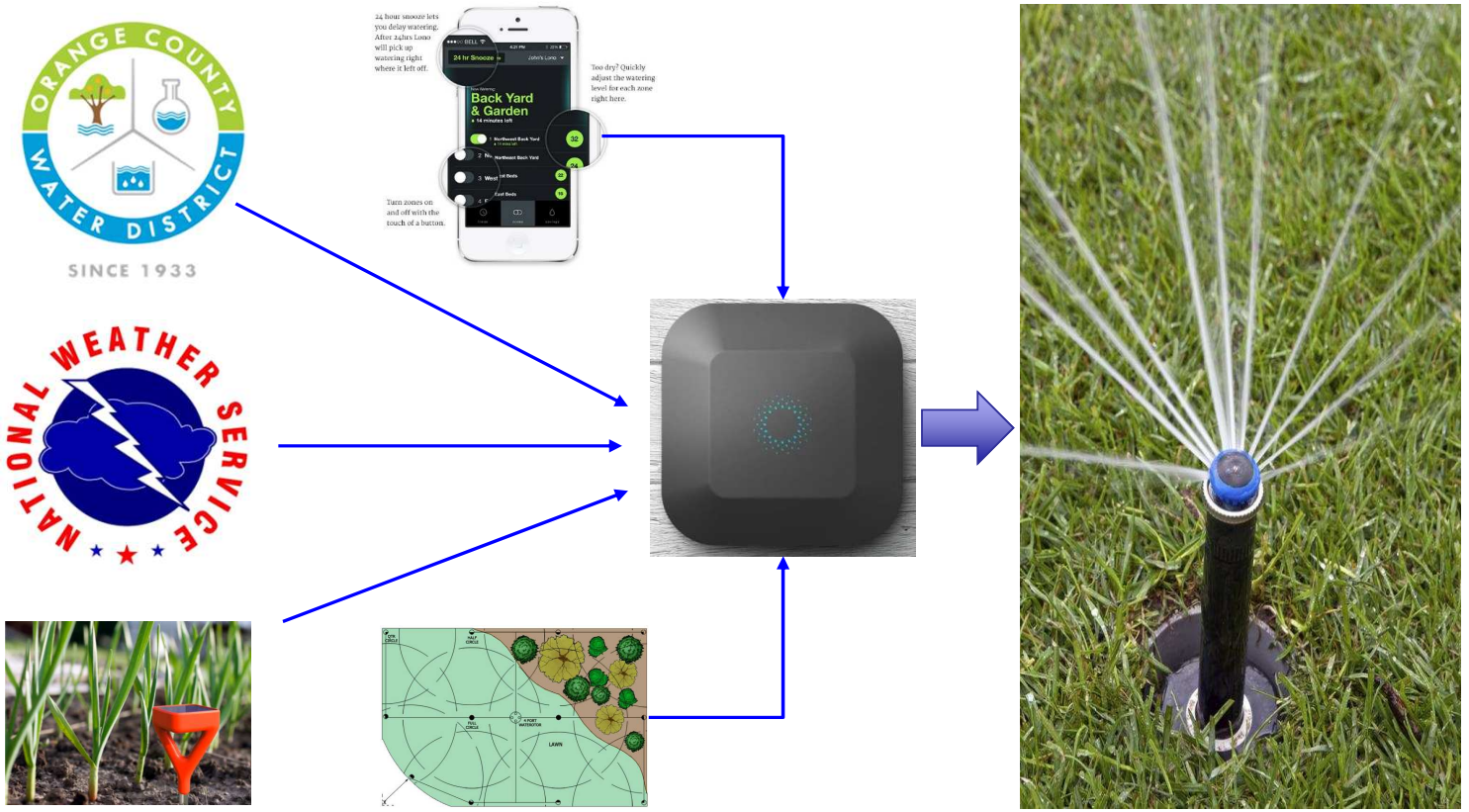
IoT Health Care Application



IoT Agribusiness: Connected Cows



IoT Smart Garden: Lawn Sprinklers



IOT ENABLEMENT TOOLS AND TECHNOLOGIES

How can EDA enable the IoT system developers?

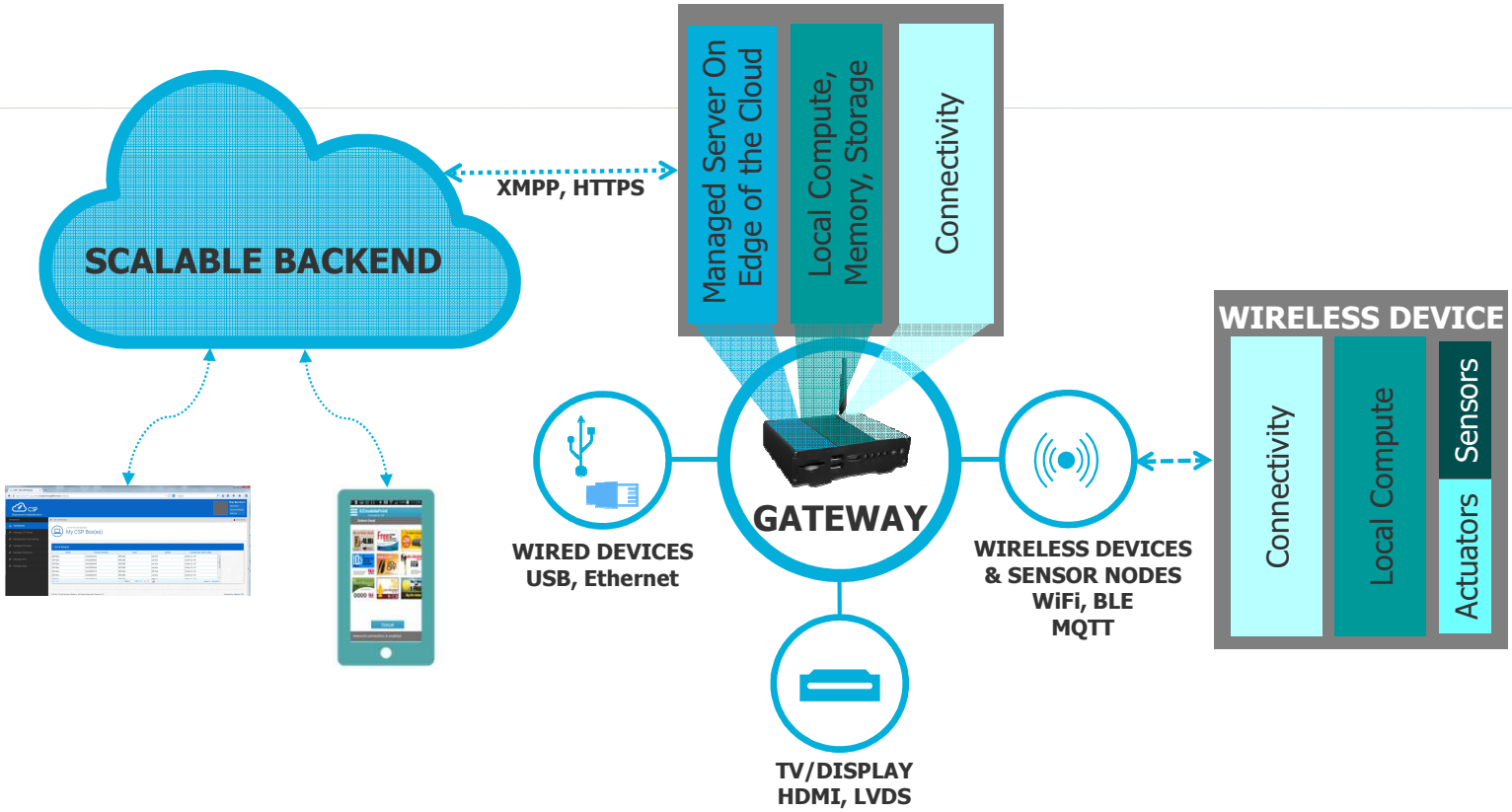
- **Technology Platform** – End-to-End, Customizable IoT platform
  - Hardware: Customizable Gateway/Aggregator
  - Software
    - Automated and Scalable Cloud-Hosted Backend (Central Node)
    - Cloud connectivity middleware, device management, cloud services
    - OS and tools for Secure Converged Gateway software
    - Embedded software for edge devices

- **Platform as a Service** – Managed IoT Platform

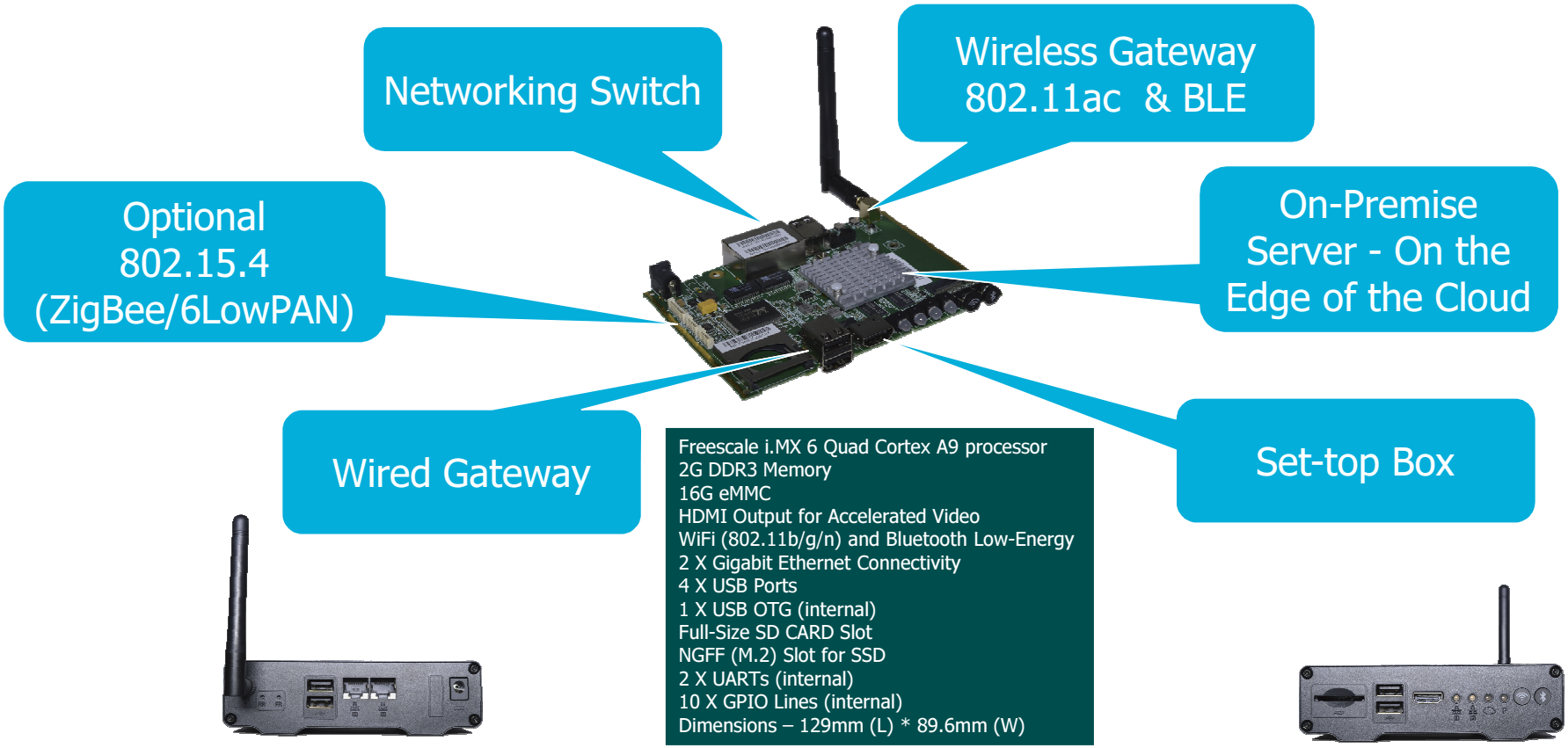
  Managed complete technology solution that includes the Central Node, Gateways and/or customer's devices

- **Solution as a Service** – Turnkey End-to-End Managed Solution

  Architect, implement, integrate, run, and support vertical solutions



Gateway is a High-Performance Computer, Managed Remotely From a Cloud-Hosted Backend



M2M and IoT Cloud Platform

Managed Solutions	Managed REST Services APIs		
	M2M Applications	Web Applications	IoT Applications
Device and Data Services	Managed REST Services APIs		
	Managed RESTful Device Services APIs	Managed RESTful Data Services APIs	RESTful Admin Services APIs and Admin Portals
Managed & Scalable "IT" Infrastructure	Server Templates & Recipes from RightScale		
	Server Provisioning Server Lifecycle	Server Scaling & High Availability	Server Monitoring & Analytics
Vendor-Independent Cloud Infrastructure	Cloud Vendor APIs		
	Amazon Web Services	Google Cloud Services	Private Clouds, Additional Public Clouds

MANAGED DEVICE SERVICES

- Device provisioning
- Device monitoring
- Utilization monitoring
- Event logging
- Remote device control
- Remote firmware updates
- Remote driver updates
- Remote feature unlocking
- Analytics & Big Data

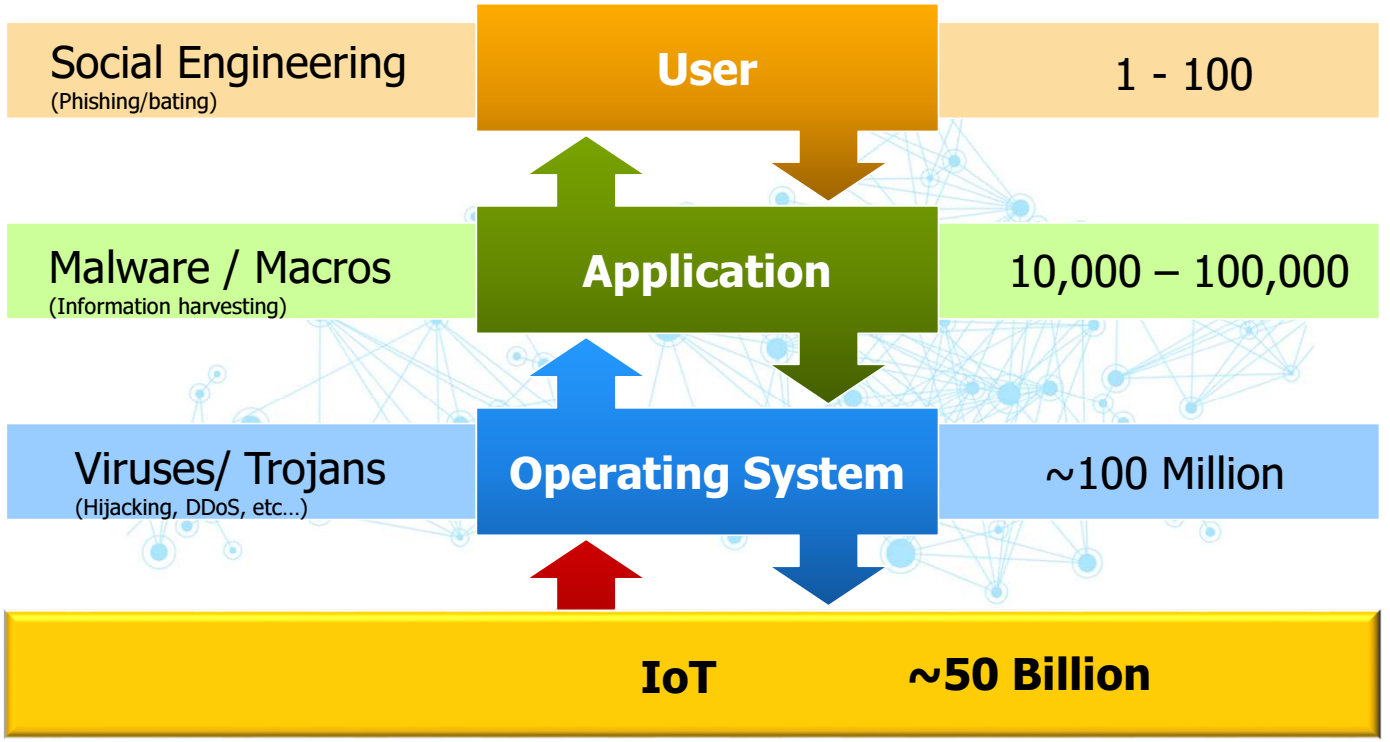
Example vertical applications

Smart Lobby

Managed Climate Control

SECURITY IMPLICATIONS OF A LARGE ATTACK SURFACE

"Race to bare metal" – cyber attacks move lower in the stack …and IoT egde nodes are "soft targets"…



IoT World is Already Under Attack

Proofpoint Research: Internet of Things (IoT) Cyber Attack Security

In January 2014, Proofpoint researchers discovered proof of a much-theorized but never before seen Internet of Things (IoT) cyber-attack. Proofpoint has observed what we believe to be an industry first of devices, including some home appliances (TVs, a refrigerator), sending malicious email spam.

As our researchers were analyzing email-borne threats, they observed a recent cyber attack campaign where more than 25 percent of the malicious email (over 750,000 messages) came from things that were not conventional laptop or desktop computers, but rather members of the Internet of Things; a "Thingbot"-net*.

Specifically, researchers observed a series of cyber attack campaigns:

- From Dec 23rd through Jan 6th
- Three campaigns per day, approximately 100k emails per campaign
- Over 450k unique IP addresses; over 100k were from IoT devices

A more detailed examination suggested that while the majority of mail was initiated by "expected" IoT devices such as compromised home-networking devices (routers, NAS), there was a significant percentage of attack mail coming from other non-traditional sources, such as connected multi-media centers, televisions and *at least one refrigerator*.

Additionally, observing the devices:

- A vast number of the devices are running embedded linux servers (usually busybox)
- Some use mini-httpd, some apache
- Some are ARM devices, some are MIPS (or something very similar) others are based on an embedded Realtek chipset (for example, media players)
- Some are believed to be game consoles
- Some are NAS devices (one specific brand has open telnet, open ssh and an SMTP server - all unsecurable)
- Some set-top boxes were also seen as exploited

This proof of a systematic compromise of IoT devices and its subsequent use of those Thingbots to further attack other networks is something we've never seen before. This suggests an unfortunate future for both home users and enterprises, the latter of whom now faces an even larger volume of malicious attack capacity.

Worse, these compromised home appliances provide a mechanism where users can unknowingly expose their work environment to such cyber attacks. All a user has to do is use a remote RDP connection, or conceivably simply take an action like checking their fridge from their work PC. If a classic drive-by or even a redirect has been installed, the work PC is now compromised (though this is arguably more farfetched). Clearly, as the trend towards smart devices and BYOD increases, the risk of enterprise exposure increases correspondingly, exponentially.

SiliconANGLE » The Internet Of Things Is Under Attack!

The Internet of Things is under attack!

MELLISA TOLENTINO | JANUARY 30TH

READ MORE

Tweet 22 | +1 0 | Like 3 | Share 6

Most of us enjoy using some kind of Internet of Things device these days – after all, IoT devices run the whole gamut of smaller gadgets, including smartphones, tablets, cars, homes, wearable devices and home appliances that are connected to the Internet, as they make our lives so much easier.

Unfortunately, as with anything that connects to the Internet, it can be exploited by hackers, and though some of you may think that hacking an Internet connected refrigerator is not a big deal, cybercriminals can use information from that to access your other online accounts.

Internet security firm Proofpoint recently described how it had uncovered the first proven IoT-based attack which involved 750,000 malicious email communications coming from over 100,000 everyday consumer gadgets, including home-networking routers, connected multi-media centers, televisions and at least one refrigerator.

'Bash' bug could let hackers attack through a light bulb

By Jose Pagliery @Jose_Pagliery September 25, 2014: 12:54 PM ET

Recommend 1.5k

2K TOTAL SHARES | 815 | 274 | 271 | 151

NEW YORK (CNNMoney)

Say hello to the bash bug, a lesson in why Internet-connected devices are inherently unsafe.

Computer security researchers have discovered a flaw in the way many devices communicate over the Internet. At its most basic, it lets someone hack every device in your house, business or government building -- via something as simple as your "smart" light bulb.

With this flaw, criminals can potentially break computers or steal private and government information.

HP: Most IoT Devices Lack Security, Open To Attack

Thu, 07/31/2014 - 3:18pm

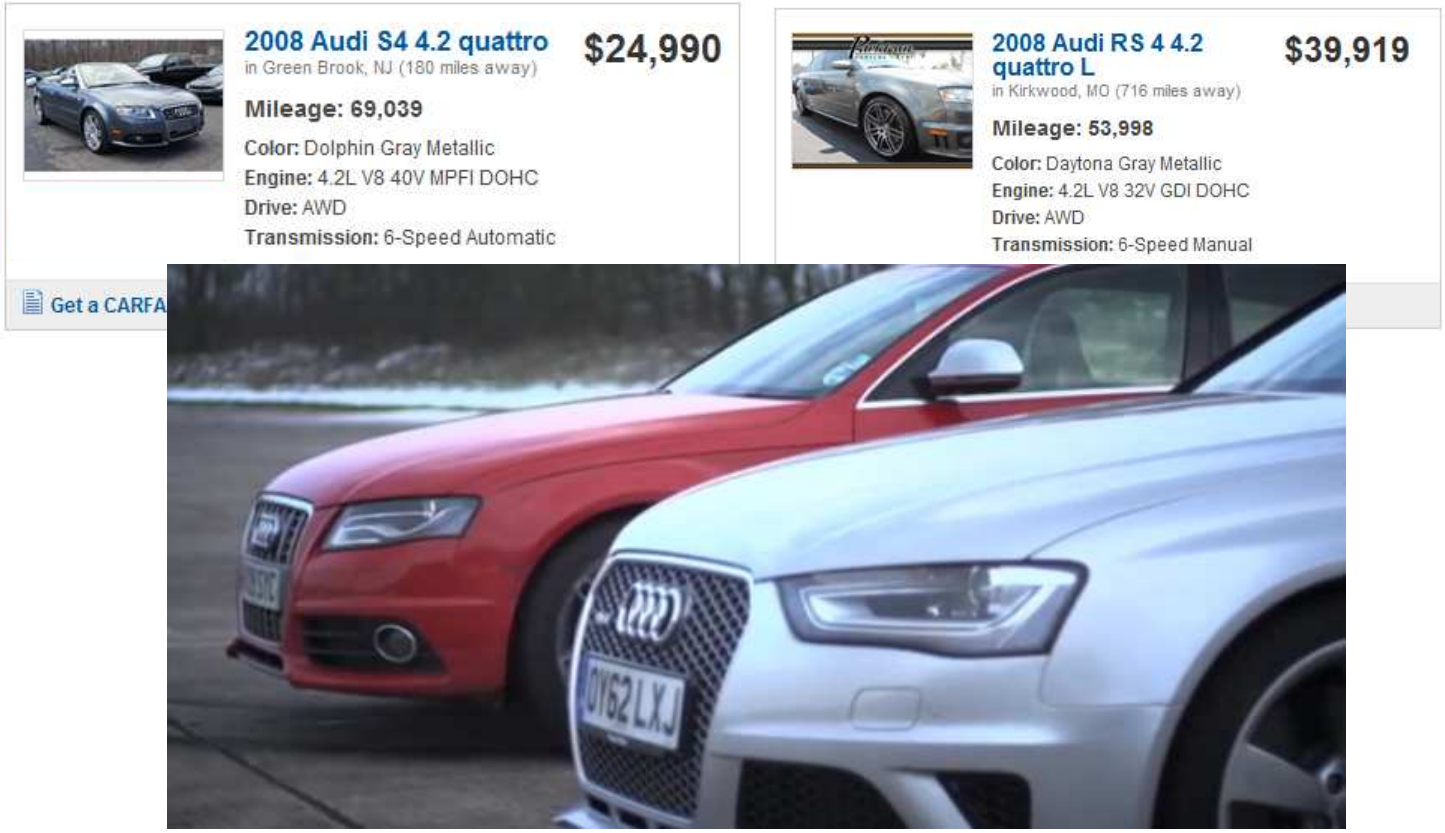
by Jon Minnick, Associate Editor, Manufacturing Business Technology

Get today's manufacturing headlines and news - Sign up now!

A recent study from Hewlett-Packard reveals that 70 percent of Internet of Things (IoT) devices — including sensors and connected infrastructure — are seriously vulnerable to attack. The Internet of Things State of the Union Study from HP's Fortify on Demand division came about after hearing a lot about IoT, but saw nothing that focused on the complete picture of IoT security.

Hack Your Audi S4

And Get the Horse Power and Torque of an RS4

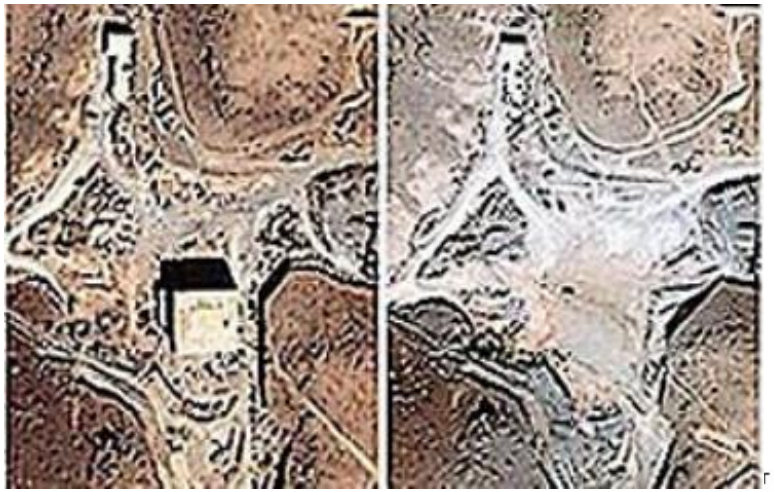


Source: Chris Harris Proves the Power of ECU Tweaks with Audi S4 vs RAS4 Comparative Test, Carscoop, April 4, 2013

Syrian Radar Case

“September 2007, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of Syrian radar, supposedly state of the art, to warn the Syrian military of the incoming assault. It wasn’t long before military and technology bloggers concluded that this was an incident of electronic warfare and not just any kind. Post after post speculated that the commercial off-the-shelf microprocessors in the Syrian radar might have been purposely fabricated with a hidden “backdoor” inside. By sending a preprogrammed code to those chips, an unknown antagonist had disrupted the chips’ function and temporarily blocked the radar”

Source : IEEE spectrum, 2007

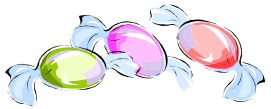


Stuxnet Virus **- Delivered by Infected USB Flash Drive**

"Stuxnet, a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran"

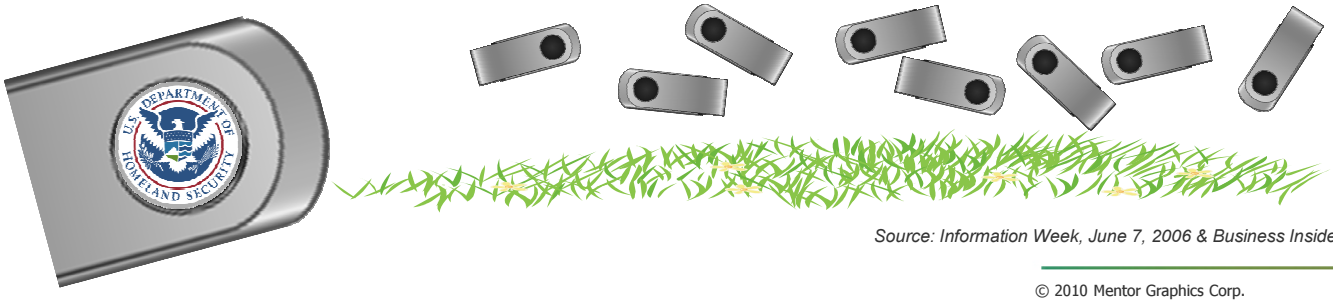
IEEE, "The Real Story of Stuxnet", February 26, 2013

The "Candy Drop"



- Security firm hired to test data security of credit union
  - — Scattered 20 infected USB flash drives in parking lot, picnic and smoking areas
  - — 15 were plugged into company computers
  - — Passwords, logins and other information were compromised

- U.S. Department of Homeland Security Test
  - — USB flash drives scattered in government parking lots
  - — 60% of those found were plugged into networked computers
  - — 90% of those with official logos were plugged in



Source: Information Week, June 7, 2006 & Business Insider, July 24th 2013

Hardware Attack Types

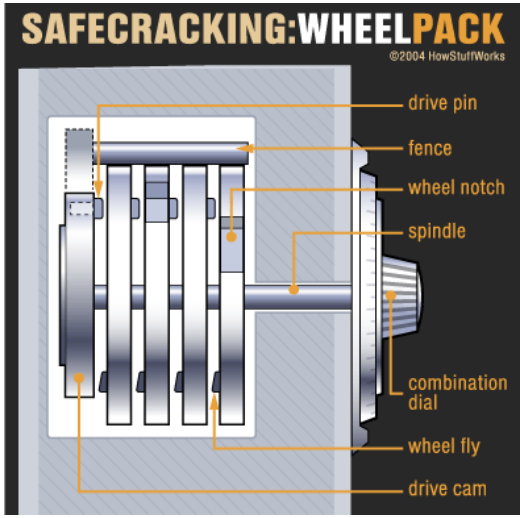
- 'Side-Channel' Attacks - (SECRET EXTRACTION)

- Malicious Logic inside Chip - (TROJANS)

- Counterfeit Chips - (SUPPLY CHAIN ATTACKS)

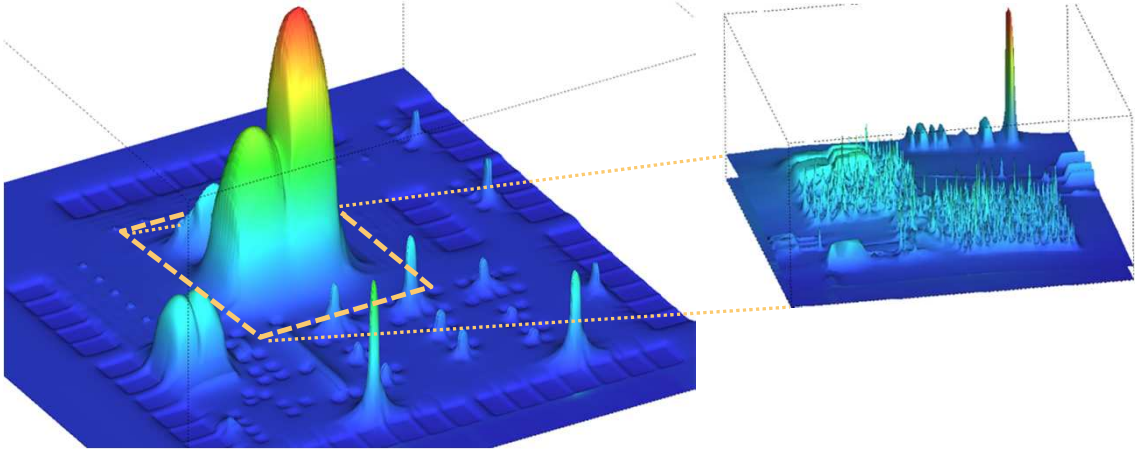
Side-Channel Attacks

To crack safes, it's essential to know how they work



DPA: Differential Power Analysis

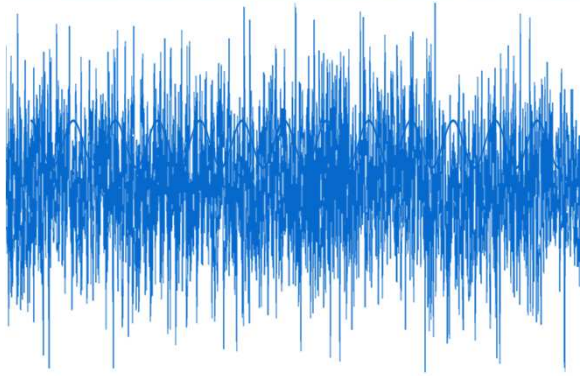
- Thermal images can help in locating cryptographic circuits
  - Attempts to enter candidate keys should exercise crypto
  - This results in visible power dissipation

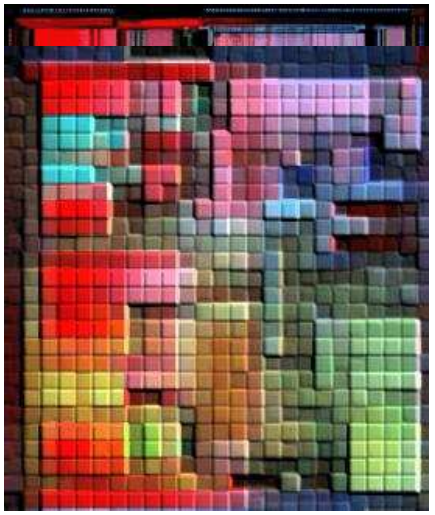


- Subsequently, different power dissipation patterns can be observed based on correct or incorrect key entry attempts
- Keys can then be inferred

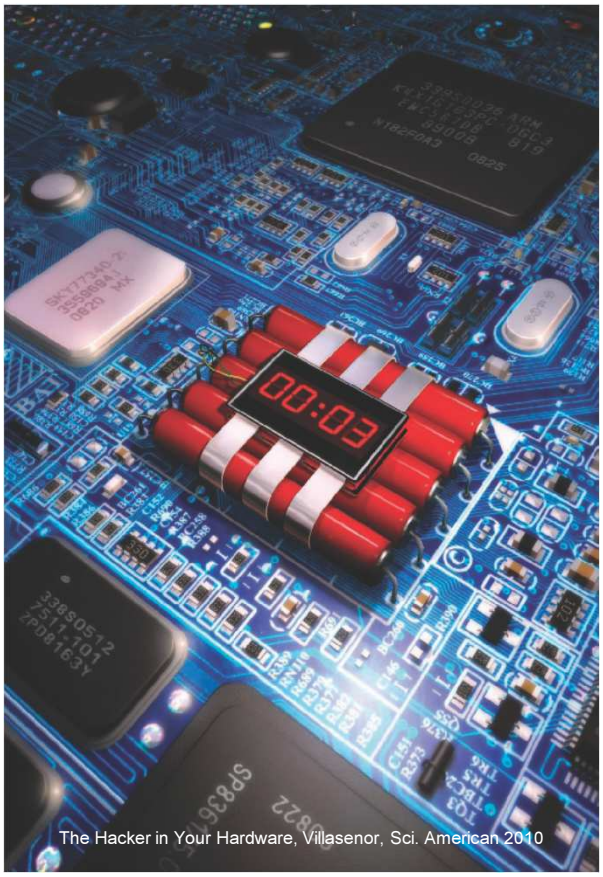
Countermeasures for Side-Channel Attacks

- Incorporate **randomness** into cryptography
- Use **fixed-time algorithms** to reduce data-related timing signatures
- **Camouflaging** structures from reverse engineering





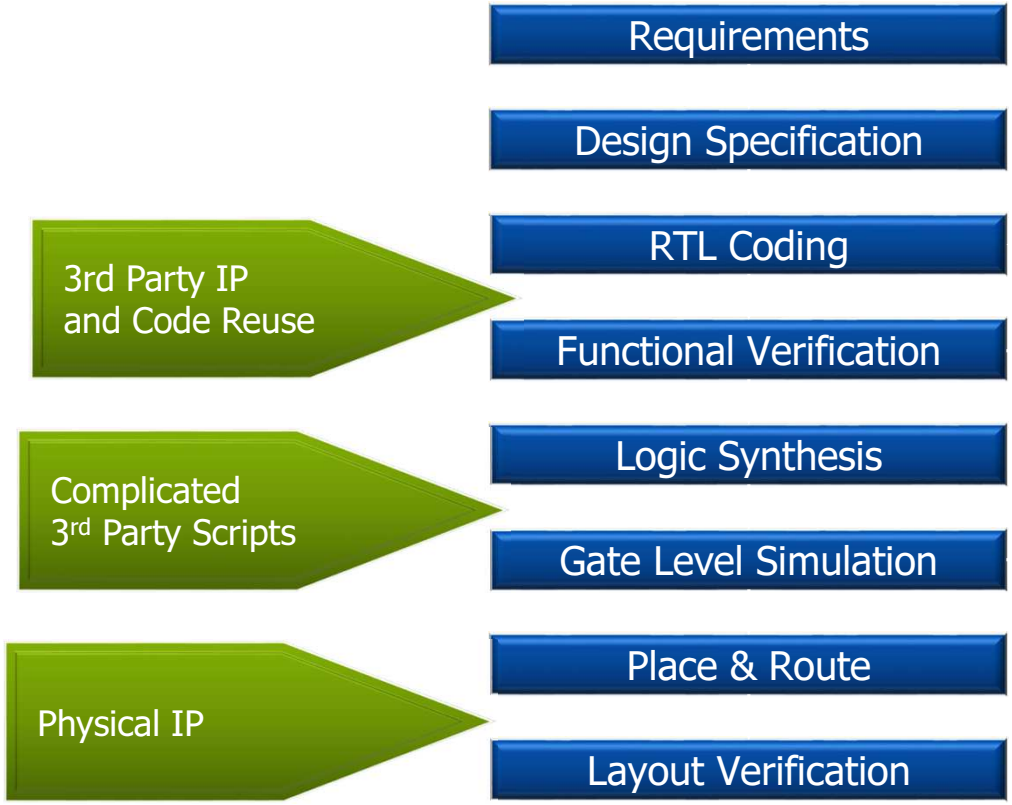
Hardware Trojans



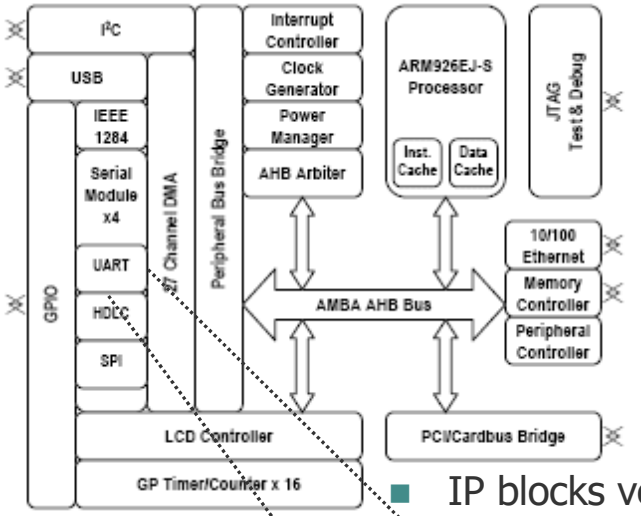
The Hacker in Your Hardware, Villasenor, Sci. American 2010

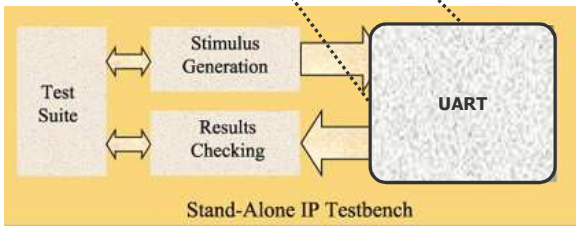
- Rogue hardware injected into the design/chip
  - Untrusted IP cores (design phase)
  - Untrusted fab (fab phase)
  - Triggered subsequently
    - Special date/time
    - Receipt of special signal
- Payload = Malicious Action
- Types of Attacks
  - Kill switch: Breaking the system
  - Backdoor: Gaining access to the system. e.g., sending confidential data off-chip
- Easiest entry point: 3rd party IP

Attacking IC Design Flow



Countermeasures: Run-time Detection?

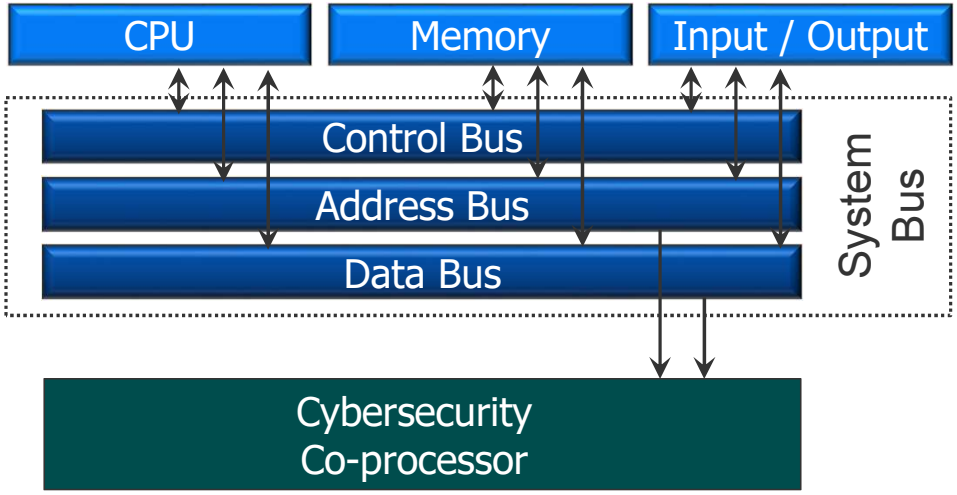




- IP blocks verified for functionality
- A key question **NOT** asked is:

"Does this block do anything ELSE?"

- **Co-processor for run-time Trojan detection**
  - Include co-processor in the design as an IP block
- Issues targeted
  - Peripherals with hidden functionality
  - Prevention of undeclared communications

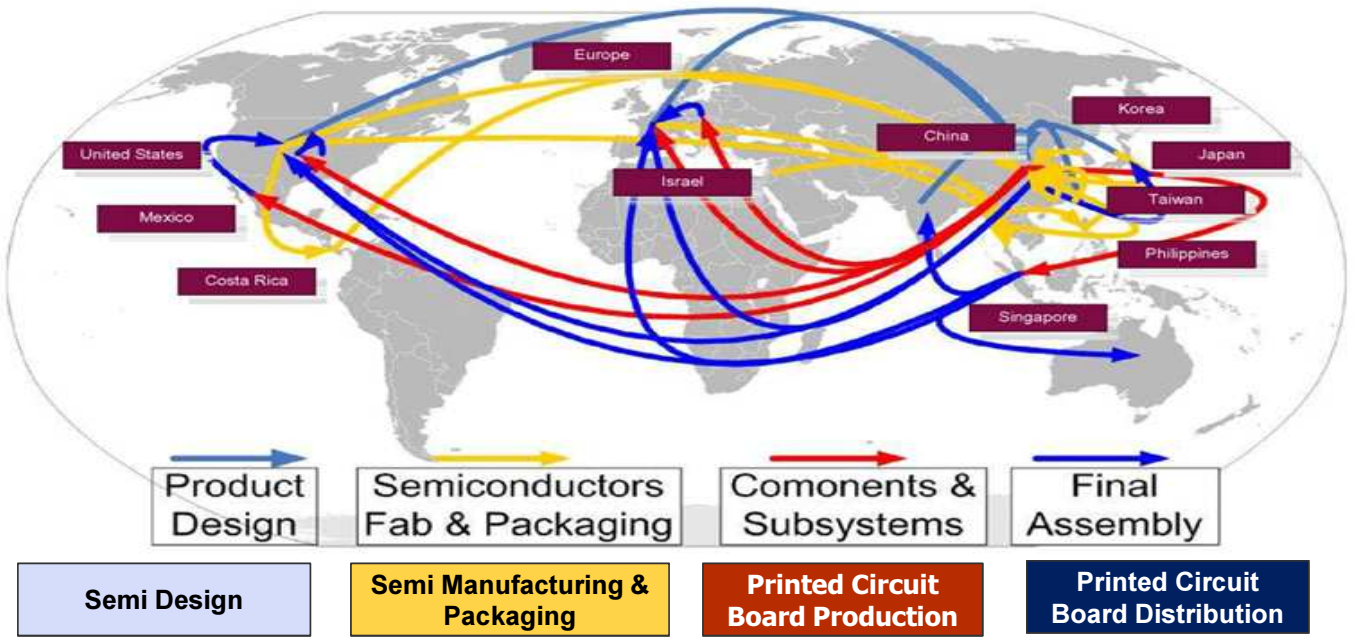


Counterfeit and recycled chips

Lifecycle for a Single IC

JSF (Joint Strike Fighter) Case Study

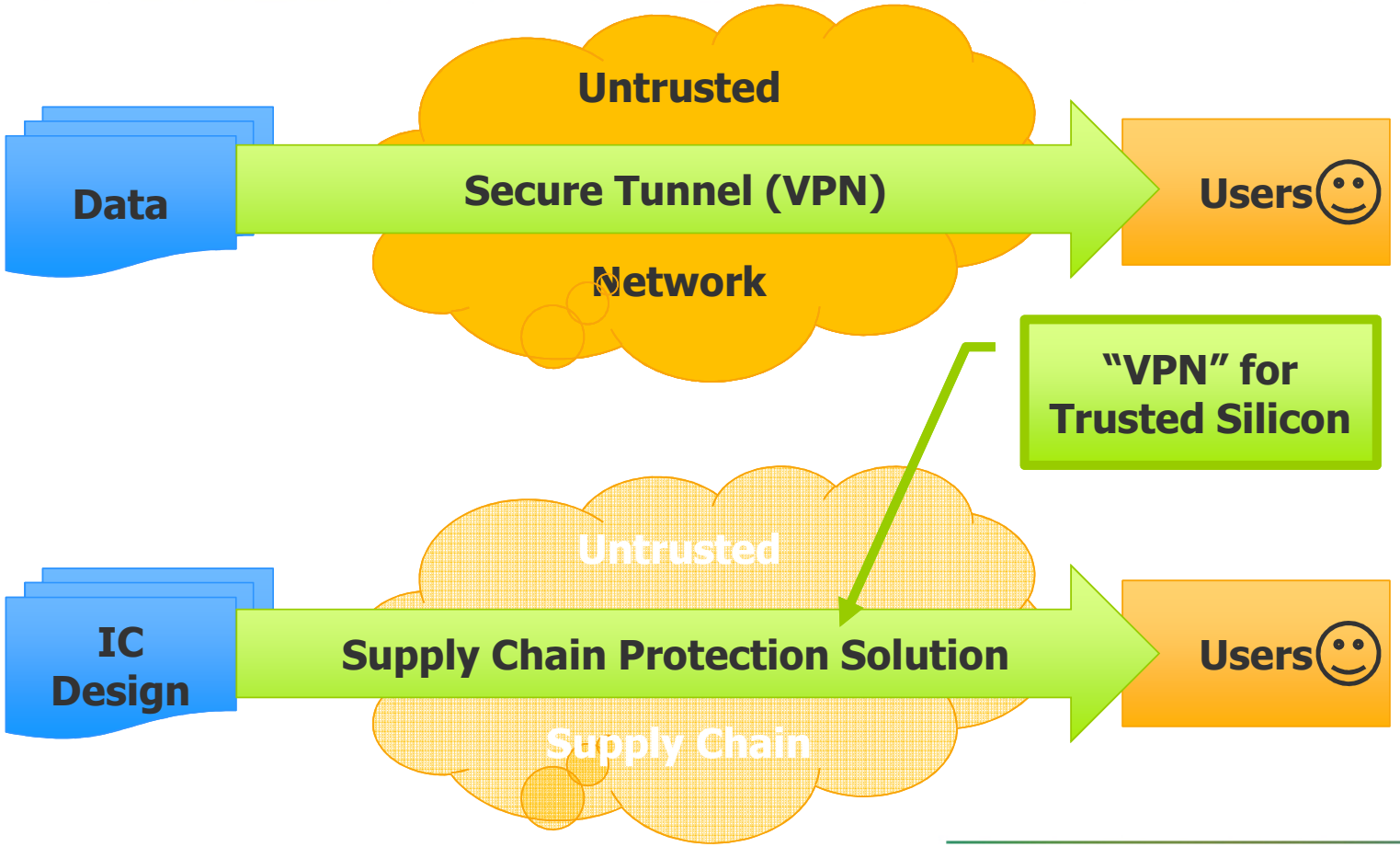
Global nature of supply chain makes chain-of-custody unworkable



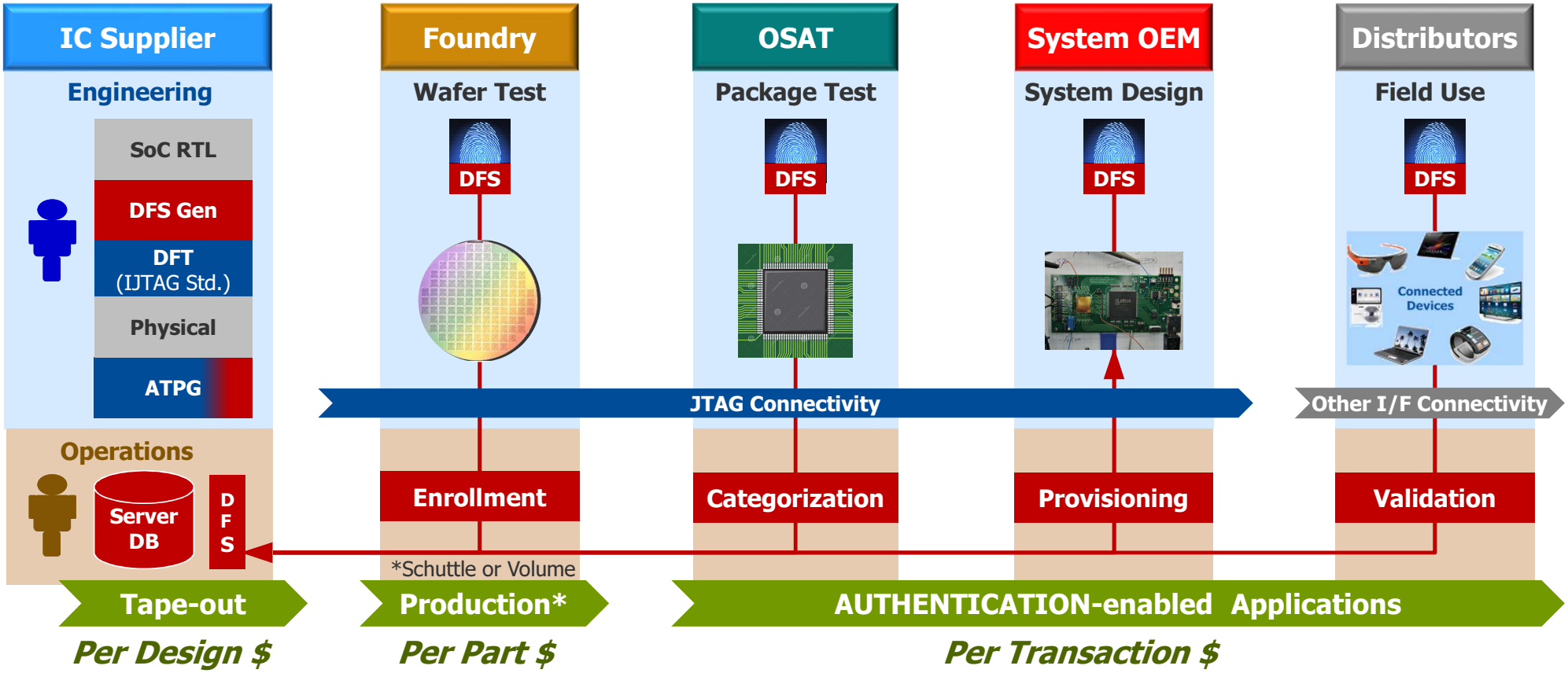
Component changes hands 15 times before final install

Source: IDC Manufacturing Insights & Booz Allen analysis

Creating Secure Silicon in an Untrusted Environment — VPN for Silicon



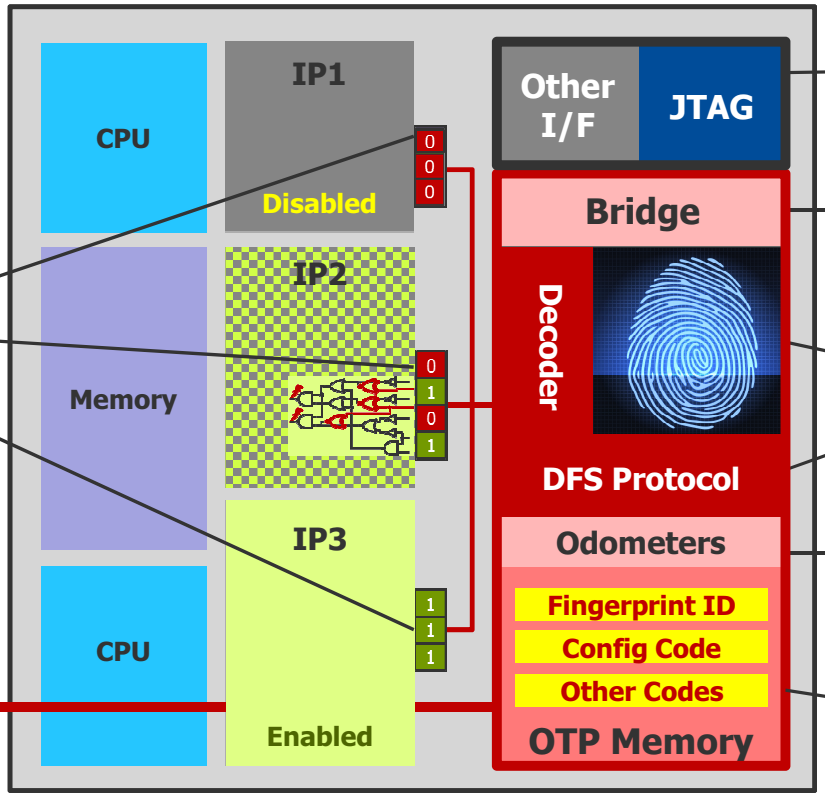
Supply Chain Enablement



Security Subsystem

Config. Registers
Holds decoded values that enable/disable IPs or lock portions of internal logic. These are unique per Chip.

Security Block
Depending upon user-driven configuration and end application



Connectivity Interface
middleman between SoC & Server

Interface Selector
JTAG (Up to OEM), Other (Field)

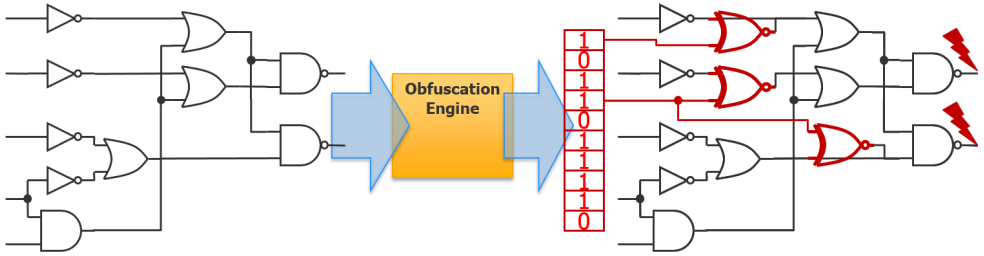
Authentication Hardware
Validates fingerprint in response to server providing a unique FP-Code

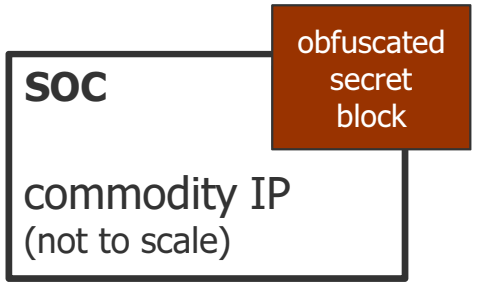
Holds Part Usage Info

Maintains Public Data
Data is decoded to authenticate the SoC or provision its features

Protecting Design and Managing IC Lifecycle

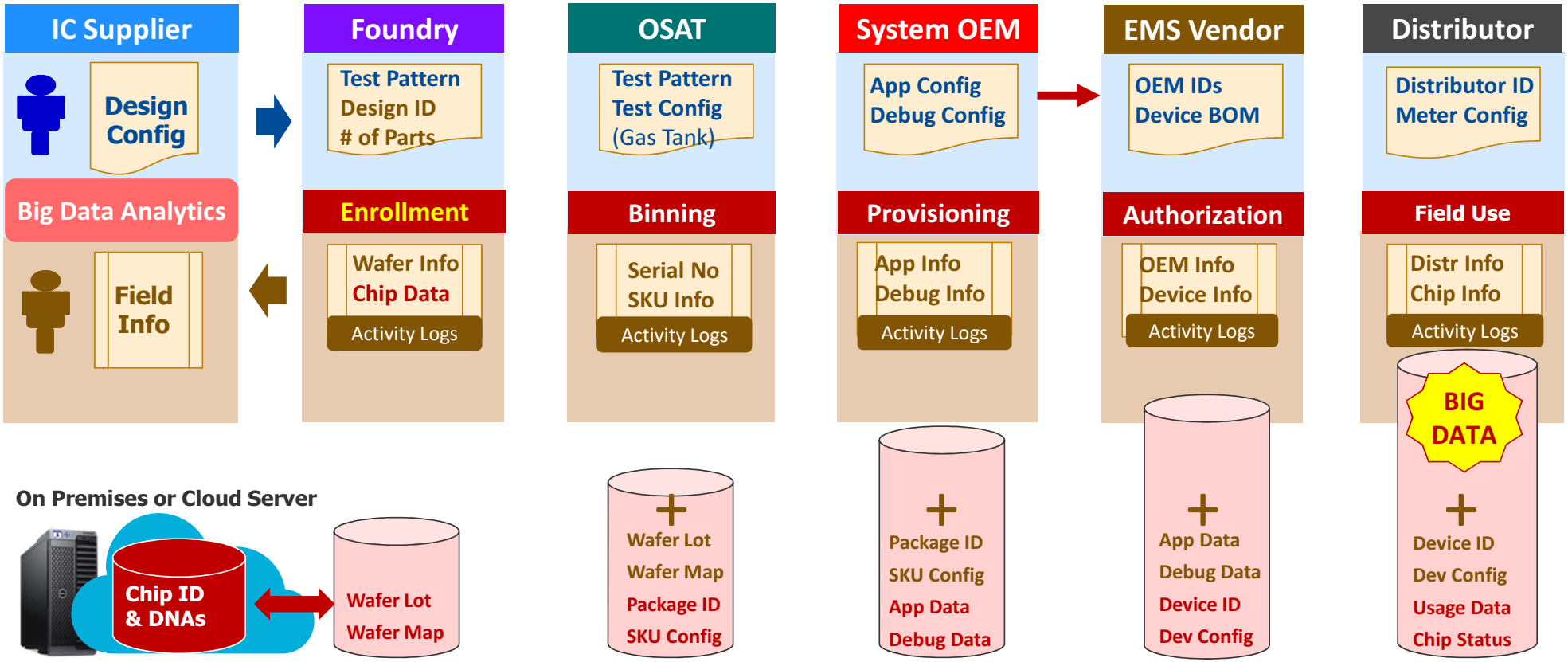
- **Provision IC to obfuscate key design IP inside**
  - Can be achieved by inserting encryption logic in areas to be protected
  - Added area (cost) may not be prohibitive (i.e. 5% for 250M gate design)
  - Strong obfuscation makes it difficult to reverse engineer the IC
  - Potential solution to mitigate for loss of trusted foundry



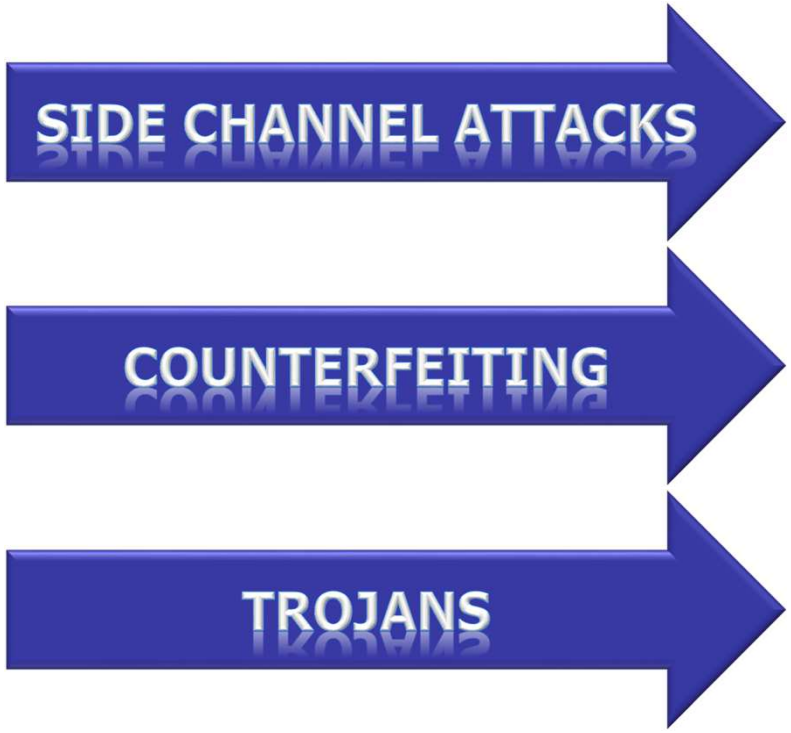


- **Provision Odometers to manage IC lifecycle**
  - Measure usage or status for each IC relative to the stage in its lifecycle
  - Limit usage or disable IC if not connected to server often for a "refresh"
  - Potential to enable new SaaS (Silicon as a Service) business model
  - Manage IC lifecycle and obsolesce relative to the application and usage

Managed SoC Lifecycle Can Drive Opportunities for Big Data Analytics



EDA Will Be the Focal Point of the Countermeasure Strategies



EDA WHERE CYBERSECURITY BEGINS

www.mentor.com