

# Panel on Safety and Resilience

## Safety and Resilience with 5G and IoT Advent

Moderator: Mark Austin,

*University of Maryland, College Park, MD*

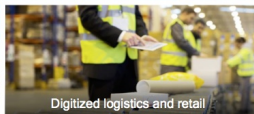
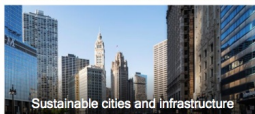
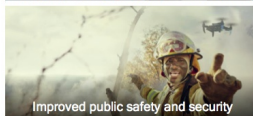
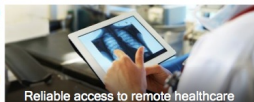
*Third International Conference on Advances and Trends in Software Engineering  
(SOFTENG 2017), Venice, Italy*

May 3, 2017

# Introduction

# Expected Impact of 5G on Society

Platform for connected services:



# Design Challenges

## Scalability to address diverse services

- Ultra-low energy – 10+ years of batter life ...
- Ultra-high reliability – 1 out of 100 million packets lost ...
- Ultra-high density – 1 million nodes per  $Km^2$  ...
- Ultra-low latency (delay) – as low as 1 millisecond ...
- Strong security – trusted data in sensitive industries (e.g., healthcare) ...
- Extreme user mobility – self-driving cars ....
- Extreme data rates – 100+ Mbps user experience ...
- Extreme capacity – 10 Tbps per  $Km^2$  ...
- Deep coverage – to reach challenging locations ...
- Deep awareness – discovery and learning (machine learning?)

....

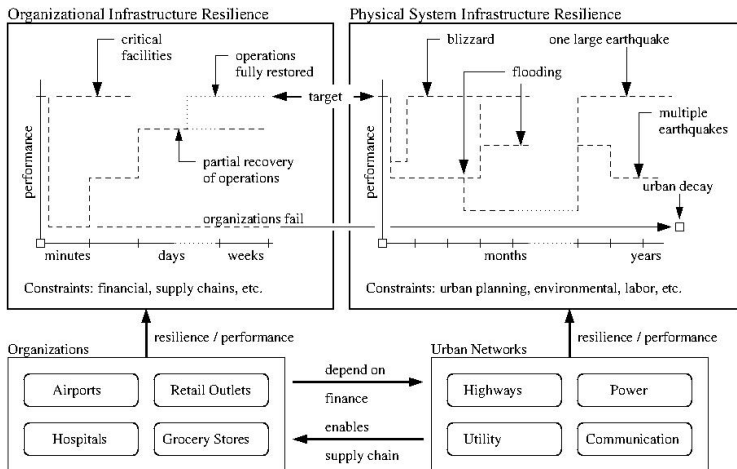
# Safety Concerns

- Will use of these technologies trigger medical problems in humans?
- How to assure cyber security?
- Who and how will entities attack these systems?
- How to design safety-critical systems?

# Resilience of Large-Scale Urban Systems

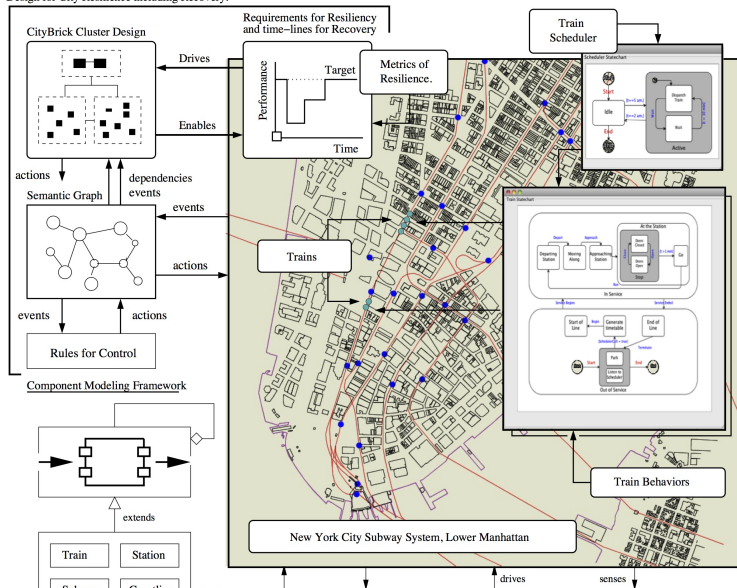
# Design Challenges

Large-scale urban systems are **highly interconnected** and **heterogeneous**. **Relief actions** occur across **multiple time scales** ...



# Planning for Relief Actions in New York City

Design for City Resiliency including Recovery.





## Moderator

- Mark Austin, University of Maryland, College Park, USA

## Panelists

- Mohammad Rajabali Nejad, University of Twente, Enschede, the Netherlands
- Seppo Yrjäl, Nokia, Finland
- Andy Snow, Ohio University, USA

# Summary of Key Points from the Panel Session

## Safety and Security

- Good news – RF is non-ionizing radiation. Bad news – linkage to cancers is suspected, but so far, not shown to be causal.
- Safety factors – frequency and power. 5G will use millimeter waves. 40% of power is reflected by the human skin.
- From a security standpoint, IoT is already targeted.

## Resilience

- Goal is to minimize the extent and duration of disruptions.
- Notions of resilience cover multiple levels of system abstraction and can include loss of situational awareness and actuation. Both factors lead to safety concerns.

# Safety and Resiliency 5G and IOT

NEXCOM 2017

International Academy, Research and Industry Association

April 24, 2017

Andy Snow  
Ohio University

# Safety and Resiliency

- 5G -- RF Safety
- IOT -- Resiliency & Safety

# 5G RF Safety

- The Good News -- RF is non-ionizing radiation
- The Bad News – linkage to some cancers is suspected, but not shown to be causal so far
- However, according to the US National Cancer Institute:
  - "Radiofrequency energy, unlike ionizing radiation, does not cause DNA damage that can lead to cancer."
  - "Its only consistently observed biological effect in humans is tissue heating."
  - "In animal studies, it has not been found to cause cancer or to enhance the cancer-causing effects of known chemical carcinogens."
- Safety factors
  - Frequency
  - Power

# Frequency

- 5G will use “millimeter waves”
- Electromagnetic band between microwave and infrared
- IEEE 802.11ad at 60 GHz
- US FCC approved licensing in the 28, 37, 39 GHz bands for 5G in 2016

**Millimeter  
Waves**

Frequency (GHz)	Wavelength (mm)
1	300.0
2	150.0
5	60.0
10	30.0
15	20.0
20	15.0
<b>25</b>	<b>12.0</b>
30	10.0
300	1.0

**3G, 4G**

**5G**

# 3G RF and Humans

- Dutch experimentation in 2003 researched low dose 3G radiation to mimic base station
- Double blind experiment
  - Experimental group (exposed to 3G radiation from base station)
  - Control group (no radiation)
  - Evaluators measured physiological data and administered cognitive tests
  - Both subjects and evaluators did not know if individual exposed to radiation
- Results? Those exposed:
  - Had elevated temperature of brain
  - Reported tingling
  - Complained of headaches and nausea
  - Performed better on cognition tests

# 5G RF and Humans

- A 2015 study<sup>1</sup> looked at millimeter wave affects on humans
  - At 60 GHz, 34 to 44 % of power is reflected from human skin
  - More thermal experiments with MRI thermal imaging are needed as millimeter waves heat up skin and eyes
- Another study<sup>2</sup> in 2016 looked at power levels
  - Evaluated array antennas intended for user equipment and low-power radio base stations in 5G in the 10-60 GHz
  - For antennas transmitting at the human body, power significantly below 3G and 4G mobile communication systems.

<sup>1</sup>T. Wu, T. S. Rappaport, C. M. Collins, "The Human Body and Millimeter Wave Wireless Communication Systems: Interactions and Implications," 2015 IEEE International Conference on Communications (ICC), Jun. 2015.

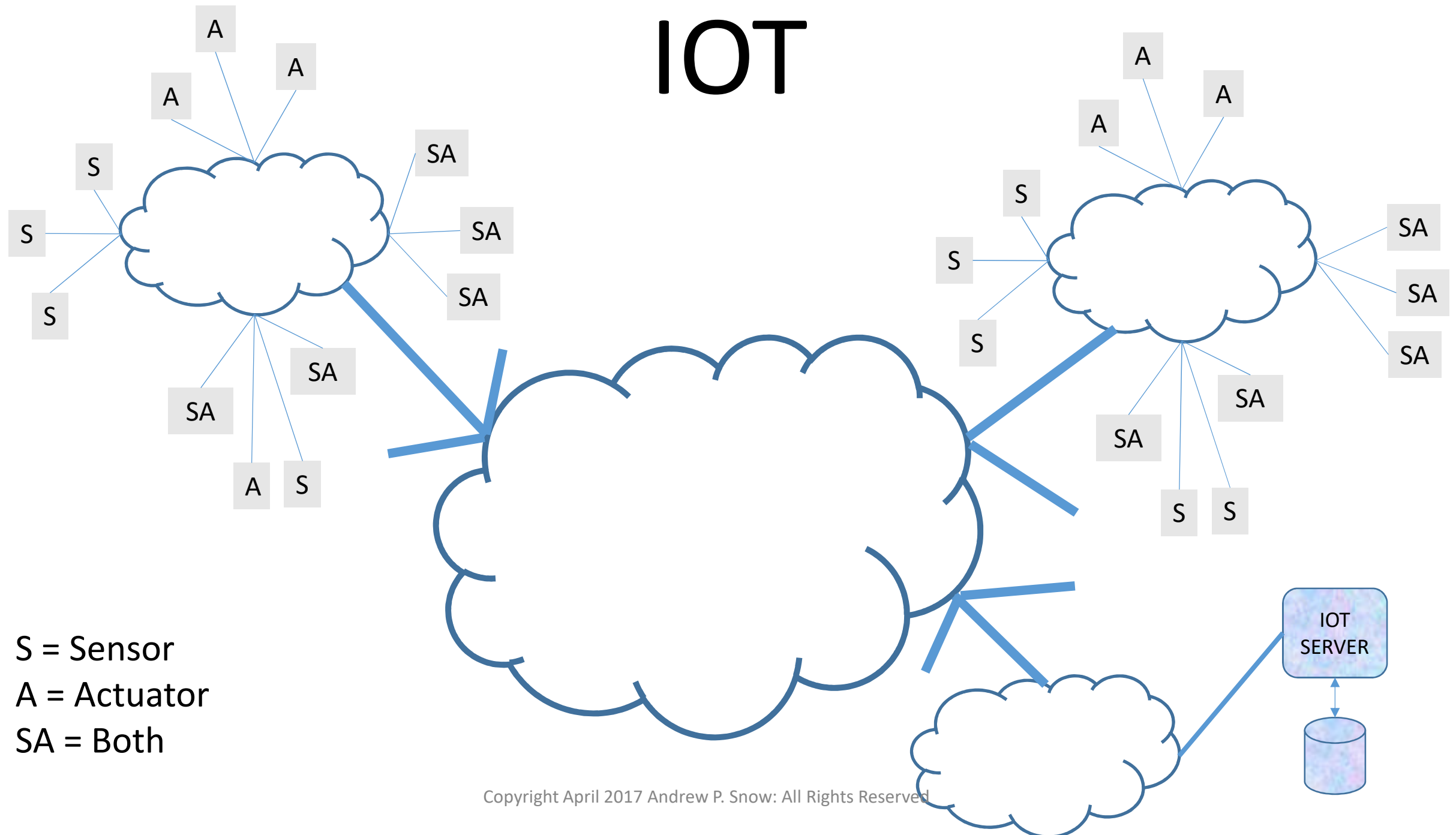
<sup>2</sup>Thors, Björn, et al. "Exposure to RF EMF From Array Antennas in 5G Mobile Communication Equipment." *IEEE Access* 4 (2016): 7469-7478.



# IOT Resiliency and Safety

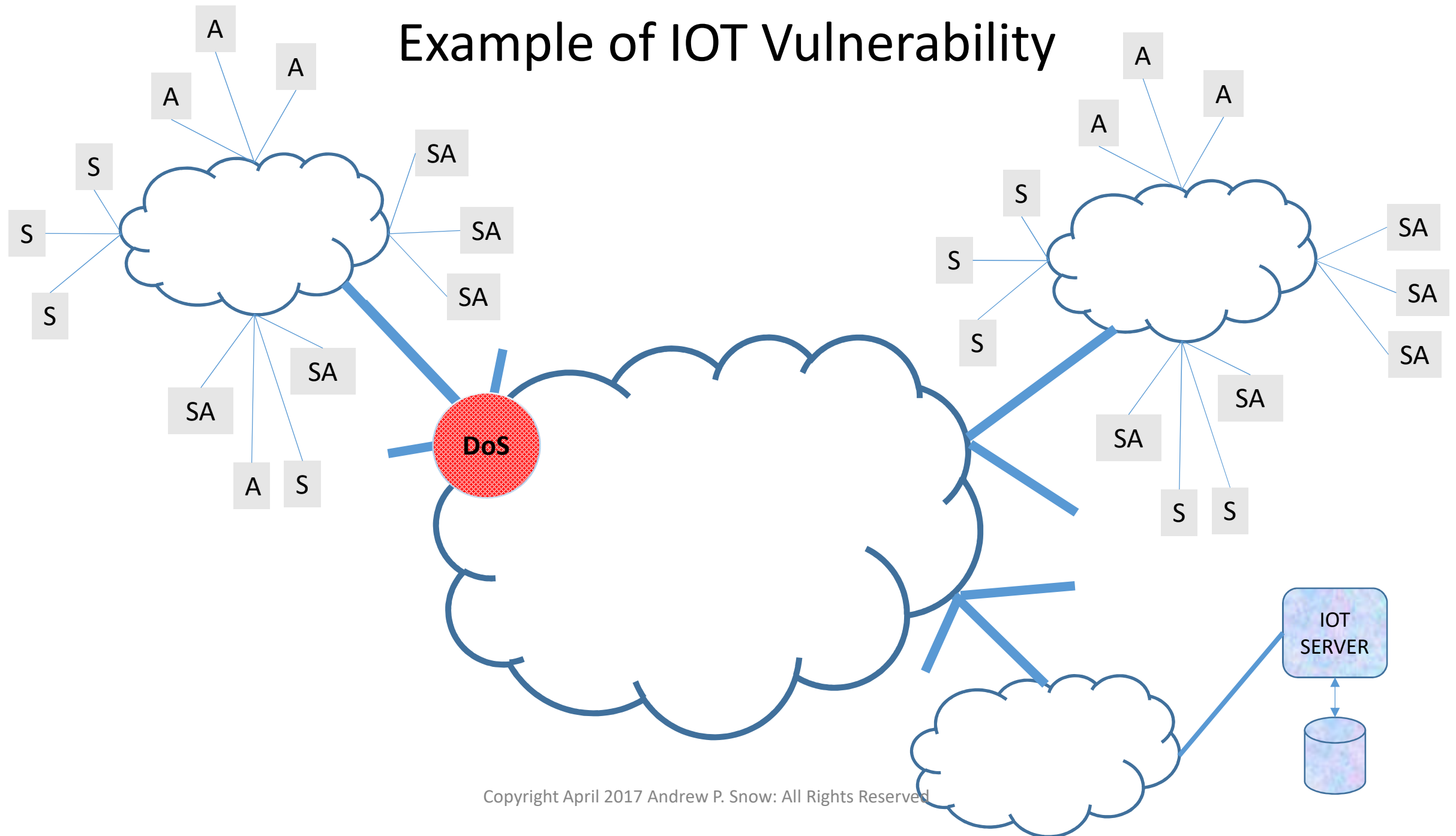
- Networked sensors and actuators
  - Sensor access problems – loss of awareness
  - Actuator access problems – loss of control
  - Both have safety implications, but which is worse?
- Depends on the application:
  - Safety versus convenience
  - Consumer versus industrial
- Resiliency
  - Ability to minimize the size and duration of disruptions

# IOT

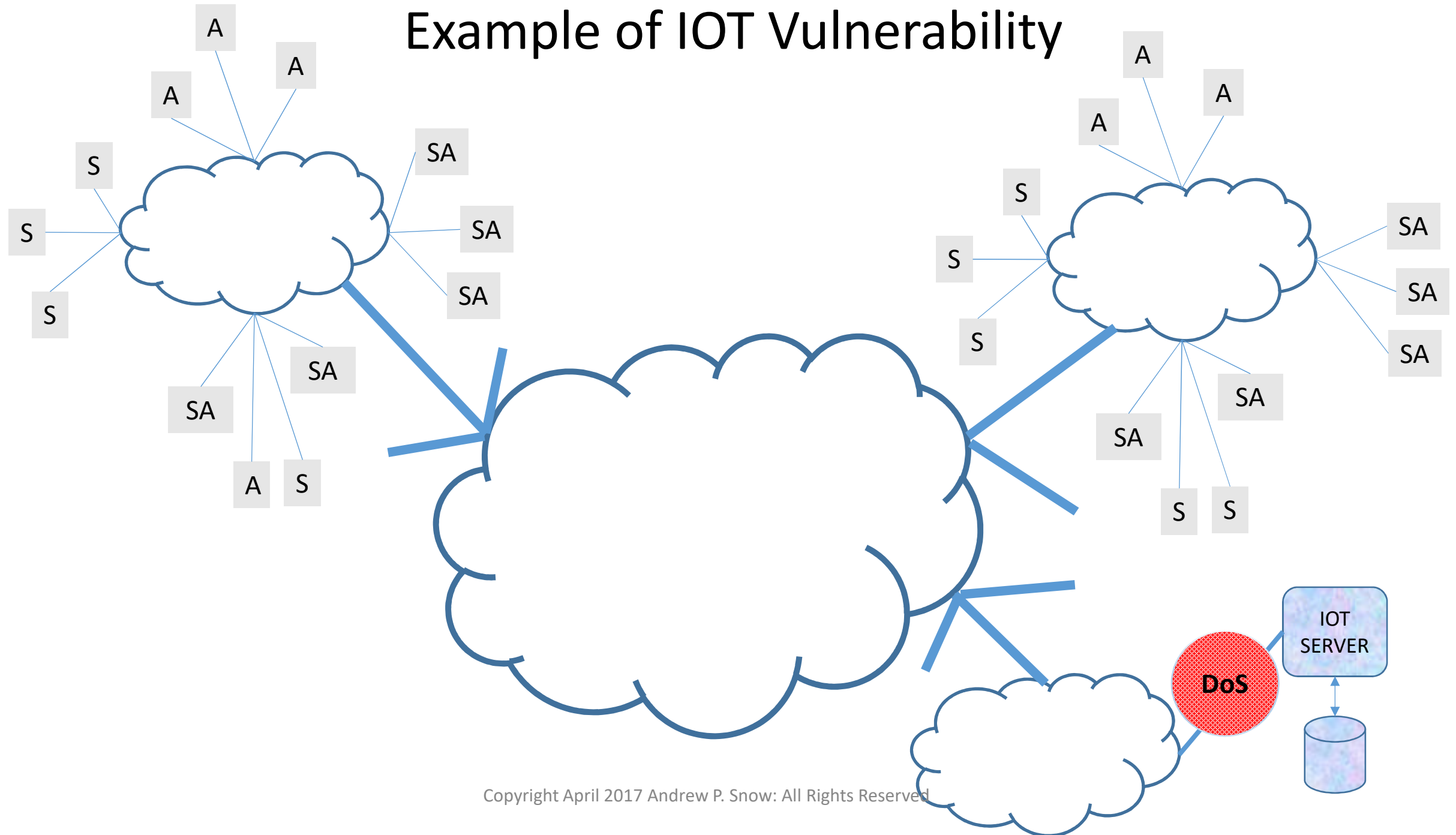


S = Sensor  
A = Actuator  
SA = Both

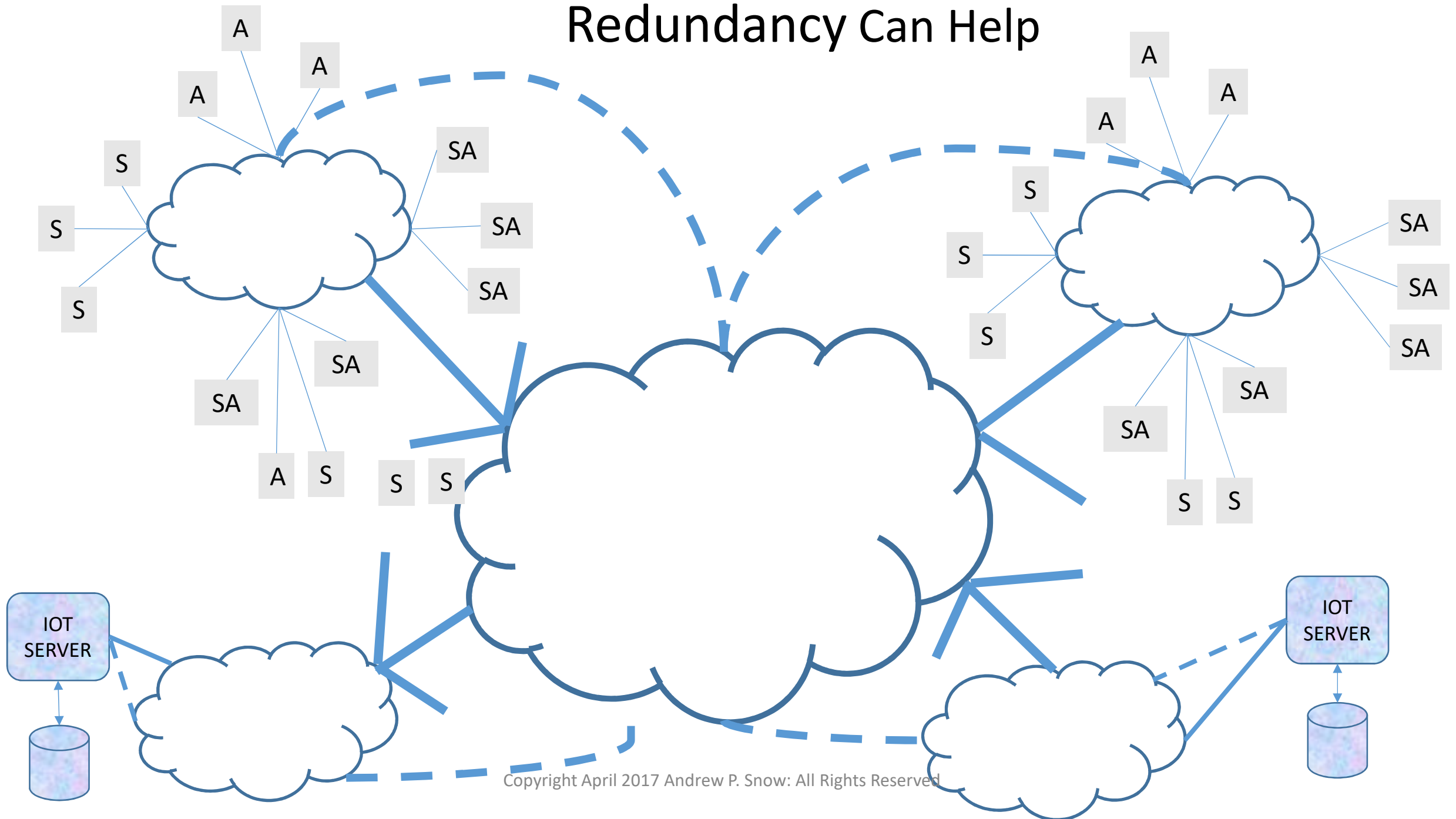
# Example of IOT Vulnerability



# Example of IOT Vulnerability



# Redundancy Can Help



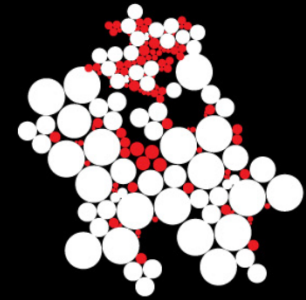
# Some Conclusions as of Today

- 5G RF Safety
  - 5G RF appears safer than 3G and 4G
  - Some fears of skin cancer risk from mm wave energy of airport security scanning
  - No evidence that low RF energy at mobile communication power causes cancers
  - Not known how deleterious thermal effects will be
  - With regard to cancers and thermal effects -- TIME will tell as there are over 3.5 Billion lab rats out there!
- IOT Resiliency and Safety
  - DoS and Hacking issues
  - High dependence on IoT will mean increased risks
  - Much research required

# What's Next?

- 5G RF -- Safety
  - Wireless service providers, equipment manufacturers and governments must fund more research.
  - Ostrich head-in-the-sand is a strategy, albeit a poor one!!
- IoT Resiliency
  - Policy makers must start the dialogue about possible restrictions on IoT services, as it relates to large-scale IoT sensor and actuator outages
  - Technologists should intensify research in the area of Re-routing Protocols at the micro network levels.

UNIVERSITY OF TWENTE.

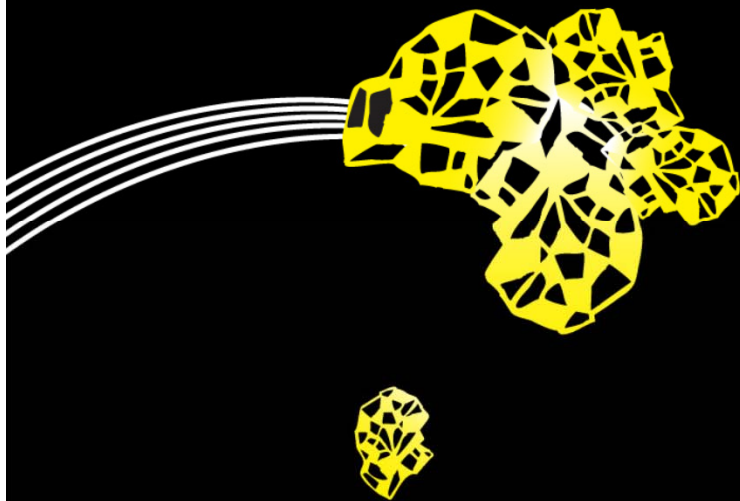


*SAFETY AND RESILIENCE WITH 5G AND IOT  
ADVENTS*

DR MOHAMMAD RAJABALI NEJAD

PESARO 2017

VENICE, ITALY





# ABOUT THE PANELIST

---

- Assistant Professor: University of Twente, System Safety
- Associate Editor: J. of Intelligent Automation and Software Engineering
- Advisory Board: J. of Advances in Systems and Measurements
  
- Postdoc, University of Montreal, Canada, “Reliability of Infrastructures”
- PhD, TUDelft, “Reliability Methods for Finite Elements Models”
- MSC, IUST, Tehran, “Safety of Civil Structures”
  
- Worked in various projects



**ASML ProRail**

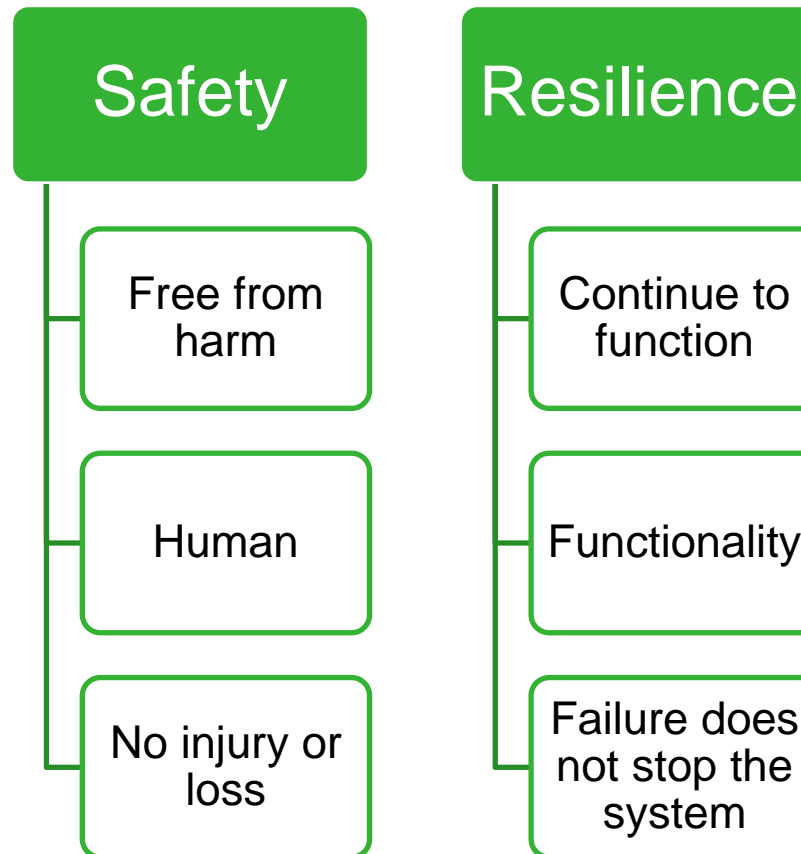


A CANON COMPANY



# SAFETY & RESILIENCE

---



# COMMUNICATION TECHNOLOGY - 5G/ IOT

## FOR PRODUCTS, MACHINES, AND SYSTEMS

---

- Products
  - Smart phones, TVs, watches
- Machines
  - Smart cars, trains, drones
- Systems
  - Smart grid, smart healthcare



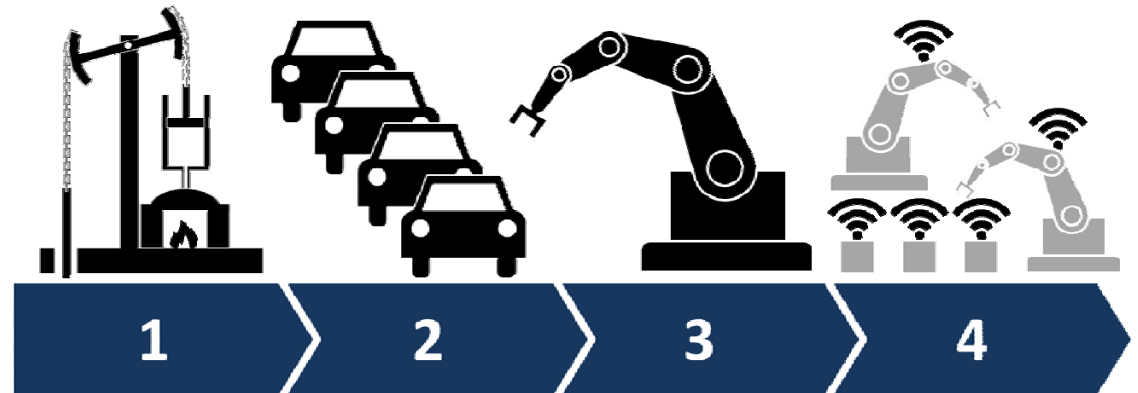
Micro-drone swarm

# IOT ENABLES INDUSTRIAL REVOLUTION

## AN EXAMPLE ADVANTEGE

---

- Capabilities such as
  - remote access
  - big data
  - artificial intelligence
- For achieving
  - low cost
  - high performances



<https://www.youtube.com/watch?v=dkddSaOOZcs>

# THE GAME IS CHANGING

## SO DOES IT RULES

---

- #1 SAFTY RULE
  - Safe guarding
    - beasts in the zoo
    - machines in work-floors
  - New rule for
    - robots, cobots, exo-skeleton
    - servant (indoor) drones

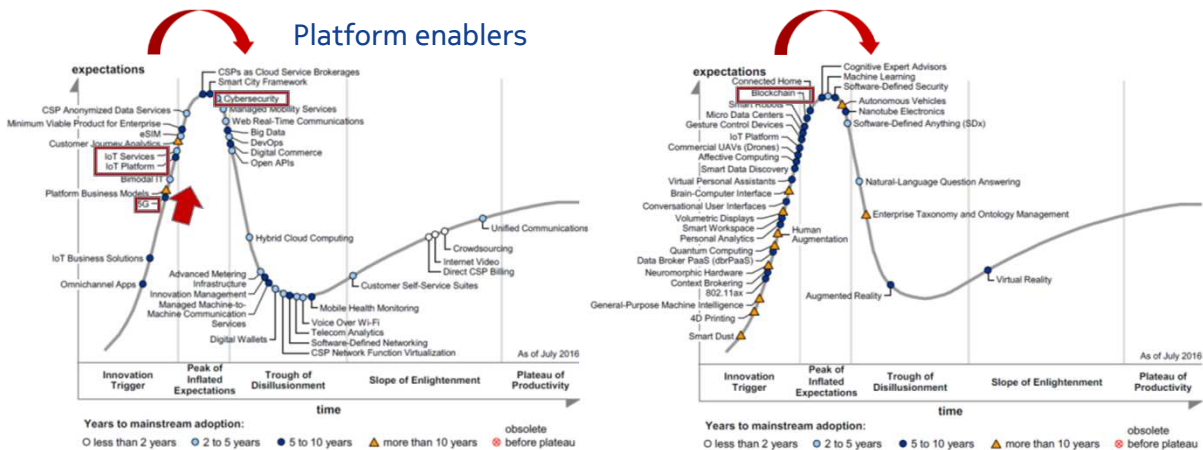


Man-machine battle: see <https://www.youtube.com/watch?v=JYuOFhFrEMw>

# The Future X Network: Building the digital fabric for the automation of everything and the creation of time

COCORA 2017: Safety and Resilience with 5G and IoT Advents  
 Wednesday, April 26th, 2017  
 Dr. Seppo Yrjölä  
 Nokia Corporate Strategy & Development

5G meets security and IoT in the hype cycle  
 Shift from technical infrastructure to ecosystem-enabling platforms



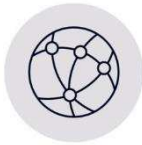
Hype Cycle for the Telecommunications Industry and Hype Cycle for Emerging Technologies, Gartner July 2016

## Six global megatrends driving massive new technology requirements – and opportunities



Network, compute & storage

Broadband everywhere, distributed cloud, near infinite storage



Internet of Things

Connectivity for a trillion things



Augmented intelligence

Human assistance and task automation at machine scale



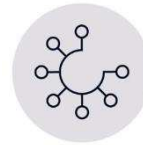
Human & machine interaction

Virtual and augmented reality, reshaping how we interact with machines



Social & trust economics

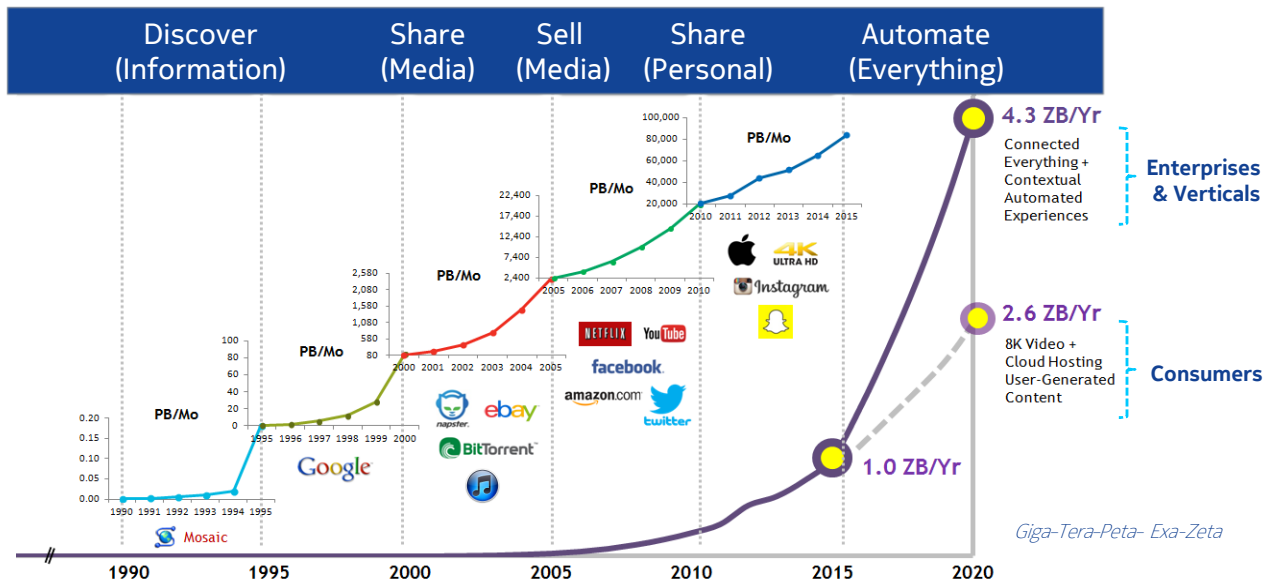
Sharing economy and digital currencies making trust and security essential



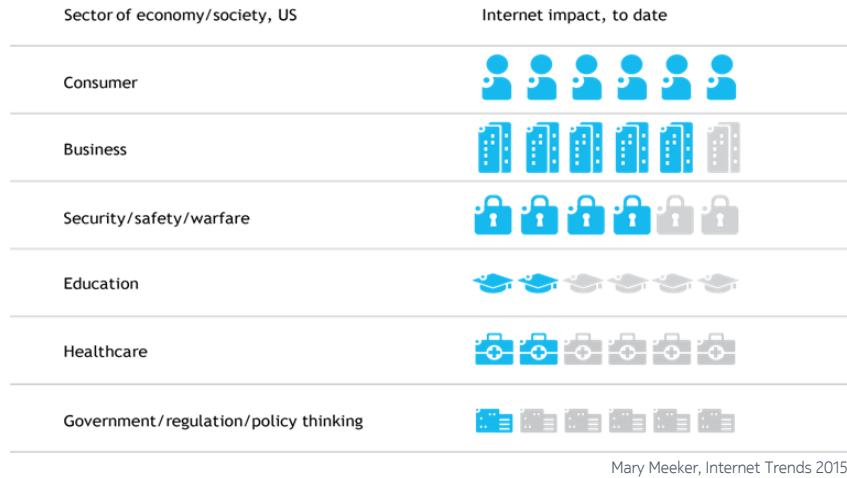
Digitalization & ecosystems

Digitalization of operations expanding into consumer and biology

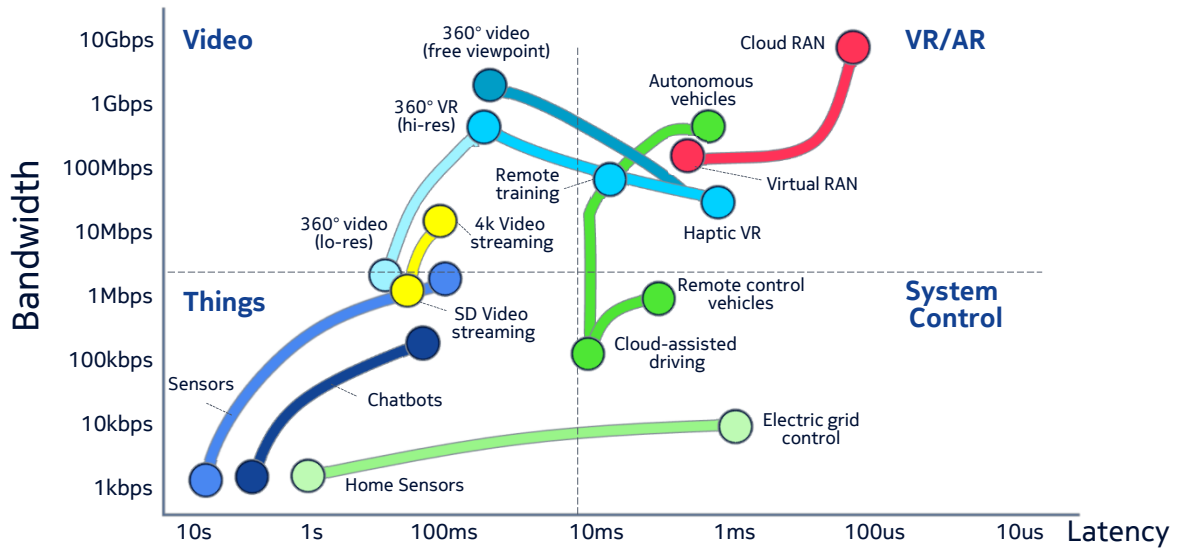
## New networking & connectivity era



### Future network driven by an enterprise/industrial revolution



### The Future X network - 4 key business value dimensions

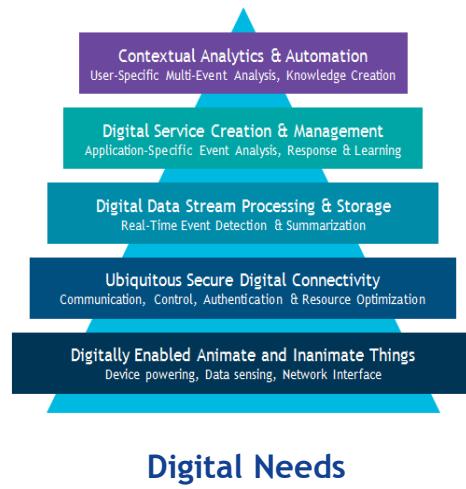




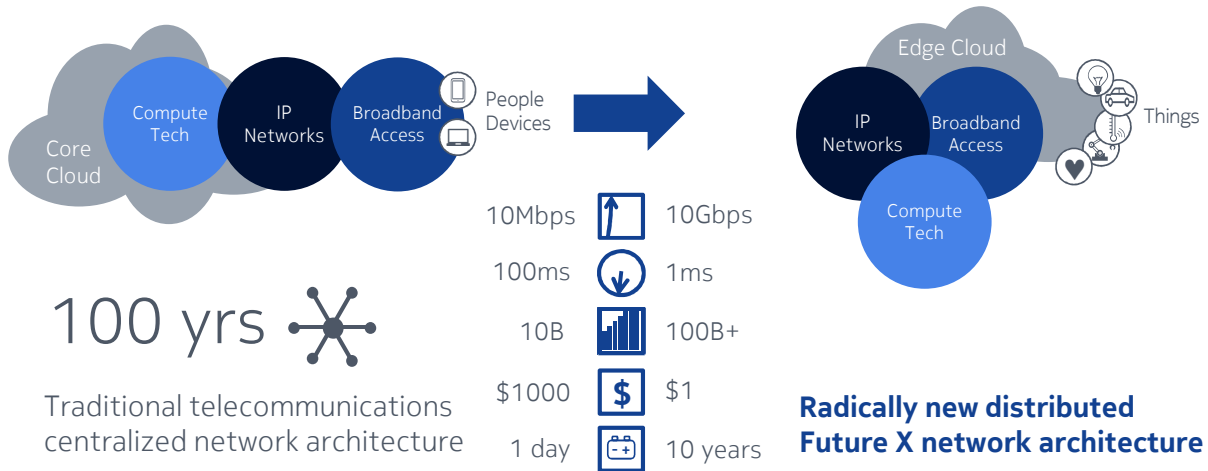
The new value in time & trust



**Create Time ...with Trust**  
 (by Prediction & Automation) (in Privacy & Security)



The 100x shift: a new digital infrastructure for the automation of everything



Cost + Performance + Agility → Confluence of Networks & Cloud

## Threat landscape: The potential attack space is growing

### Fixed and mobile malware grows

- Fixed remains strong at 11%<sup>6</sup>, mobile doubled<sup>1</sup>
- Android attacks increased 4-fold<sup>2</sup>, iOS starting to be attacked
- More sophisticated and dangerous than ever<sup>6</sup>

### IoT is already targeted

- 70% of devices do not use encryption<sup>3</sup>
- 90% of devices collected at least one piece of personal information<sup>3</sup>
- Several examples of attacks already

### Cybercrime is a big business

- Professional, organized and funded
- Same level as illegal drug trade (~1% GDP)<sup>4</sup>
- 53% of organizations don't feel protected against attacks<sup>5</sup>

1) McAfee Labs Threats report 2015; 2) Kaspersky Security Bulletin 2014; 3) HP - Internet of Things Research Study - 2014 report; 4) Intel - McAfee: Net Losses: Estimating the Global Cost of Cybercrime; 5) Ponemon Institute - report-2014; 6) Nokia Threat Intelligence Labs report, H2 2015

## Transforming security paradigms & approaches

### Legacy Security Software

- Security Information Event Management
- Manual Operations & Mitigation
- Antivirus
- Authentication, Authorization & Accounting



### Next Generation Solutions

- Security Intelligence & Analytics
- Orchestrated Operations & Predictive Response
- Automated Malware Detection & Threat Intelligence
- Identity & Access Management – “The New Perimeter”



Security and privacy are  
fundamental elements to  
expand the human possibilities  
of a connected world

Thank you  
Questions/discussion?

[seppo.yrjola@nokia.com](mailto:seppo.yrjola@nokia.com)