# DELVING DEEP INTO THE INTERSECTION OF AI AND IOT

Susie Su
Global Software Operations Architect
@Signify (Philips Lighting)

# OPEN SOURCE


**Susie Su**

DevOps Manager

Global Software Operations Arch

@Signify (Philips Lighting)

14 years Software Development

10 years Cloud Compute (AWS & Ali Cloud)

8 years Team Manager & Project Management

5 years IoT & Kubernetes/Docker & Prometheus & Spring Boot

4 years ISP & 3 years Overseas

* 3 years AI, ML, Deep Learning and Blockchain

# 1

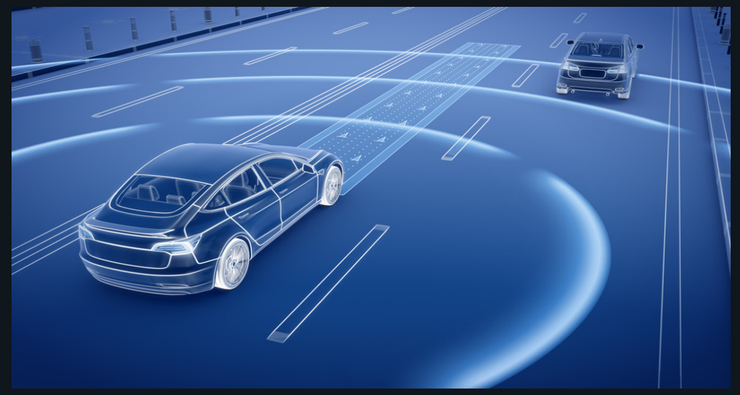
# AIOT (AI OF THINGS)

What does AIoT mean?

# AIOT = AI + IOT

## Automated Vehicles

Tesla, Waymo, Mobileye, Cruise and Baidu



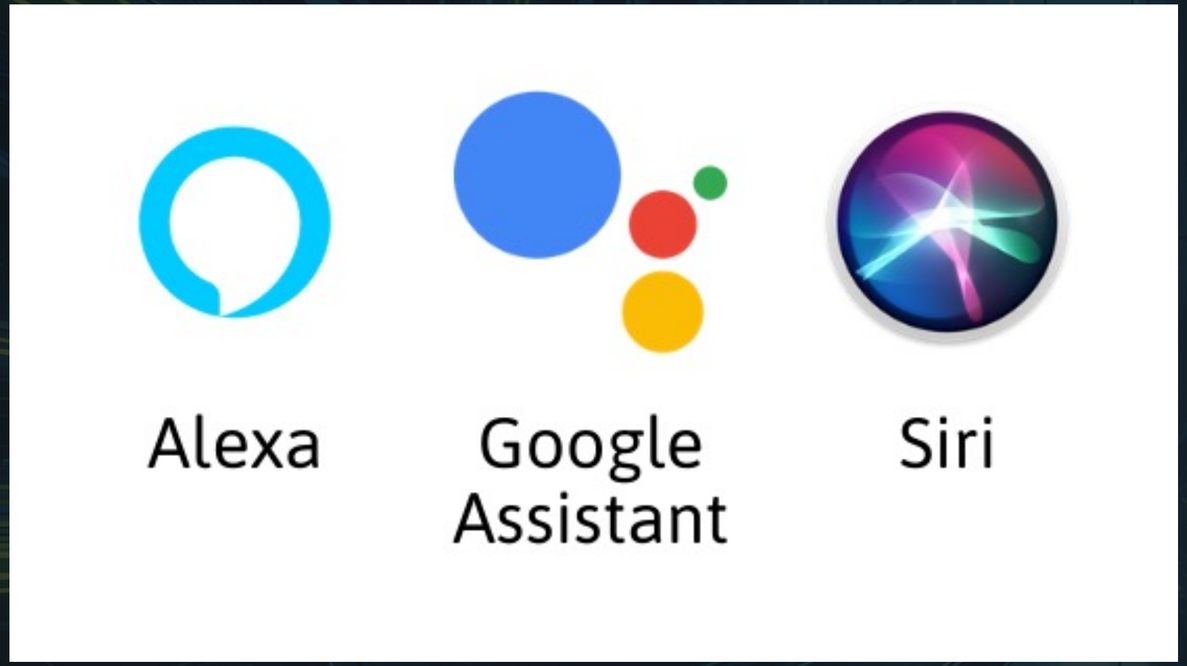
## Smart City

Lighting, Video Surveillance, Monitoring traffic and smart buildings

## Manufacturing

Deep Learning and deep neural networks.

# REAL-LIFE AIOT USE CASE



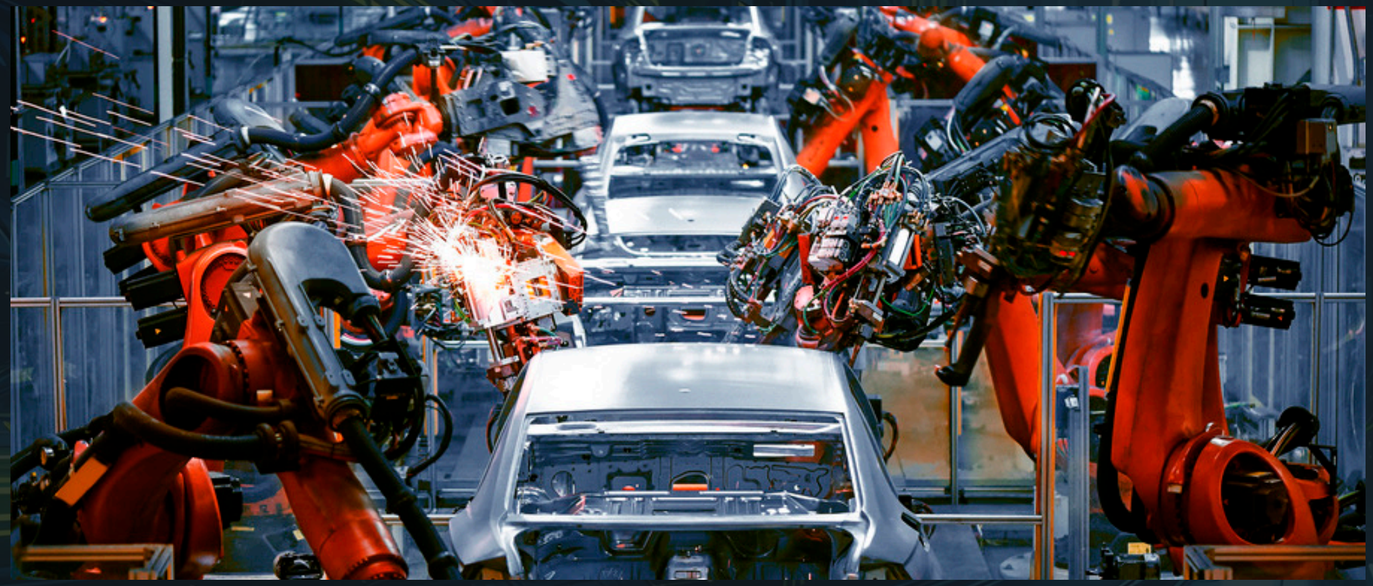

1. Natural Language Processing (NLP)

# REAL-LIFE AIOT USE CASE

IBM Watson™

2 Expert Systems

# REAL-LIFE AIOT USE CASE



3 Machine Vision

# REAL-LIFE AIOT USE CASE

Self-driving Car

4 Planning

# REAL-LIFE AIOT USE CASE

Boston Dynamics' Spot robot(

5 Robotics

# 2

# AIOT SECURITY

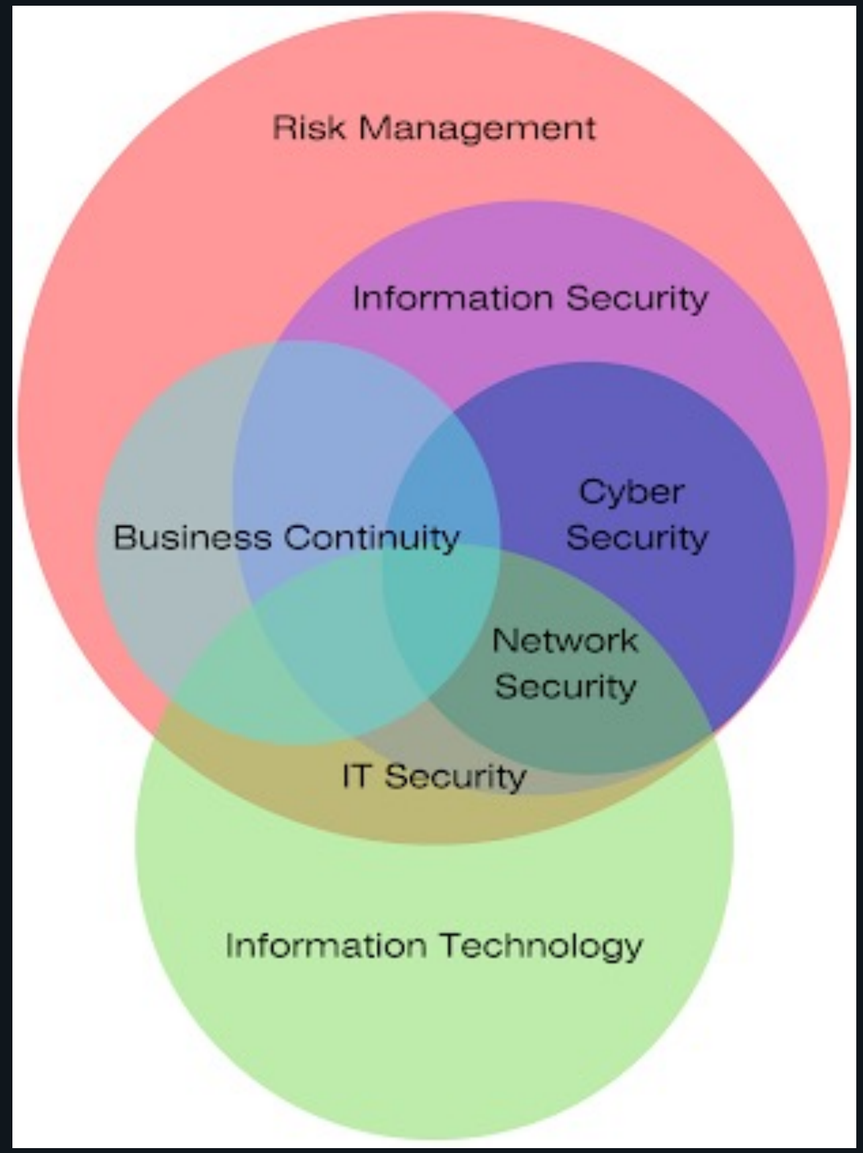
How can we enhance security
in AIoT?

# CYBERSECURITY

- Network Security
- Cloud Security
- Endpoint Security
- Application Security
- IoT Security

- 5G Networks
- IoV (Internet of Vehicles)
- IIoT (Industrial IoT)

...



# IOT SECURITY

AIoT Security

- 5G Networks
- IoV (Internet of Vehicles)
- IIoT
  - ICS (Industrial Control System)

*Table 1.* ICS cyber-incident timeline.

| Year | Type | Name | Description |
|---|---|---|---|
| 1903 | Attack | Marconi Wireless Hack | Marconi's wireless telegraph presentation hacked with Morse code. |
| 2000 | Attack | Maroochy Water | A cyber-attack caused the release of more than 265,000 gallons of untreated sewage. |
| 2008 | Attack | Turkey Pipeline Explosion (not quite cyber) | Did attackers use a security camera's vulnerable software to gain entrance into a pipeline's control network? |
| 2010 | Malware | Stuxnet | The world's first publically known digital weapon. |
| 2010 | Malware | Night Dragon | Attackers used sophisticated malware to target global oil, energy, and petrochemical companies. |
| 2011 | Malware | Duqu/ Flame/Gauss | Advanced and complex malware used to target specific organizations, including ICS manufacturers. |
| 2012 | Campaign | Gas Pipeline Cyber Intrusion Campaign | ICS-CERT identified an active series of cyber-intrusions targeting the natural gas pipeline sector. |
| 2012 | Malware | Shamoon | Malware used to target large energy companies in the Middle East, including Saudi Aramco and RasGas. |
| 2013 | Attack | Target Stores | Hackers initially gained access to Target's sensitive financial systems through a third-party that maintained its HVAC ICSs, costing Target $309M. |
| 2013 | Attack | New York Dam | The U.S. Justice Department claims Iran conducted a cyber-attack on the Bowman Dam in Rye Brook, NY. |
| 2013 | Malware | Havex | An ICS-focused malware campaign. |

# AI SECURITY

- Data Security
- Privacy Preservation
- Information Security
- Explainability and Transparency
- IoT Security
- Human-AI Interaction Security
- Model Security
- Bias and Fairness Security
- Lifecycle Security
- Regulatory Compliance
- Hybrid AI-human security

# SUMMARY

- AIoT Definition and Applications in Reality.
- InfoSec and IoT Security in AI and AI Security Definition

# THANK YOU !