How to prepare the automotive V2X-ecosystem for the quantum age ? A perspective on cybersecurity with the US highway and smart city infrastructure in mind

Dr. Joachim G. Taiber, Chief Technology Officer International Transportation Innovation Center (ITIC), Founder of the International Alliance for Mobility and Standardization (IAMTS) and Adjunct Professor of the Clemson University International Center of Automotive Research

IEEE Cybersecurity Webinar, January 27, 2021

iamts™
International Alliance for Mobility Testing and Standardization
A Program of SAE ITC

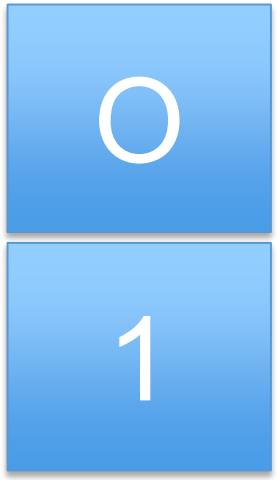
iTiC INTERNATIONAL TRANSPORTATION INNOVATION CENTER

CUICAR
CLEMSON UNIVERSITY INTERNATIONAL CENTER FOR AUTOMOTIVE RESEARCH

The emergence of the quantum age

Classical computer

BIT

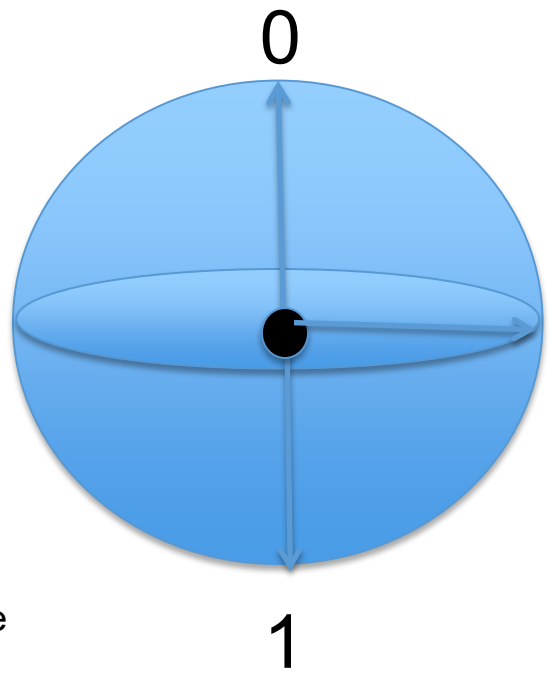


Data storage and calculations are based on a binary system

0110010, 10111010
10110110, 00101011 …

Quantum computer

QBIT



Quantum bits can take any state between 0 and 1 (superposition and entanglement)

Quantum computers can solve certain problems in a fraction of time classical computers would need

Quantum safe systems can withstand cyber attacks both from classical and quantum computers

Quantum computers are not widely commercially available at this time and in general the technology is still at a very early stage of development

Once quantum computers mature and become commercially available, existing IoT and V2X systems become vulnerable from a cybersecurity perspective unless they are designed as crypto-agile systems

IBM promises 1000-qubit quantum computer—a milestone —by 2023

Potential application areas of quantum computing in Automotive

Automotive R&D

Vehicle crash simulation

Aerodynamic optimization

Acoustic optimization

Weight optimization

Energy storage

Supply chain optimization

Embedded systems

Data centers

V2X

Situational Awareness (crash avoidance)

Cybersecurity threat prevention

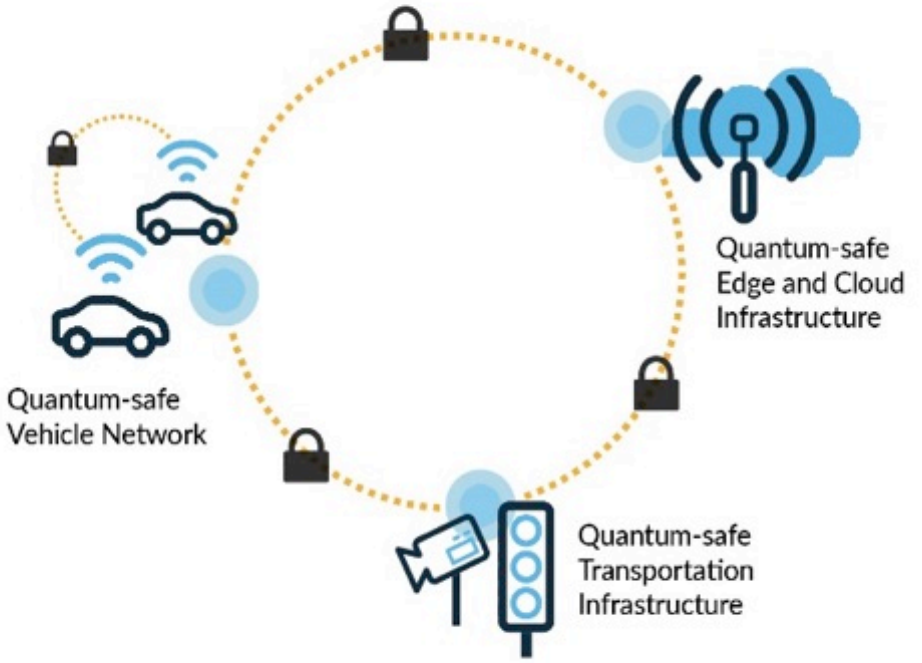
Automotive fleet operation

Traffic route optimization

Energy use optimization

Autonomous driving (co-simulation virtual and physical vehicles in real time)

A quantum-safe V2X ecosystem



Quantum Random Number Generation (QRNG)

- ✓ Instantly strengthen your network encryption key material
- ✓ Feed higher quality entropy into key generation servers, HSMs, Linux & crypto applications

State-of-the-art and Quantum-ready encryption

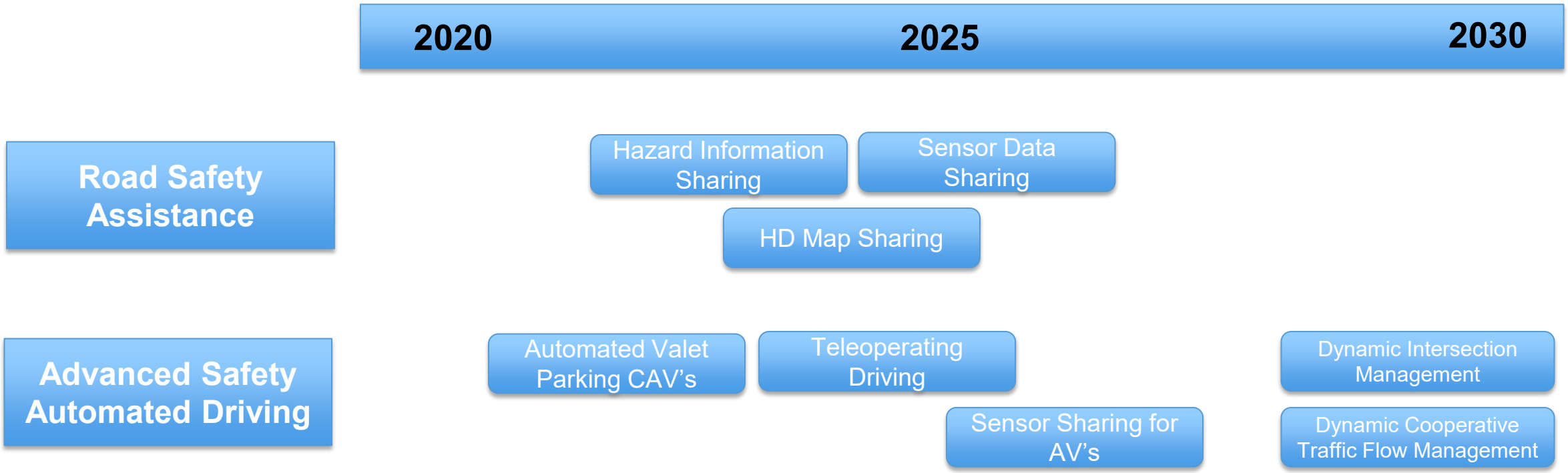
- ✓ Only go with AES-256 symmetric encryption and dedicated robust appliances
- ✓ Be **crypto-agile** & be **QKD ready** (ready to upgrade to quantum cryptography)
- ✓ Protect your investments for the next decade and further

Quantum Key Distribution (QKD)

- ✓ Quantum-Safe Network Encryption or **Quantum Cryptography**
- ✓ Provide forward secrecy and anti-eavesdropping of the encryption keys
- ✓ Ensure sovereignty and data ownership for the next decade (Post-Quantum era)

Source: ID Quantique

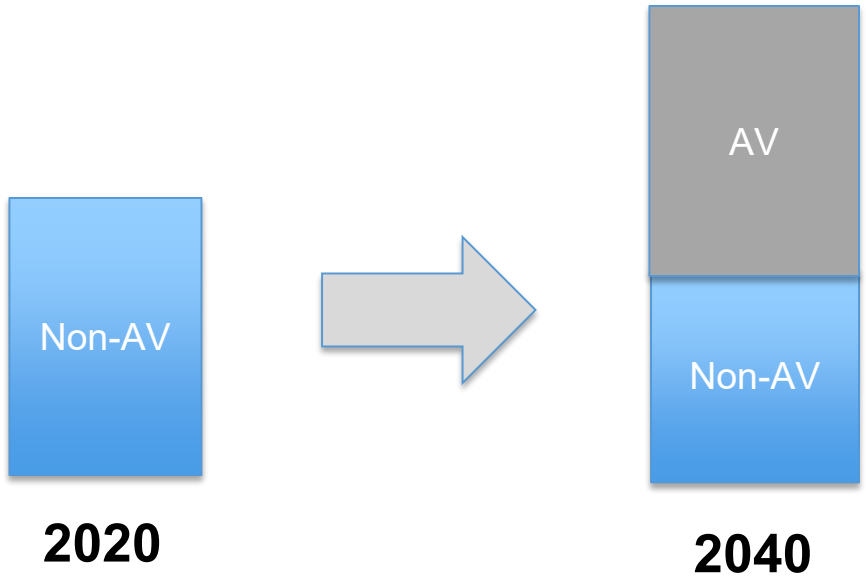
Technology roadmap V2X until 2030



Source: 5GAA

Outlook role of AV driving

Autonomous vehicles will travel about 66% of total passenger miles in 2040



*The software complexity will increase drastically until 2030 until AV technology becomes mainstream whereas software productivity will fall behind not being able to cope with the complexity gap. This will lead to a **higher security risk level** for CAV's as their penetration in vehicle fleets rises.*

Source: McKinsey

It is estimated that the total miles driven per vehicle (in particular AV's) will significantly increase (note that this is a qualitative illustration)

How much computing power will be needed to “harden” automotive V2X-systems to be quantum-safe ?

Automotive systems represent “Life Critical Embedded Systems” which require “enough computing capacity for stronger cryptographic and runtime protection that will need to be added within the lifetime of the systems” as described in a US Department of Homeland Security report*. The report recommends the following system design principles:

- All interactions between devices MUST be mutually authenticated.
- Continuous authentication SHOULD be used when feasible and appropriate.
- All communications between devices SHOULD be encrypted.
- Devices MUST NEVER trust unauthenticated data or code during boot-time.
- Devices MUST NEVER be permitted to run unauthorized code.
- Devices SHOULD NEVER trust unauthenticated data during run-time.
- When used, cryptographic keys MUST be protected.

*https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

How to apply a quantum risk assessment

First and foremost, it is essential to complete a thorough risk assessment across all system levels (end-to-end) to analyze where in the automotive ecosystem quantum technologies can pose a risk*.

There are five key steps to such a quantum risk assessment:

1. Analyse all assets and determine their cryptographic protection.

2. Map the technological progress in quantum technologies to the state-of-the-art technology being used in the target system.

3. Test and validate quantum-safe cryptography methods.

4. Identify potential threat actors and estimate the time until they could apply quantum technologies for attacks, which determines the timeline to make the target system quantum-safe.

5. Develop a plan to bring the target system into a quantum-safe system state and prioritize activities to anticipate the highest risks

*https://globalriskinstitute.org/publications/3423-2/

NIST working on post-quantum cryptography standard

After spending more than three years examining new approaches to encryption and data protection that could defeat an assault from a quantum computer, the National Institute of Standards and Technology (NIST) has winnowed the 69 submissions it initially received down to a final group of 15. NIST has now begun the third round of public review. This "selection round" will help the agency decide on the small subset of these algorithms that will form the core of the first post-quantum cryptography standard.

NIST plans to release the initial standard for quantum resistant cryptography in 2022.

Source: NIST

The implementation of quantum resistant cryptography will be a major challenge for the Automotive industry !

Influence of NIST framework for improving critical infrastructure cybersecurity on Automotive

It is important to note that the Alliance of Automobile Manufacturers and the Association of Global Automakers adopted content from the NIST framework for improving critical infrastructure on cybersecurity to develop an

Automotive Cybersecurity Best Practices Framework

to consider the safety and security of the overall vehicle ecosystem.

However, it is important to note that so far the emergence of quantum computing and quantum resistant cryptography is NOT considered so far in context of protecting the V2X ecosystem end-to-end !

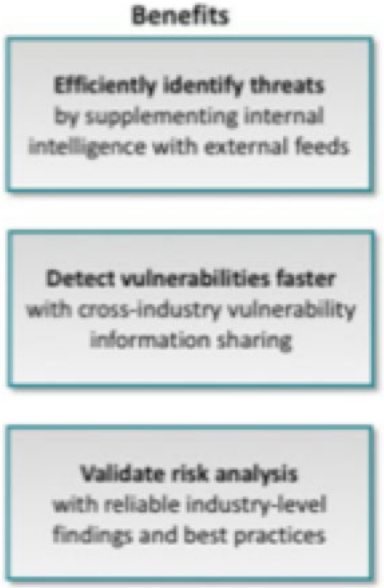
Role of Auto-ISAC with respect to automotive cybersecurity in the US

AUTO-ISAC stands for Automotive Information Sharing and Analysis Center

AUTO-ISAC was created in 2015 and was preceded by the establishment of Consumer Privacy Protection Principles for Vehicle Technologies and Services in 2014.

SCOPE of AUTO-ISAC:

Aggregate, analyze and share auto-specific cyber information across the industry's attack surface



Currently Auto-ISAC accounts for more than 99% of light duty vehicles in North America with more than 30 global Automotive OEM and supplier members and is expanding into the commercial vehicle sector.

Source: Auto-ISAC

Cybersecurity approach of USDOT

The USDOT has several research programs dedicated to ensuring a secure connected transportation environment:

- Vehicle Cyber Security – Focuses on preventing attacks from entry into our vehicle systems and components
- Infrastructure Cyber Security – Focuses on protecting against threats and vulnerabilities to our nation's roadside equipment, devices, and systems
- Dedicated Short-Range Communications (DSRC) Security – Focuses on ensuring trusted communications between vehicles and between infrastructure and vehicles
  - Security Credential Management System (SCMS) Operations
  - SCMS Management
- ITS Architecture and Standards Security – Focuses on the development of architecture and standards required to ensure security in the connected vehicle environment.

Note that on November 18, 2020 FCC repurposed a major portion of the 5.9 GHz band for Wifi use and C-V2X

Source: USDOT

The relevance of the transportation network in the US

- **Jobs:** The Federal Highway Administration (FHWA) estimates that every $1 billion in highway spending supports 13,000 jobs throughout the economy. At current levels, transportation investment supports 4 million U.S. jobs across all sectors of the U.S. economy.
- **Economic Growth:** Construction work performed on transportation projects, including highways, bridges, subways, light rail systems, freight rail, airports and water ports, generates over $508 billion in total annual U.S. economic activity and contributes approximately $254 billion to the U.S. Gross Domestic Product.
- **Freight Shipments:** More than $18.1 trillion in freight was shipped in the United States in 2016, according to FHWA. Trucks were involved in 82 percent of all freight shipped. Rail, air, water, and pipelines accounted for the remaining 18 percent of freight shipments. FHWA estimates that the value of freight shipments will increase by 84 percent between 2016 and 2040.

Source: ARTBA

The US transportation network would be vulnerable to quantum computing attacks in the future if no prevention is being addressed !

The future of the US road system

Cooperative Adaptive Cruise Control Platoon Scenario

Source: USDOT

Enabling groups of vehicles to jointly agree on maneuvers, path and speed trajectories.

Real-time coordination promises to improve overall traffic throughput, road capacity, and passenger safety.

Control strategies can be implemented on a vehicle-to-vehicle basis (decentralized) but also on a vehicle-to-infrastructure basis (centralized)

Coordinated driving will emerge and will primarily influence:

> Highway corridors

> Smart intersections in urban environments

As coordinated driving requires V2X interoperability it is very important to consider quantum resilience from a cybersecurity perspective (working in collaborative structures across OEM's, suppliers and critical infrastructure service providers) !

The quantum age needs to be considered in the further development of the V2X ecosystem

How to make the complete V2X ecosystem quantum-safe:

> Implement standardized components such as QRNG (quantum based random number generator)

> Use PQ (post quantum) encryption algorithms

> Apply QKD (quantum key distribution) concepts

> Use reconfigurable hardware

In this context it is important to adapt system engineering processes to consider new quantum-safe design principles and to train system development engineers accordingly.

Source: SAE Edge report 2020 “Unsettled Topics Concerning the Impact of Quantum Technologies on Automotive Cybersecurity”