# INNOVATION & RESEARCH IN INTELLIGENT TRANSPORT SYSTEM

Riaz Zolfonoon
Sr. Distinguished Engineer
RSA Office of the CTO`

November 15, 2018 - Beijing, China
IIC Global Event Series

RSA BUSINESS-DRIVEN SECURITY™

# ITS RESEARCH

- IIC
- Dell Technologies

industrial internet CONSORTIUM

Automotive Initiatives @IIC

Quantum Computing Readiness

Connected Car Ecosystem

Advanced Automotive Manufacturing

RSA

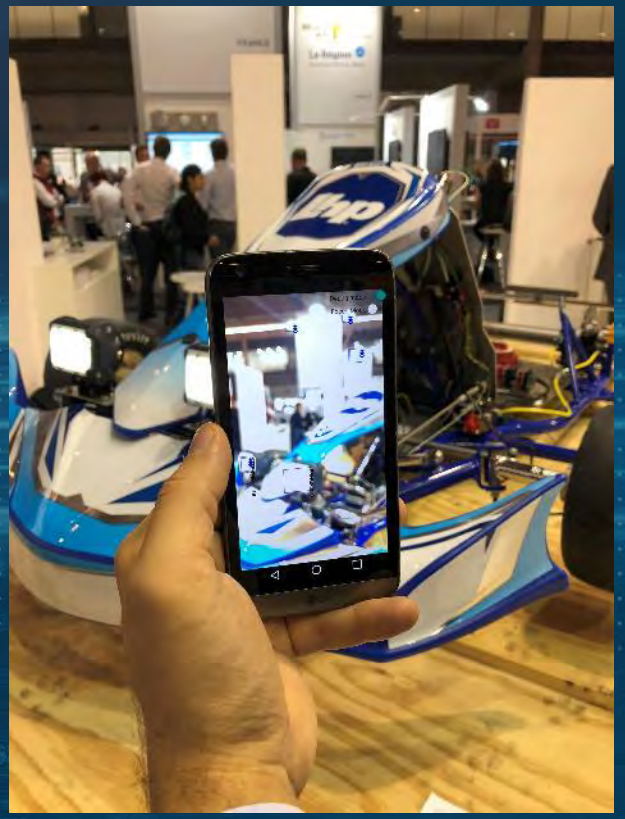
# IIC AUTOMOTIVE INITIATIVES

- Task Groups
  - Automotive
  - Automotive Security
- Automotive  Demonstrators & Testbeds
  - First demonstrator presented at IOT SWC, Oct 2018
- Collaboration with External Groups
  - Alliances/consortia (5GAA, AutoISAC, …)
  - Standards organizations (SAE, AUTOSAR,…)
- Thought Leadership
  - Automotive Trustworthiness Whitepaper

RSA

# IIC AUTOMOTIVE DEMONSTRATOR







RSA

# ITS RESEARCH

- IIC
- Dell Technologies

industrial internet CONSORTIUM

Automotive Initiatives @IIC

Quantum Computing Readiness

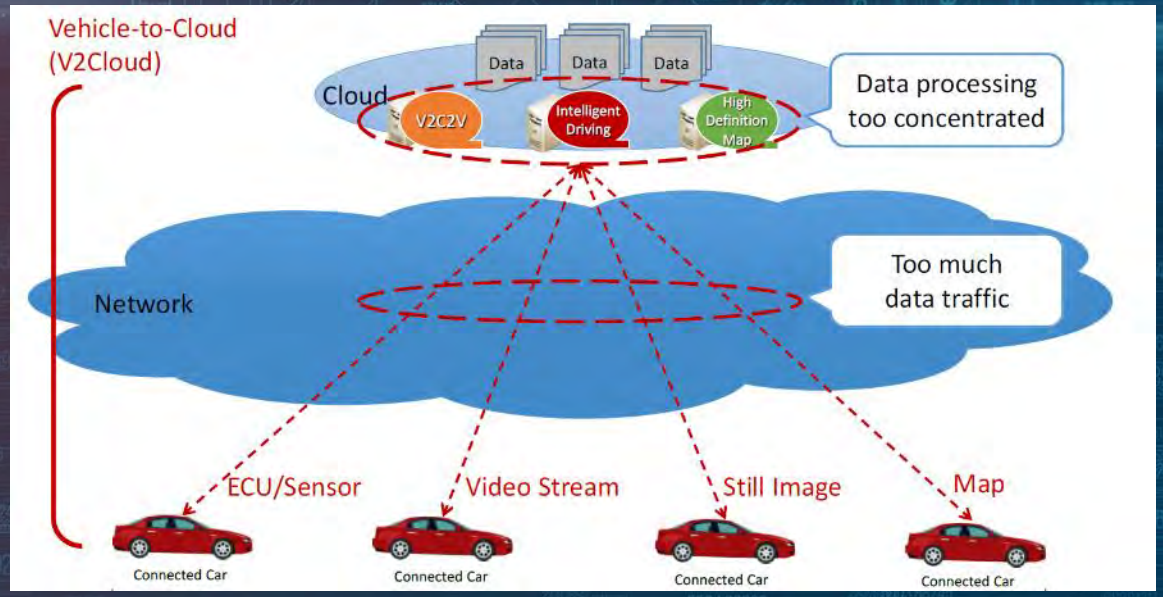
Connected Car Ecosystem

Advanced Automotive Manufacturing

RSA

# CONNECTED CAR ECOSYSTEM

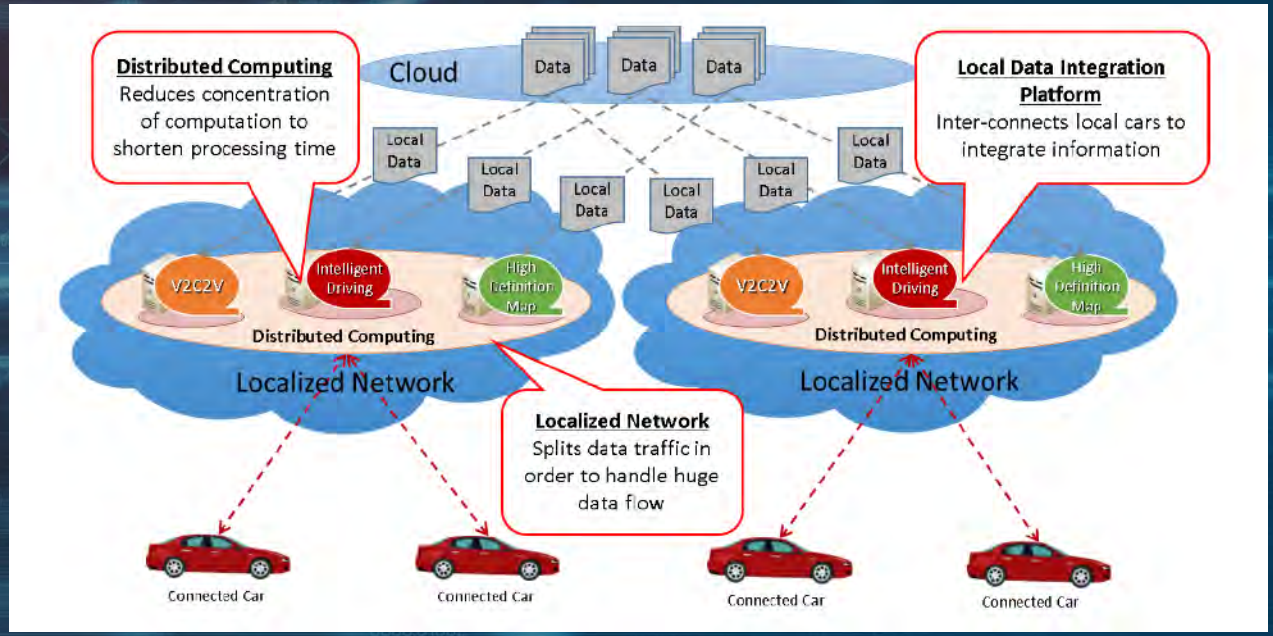
- Opportunity
  - By 2020, it is expected that 10 million self-driving cars will be on the road while there will be more than 250 million smart cars connected to high-tech networks sharing the road with them.[1]
- Data is the new Fuel Driving Innovation




1 Business Insider

# CONNECTED CAR ECOSYSTEM

- Challenges
  - Global scale
  - Data storage
  - Device management
  - Security
- Dell Technologies Research
  - Collaboration with a number of automakers and
  - Standards groups (e.g. AECC)




1 Business Insider

# ITS RESEARCH

- IIC
- Dell Technologies

industrial internet CONSORTIUM

Automotive Initiatives @IIC

Quantum Computing Readiness

Connected Car Ecosystem

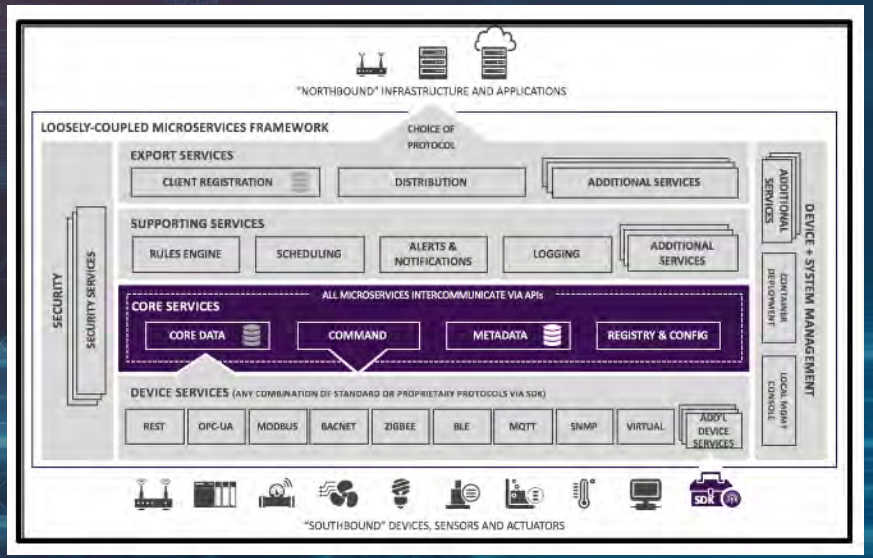
Advanced Automotive Manufacturing

RSA

# ADVANCED AUTOMOTIVE MANUFACTURING

- Edge Computing
  - Open Platform

EDGE X FOUNDRY™




- Security Research

**Threat Detection**

Monitoring and Threat Detection using Anaytics/ML

**Data Protection**

Lightweight, FIPS-Compliant Cryptography for IoT

**Identity Management**

Decentralized ID based on a Distributed Ledger

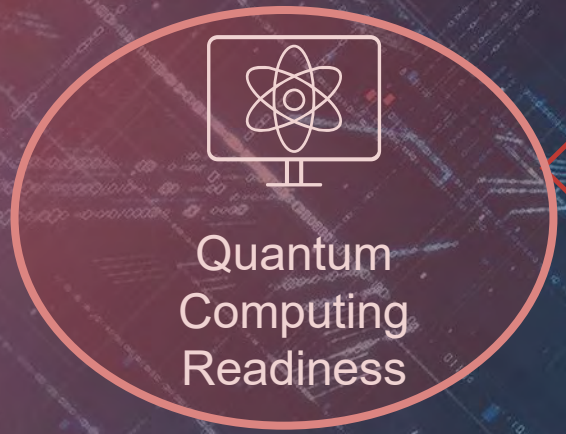
RSA

# ITS RESEARCH

- IIC
- Dell Technologies

industrial internet CONSORTIUM

Automotive Initiatives @IIC



Quantum Computing Readiness

Connected Car Ecosystem

Advanced Automotive Manufacturing

RSA

# QC IMPLICATIONS FOR IIOT

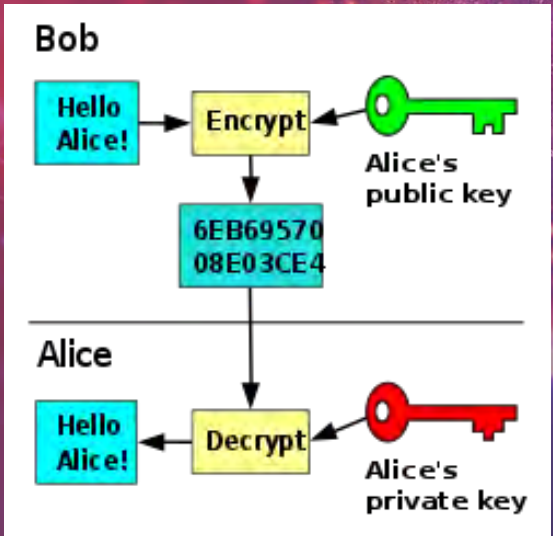
The Average Life of An Industrial Asset
Is
19 Years!

*Diagrams source: Wikipedia.*

# QC AND PUBLIC KEY CRYPTOGRAPHY

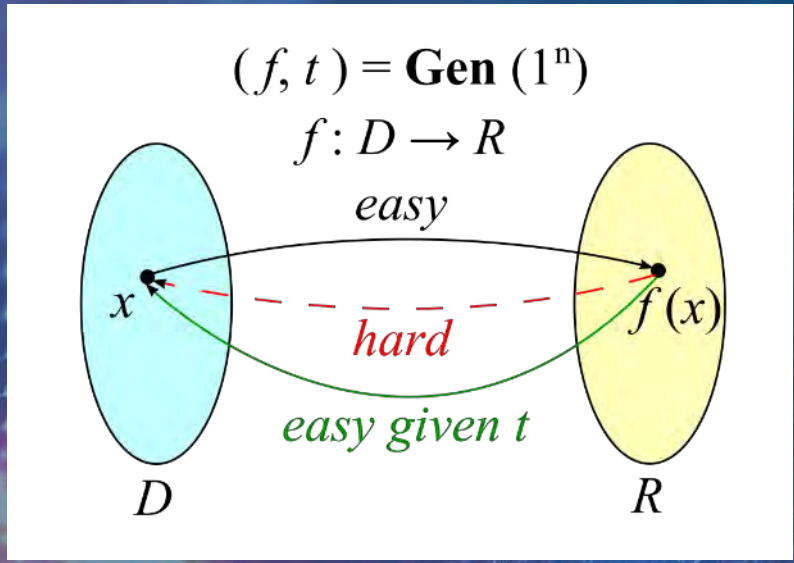
One-way (trapdoor) functions

PKC: Solves the problem of key exchange between the sender and receiver over an insecure communication channel.




**Trapdoor functions:**

- Easy to generate public key from private key
- Hard to find private key from public key!




Key underlying hard problems:

RSA: Integer factorization problem
DSA: Discrete logarithm problem
ECC: Elliptic curve discrete logarithm problem

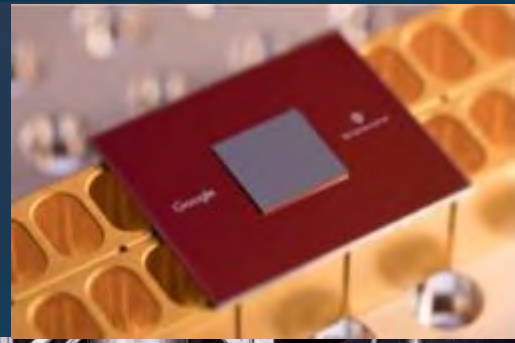
Could widely used trapdoor functions in PKC be vulnerable to QC?

*Diagrams source: Wikipedia.*

# QUATUM COMPUTING IMPACT

Google's new 72-Qbit quantum processor called Bristlecone. (March 2018)

"We are cautiously optimistic that quantum supremacy can be achieved with Bristlecone



## 1990

Peter Shor demonstrates efficient quantum algorithms for breaking RSA, Diffie Hellman, and Elliptic Curve Diffie Hellman (assuming quantum computers can be built to scale)

IBM Q
50 qubits
Can maintain state for 90 microsec.

Intel test chip
49 qubits
Si + quantum dots

D-Wave
2000 qubit
Quantum Annealer

# QUANTUM COMPUTING READINESS

## Cryptographic Agility

Designing for cryptographic “agility”
(simplifying process of replacing algorithms)

## Impact Analysis

Monitoring / assessing risks of
quantum computing through impact analysis

RSA

# THANK YOU

rzolfonoon@rsa.com

RSA BUSINESS-DRIVEN SECURITY™