RIOT CONTROL
The Art of Managing Risk for Internet of Things

Kim Singletary
McAfee

Session ID:

Session Classification: Advanced

Intro

- What is IoT and why is it different?
- What are the risks?
- What are the emerging areas that will help provide security
- What can be done today

The Art

The outcome of the application of human creative skills and imagination.

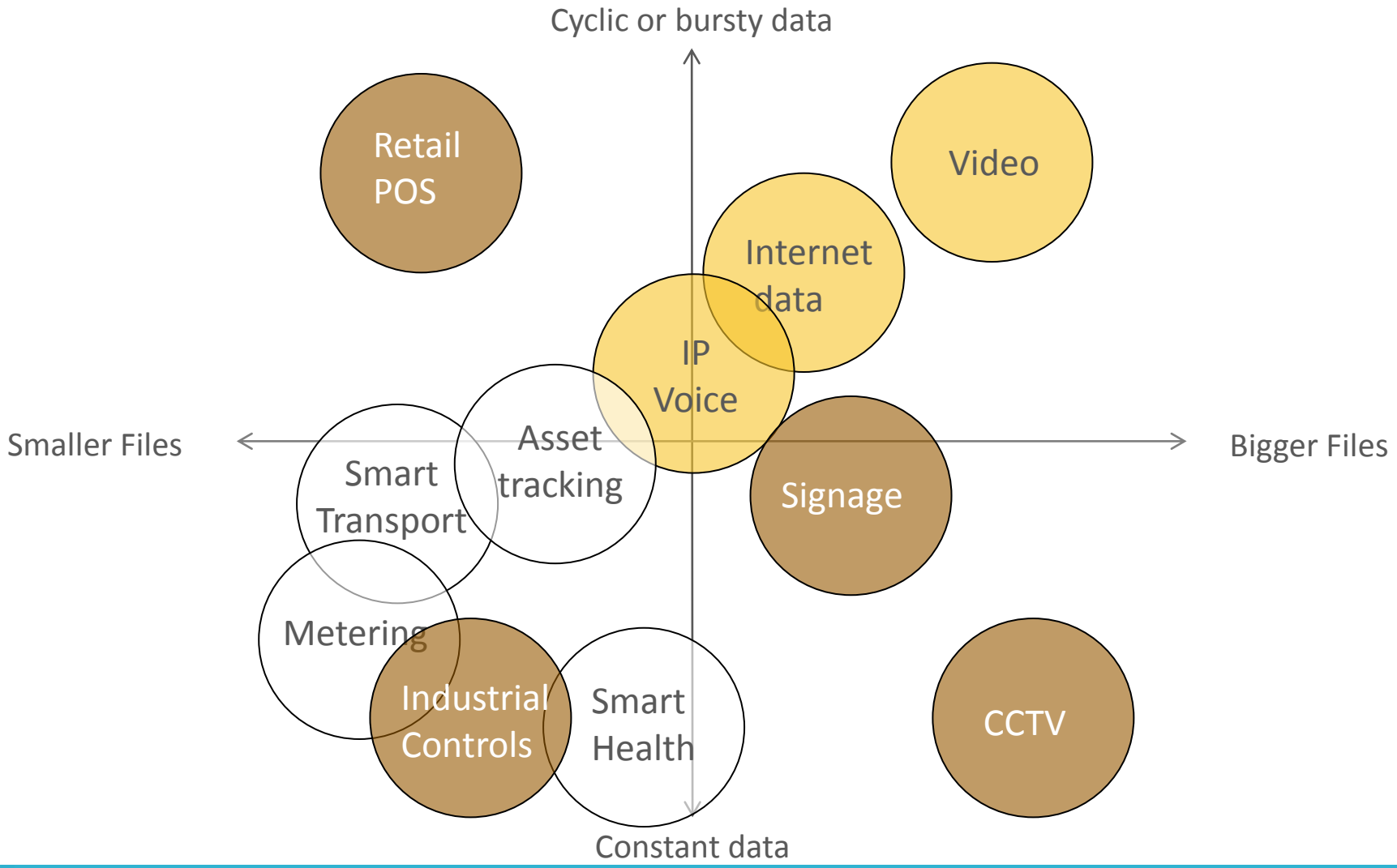
http://news.nationalgeographic.com/news/2012/12/pictures/121205-earth-night-science-space/

IoT is BIG

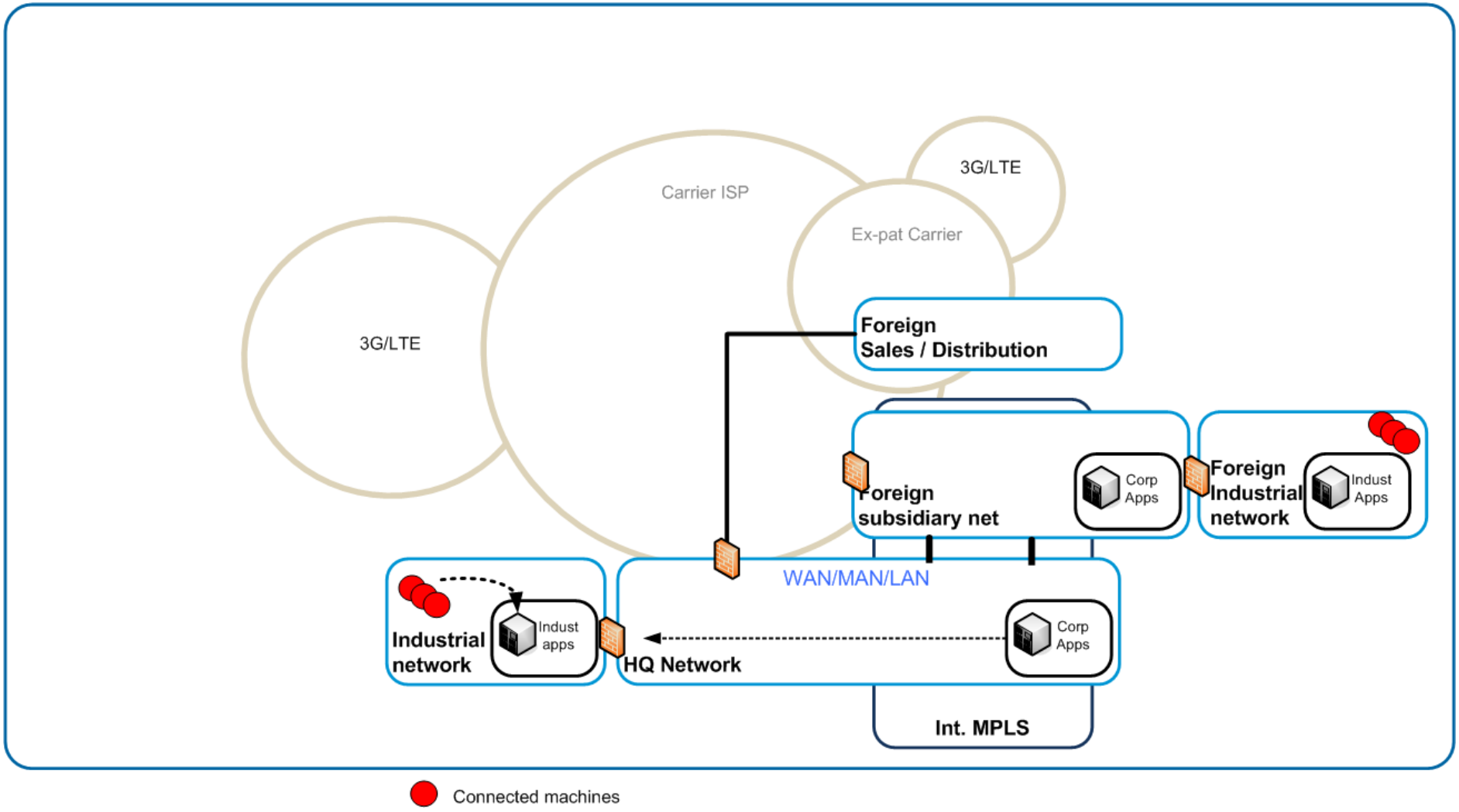
- 40% projected growth in global data generated year over year vs. 5% growth in global IT spending [1]
- By 2020
  - 40% of data will be generated by IoT [2]
  - Connected Devices (IoT) will represent 24 Billion [3]

1. McKinsey, Big Data:The next frontier for innovation, competition and productivity (June 2011)
2. IDC/EMC, Digital Universe (2011)
3. GSMA conducted by Machina Research

Change in Types of Data



Connected Devices In The Past



Why IoT?

Ability to put Sensors in Everything

- Improved Power Management
- Ipv6

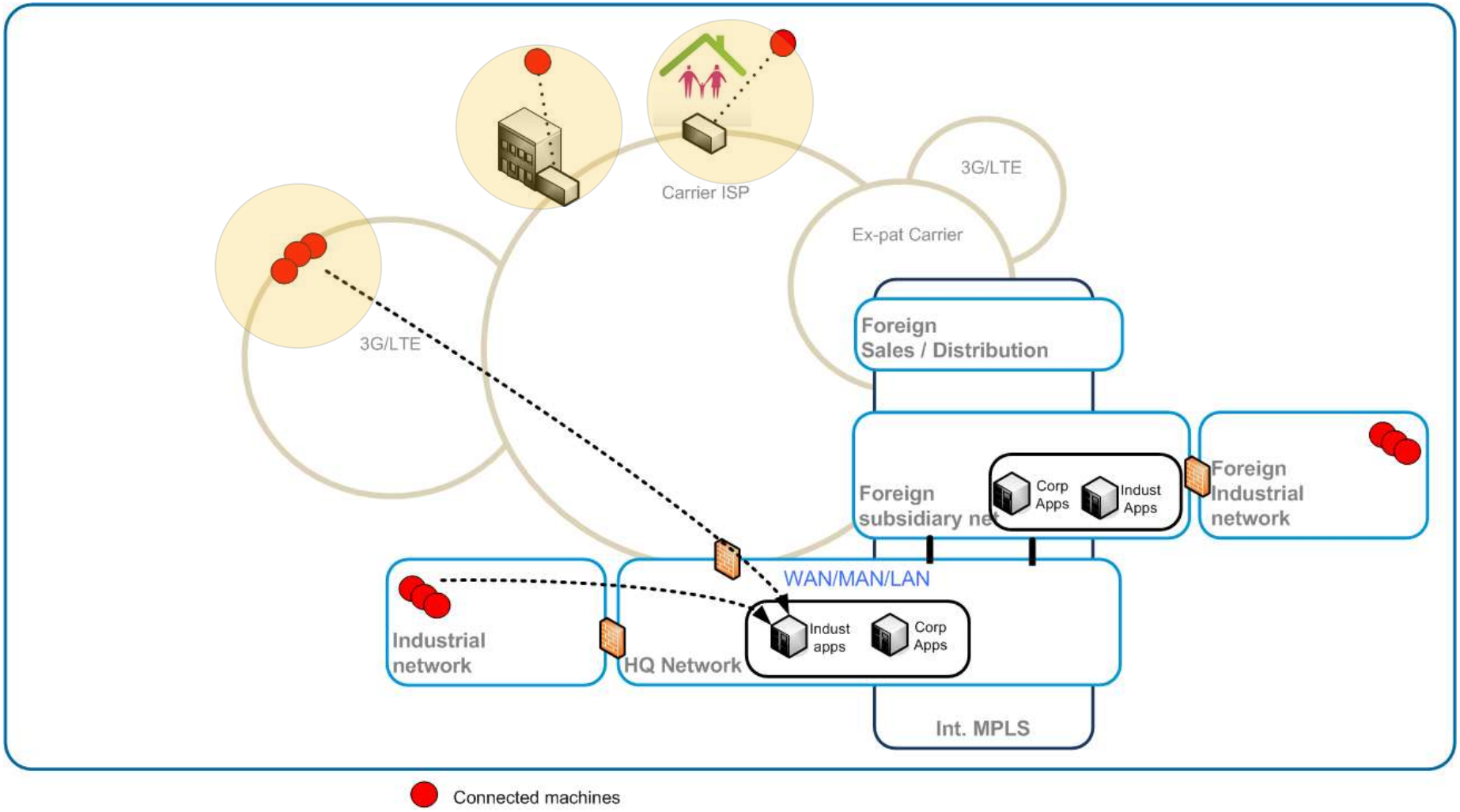
Ambient Networking (Everywhere)

- Open Standards
- Increased bandwidth and coverage

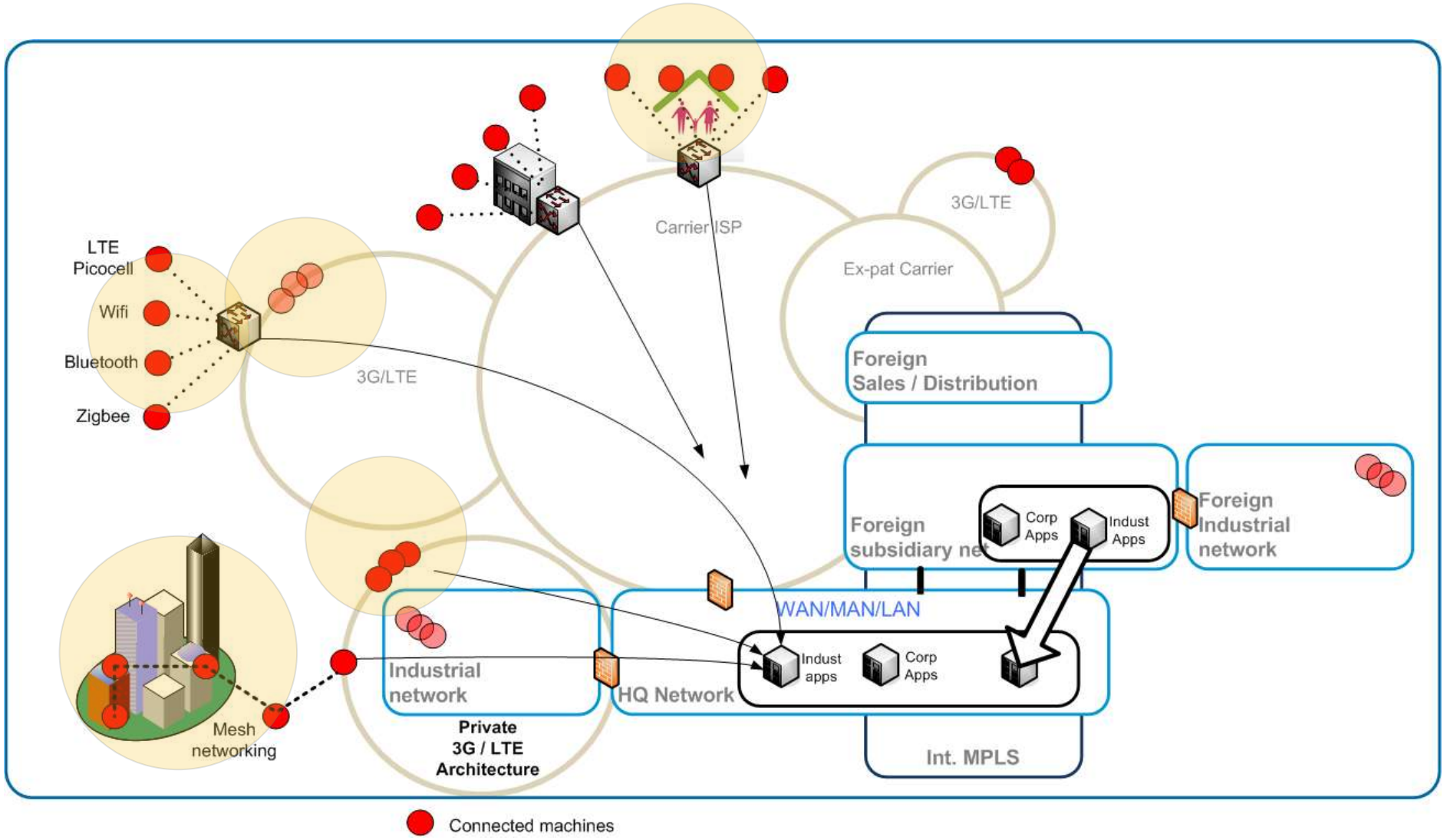
Analyze Everything

- Processor Speed
- Big Data

Current Connected Devices

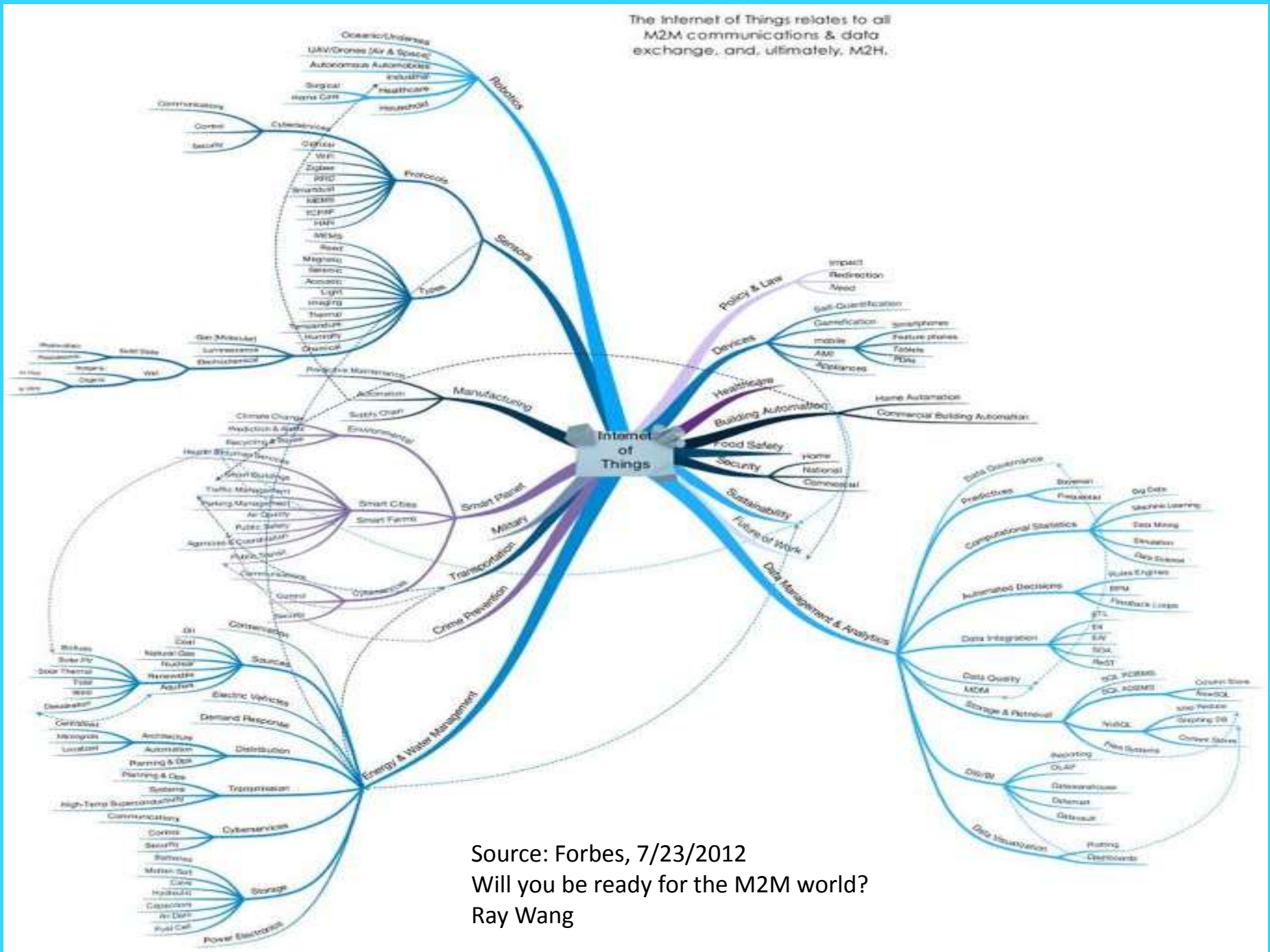


Future of IoT



IoT Applications

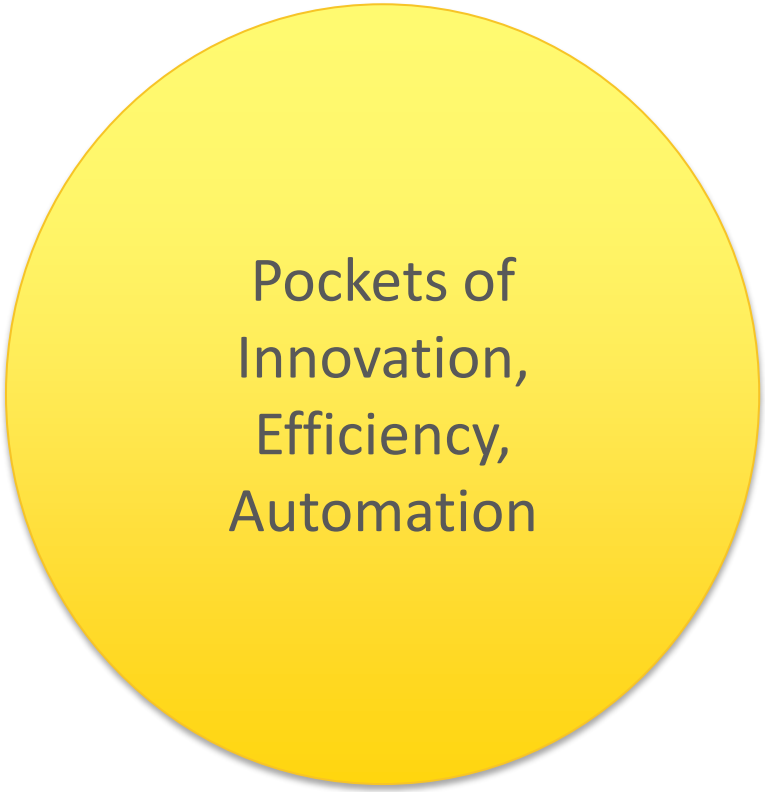
Information and Analysis	Tracking Behavior/Usage Enhanced Situational Awareness Sensor Driven Decision Analytics
Automation And Control	Process Optimization Optimized Resource Consumption Complex Autonomous Systems



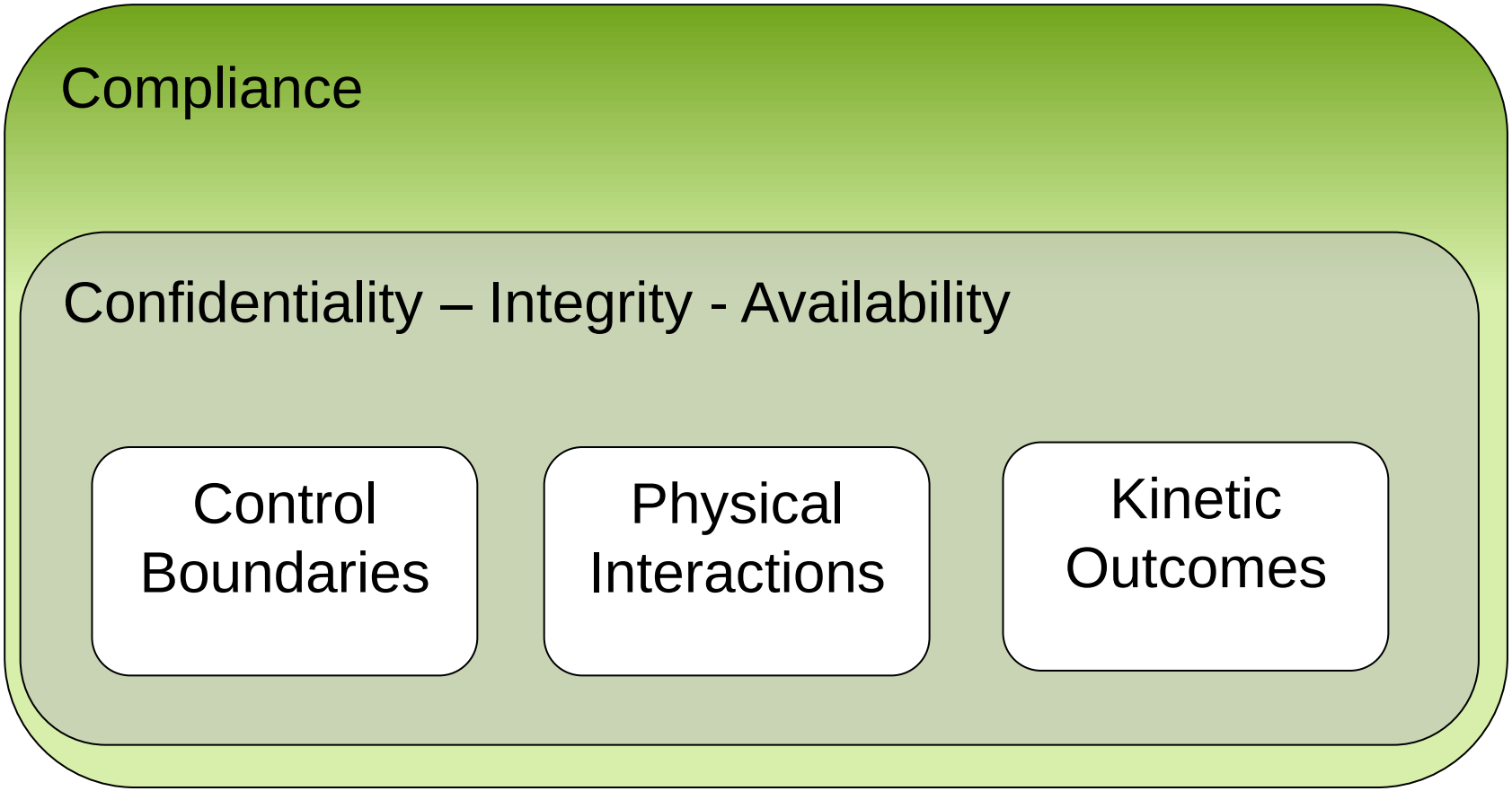
Source: Forbes, 7/23/2012
Will you be ready for the M2M world?
Ray Wang

Industries

- Energy & Water Mgmt.
- Smart City/Smart Planet
- Robotics/Industrial Control
- Bldg. Mgmt./Automation
- Transportation
- Healthcare
- Military
- Retail
- Consumer Tech.



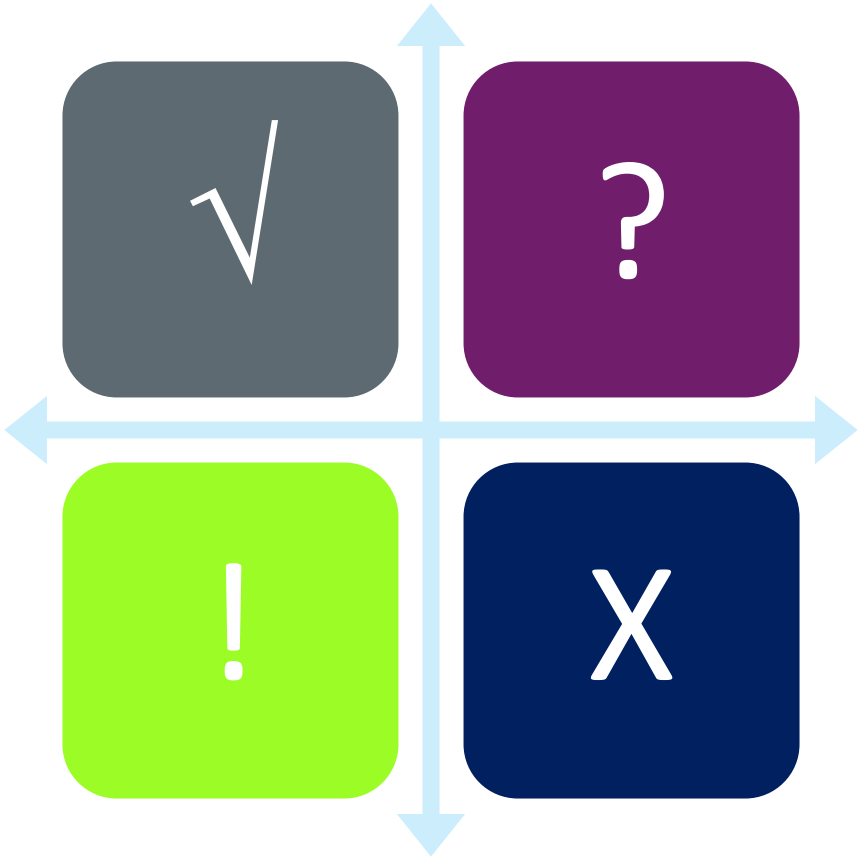
Intent of Use = Risk



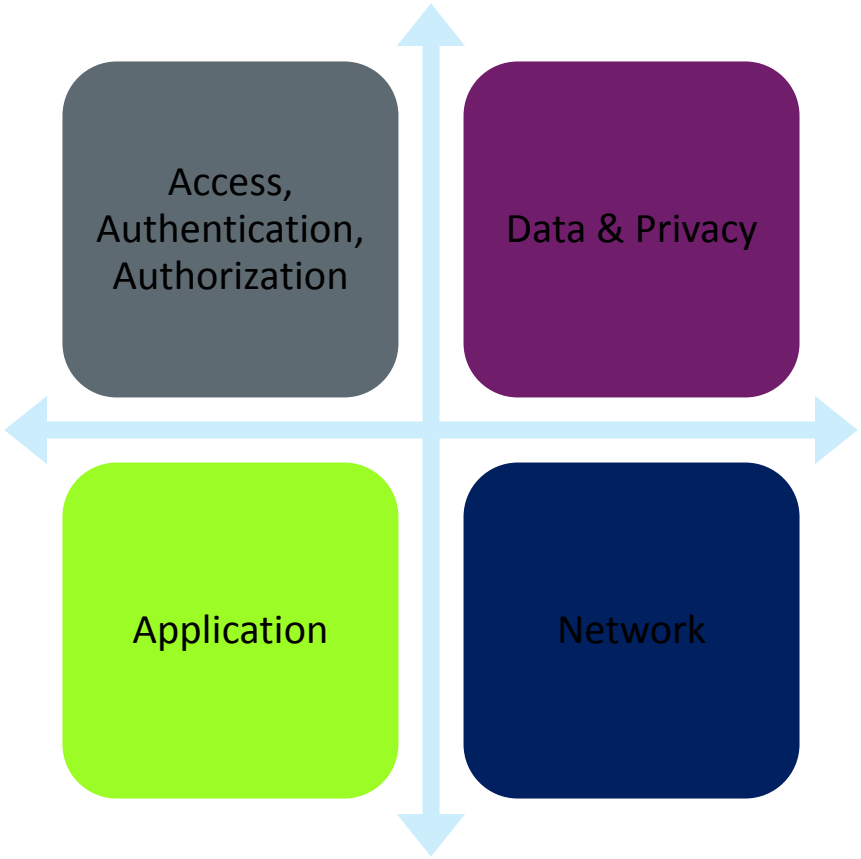
Engine or Service?

Power by the Hour

The Thing Lifestyle



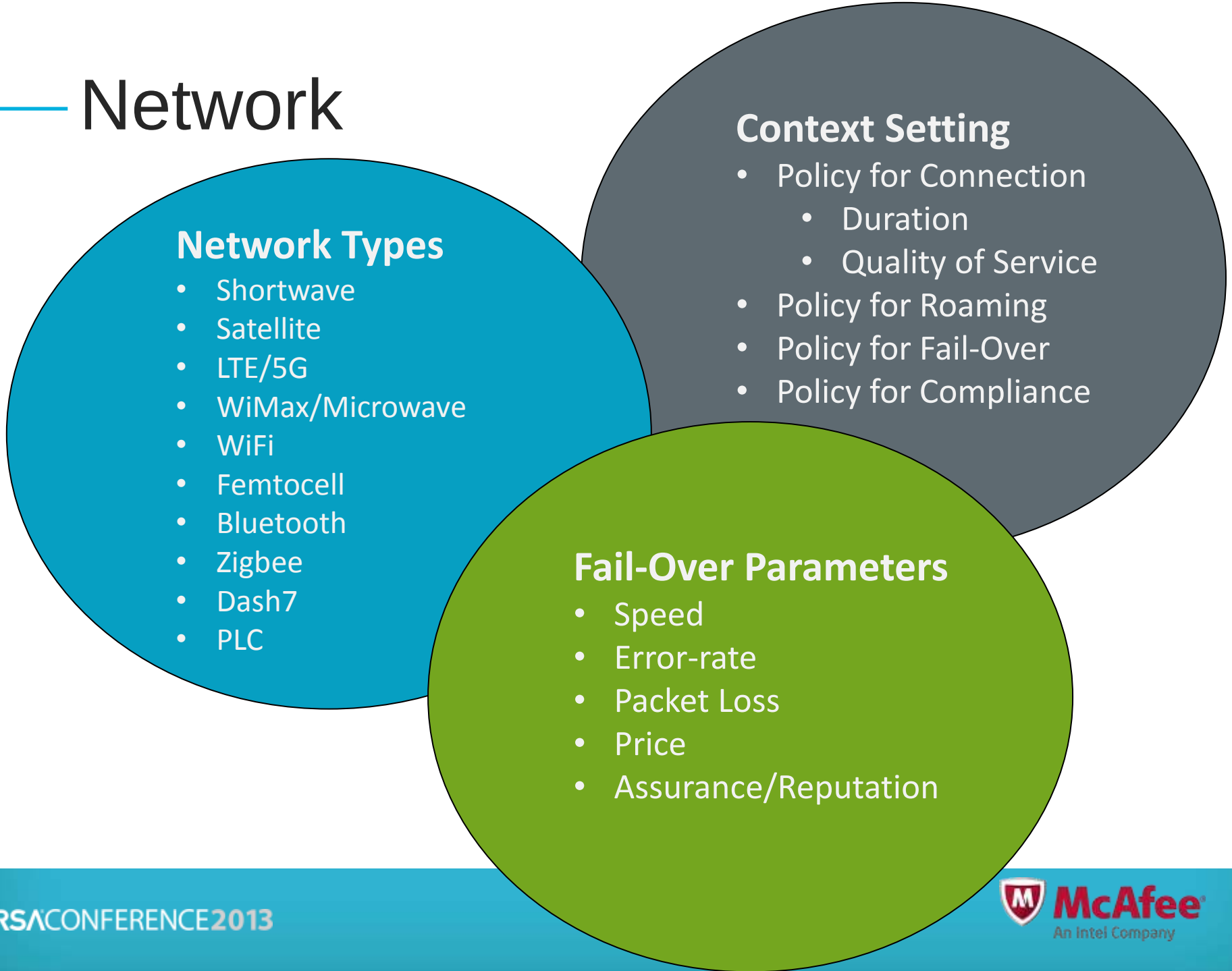
The Security Architecture



Security Issues for Pervasive IoT

- End-to-end security is not yet addressed in all the IoT related standards
- Attacks at physical layer
- Machine level integrity checks
- Identity linking
- Anonymity
- Secure deployment of credentials for lots of objects
- User interface to control/manage security

Network



Emerging Network for IoT

- IPv6
  - Management Tools Available?
  - Support in organization for dual networks?
  - Ready to leave comfort of NAT?
  - Is someone squatting in your dark space?
- Open Flow to Software Defined Networks
  - Take control out of hands of infrastructure
  - ACL's and routing protocols will not provide enough agility security

Emerging Network for IoT

- TRILL
  - Possible Spanning Tree Alternative
  - Get more efficiency of available bandwidth and meshed network
  - Opportunity to Load Balance

- DNS Sec/DANE
  - Prevent DNS cache poisoning
  - Obtain Authentication of Named Entities with SSL info on certs

IoT Endpoint Control

- Boot or Power On Authentication
  - Stop unauthorized devices from entering the network
- Proactive Intelligence in the Flow
  - IETF REPUTON and IETF 6MAN/Packet Staining WG
  - Include suspicious behavior indicator in flow
- Adaptive Information Infrastructure
  - Holonic Systems; Dual in Nature
    - Wholes in themselves
    - Simultaneously integral or larger wholes
  - Competitive Learning
    - Nodes compete for right to respond
    - Increasing specialization of each node of the cluster

Cloud – Data Center - App

- Hardware Identification and Access Control
  - Specify computing platforms - Intel TXT
- Cloud Security Standards and Metrics
  - Zones/Compliance/Service Level for IoT
- Big Data/Analytics/Management
  - Access Authority
  - Retention Policy
  - De-Identification of Context Specific Data

Today's Security Options

- Integrity Control (Endpoints and Embedded Systems)
- Hardware Assisted Rootkit Defense
- Global Threat Intelligence integrated at endpoint and network
- Network IPS and Softswitch IPS
- Asset Detection and Real-time Mgmt.
- Big Security Data Management

Summary

- IoT will be everywhere
- IoT will need orchestrators who can design and balance risk and reward models
- IoT is challenging and will be complex and intriguing

@ksingletary