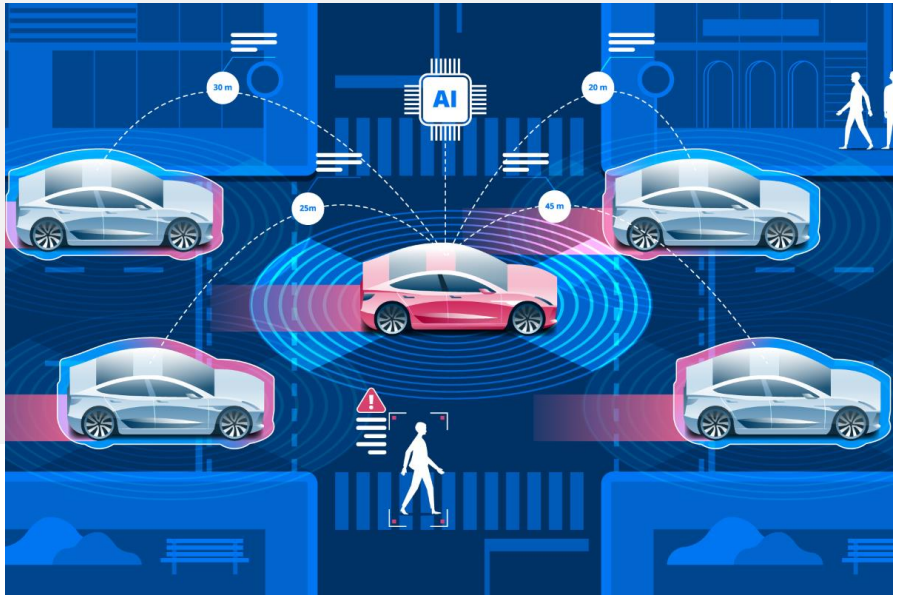
CYBER + ASAP

The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

AI-DRIVES
- AI-Driven Secured Connected and Autonomous Vehicles (CAVs)

Why: Fast emerging CAVs vulnerable to security risks
Product: Secured and fast Vehicle-to-Everything (V2X) communications
How: Machine learning compliant to V2X standards
Who: Tier 1 automotive transceiver providers

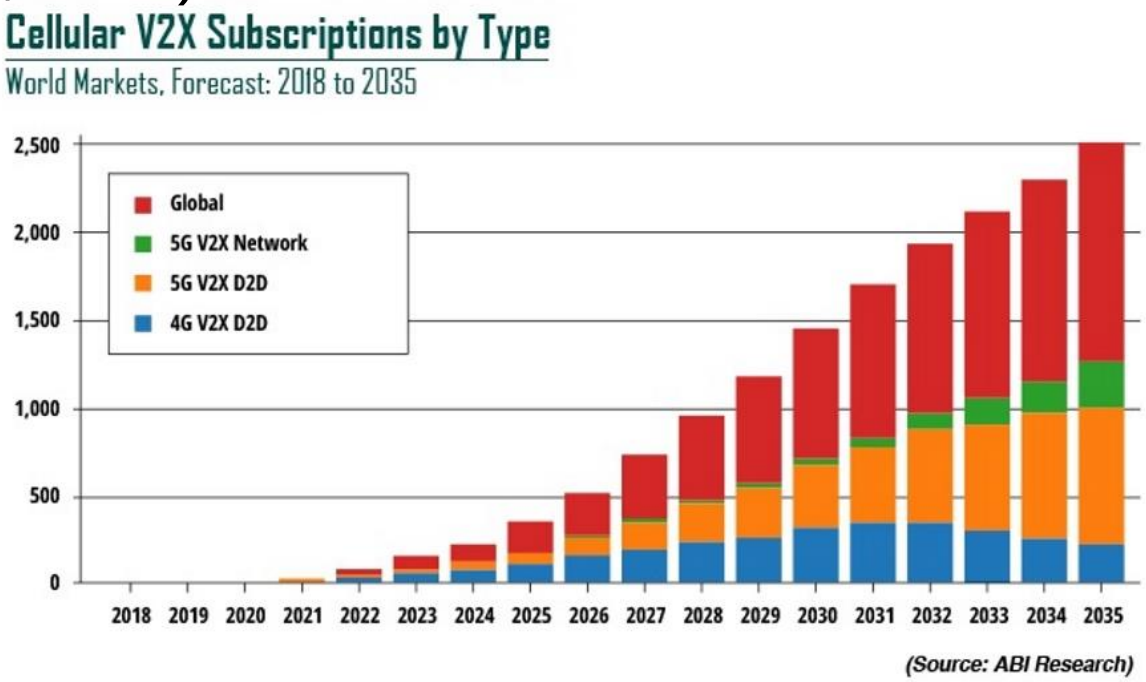
Rong Qu, Jeremie Clos, Vaughan Wang
School of Computer Science
Mr George Rice
Head of Commercialisation



Challenges

- By 2026: all new cars in the UK will be connected (SMMT 2019)
- By 2030: 146M connected cars, 31.3M in 2017 (statista.com)

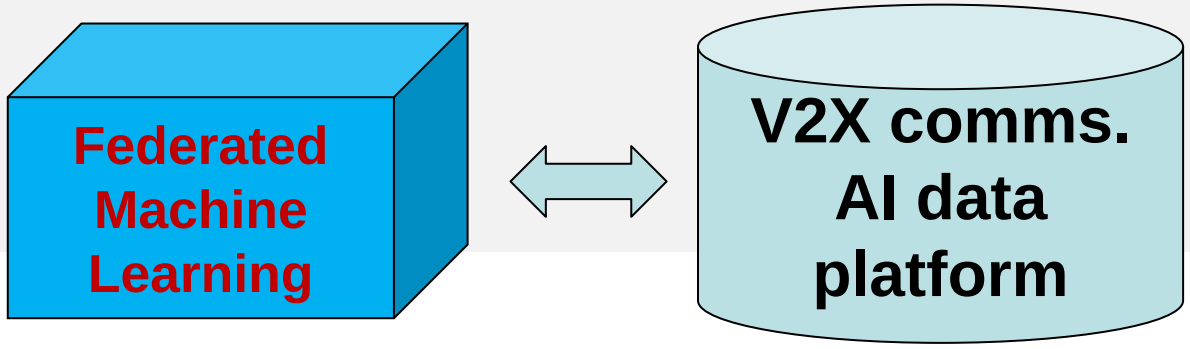
- Significant and urgent need of secured V2X communications
  - "most readily-used tech focuses entirely on the autonomous elements and not on connectivity" (UK AutoDrive, 2017)
  - Risks: fatalities, data / financial losses

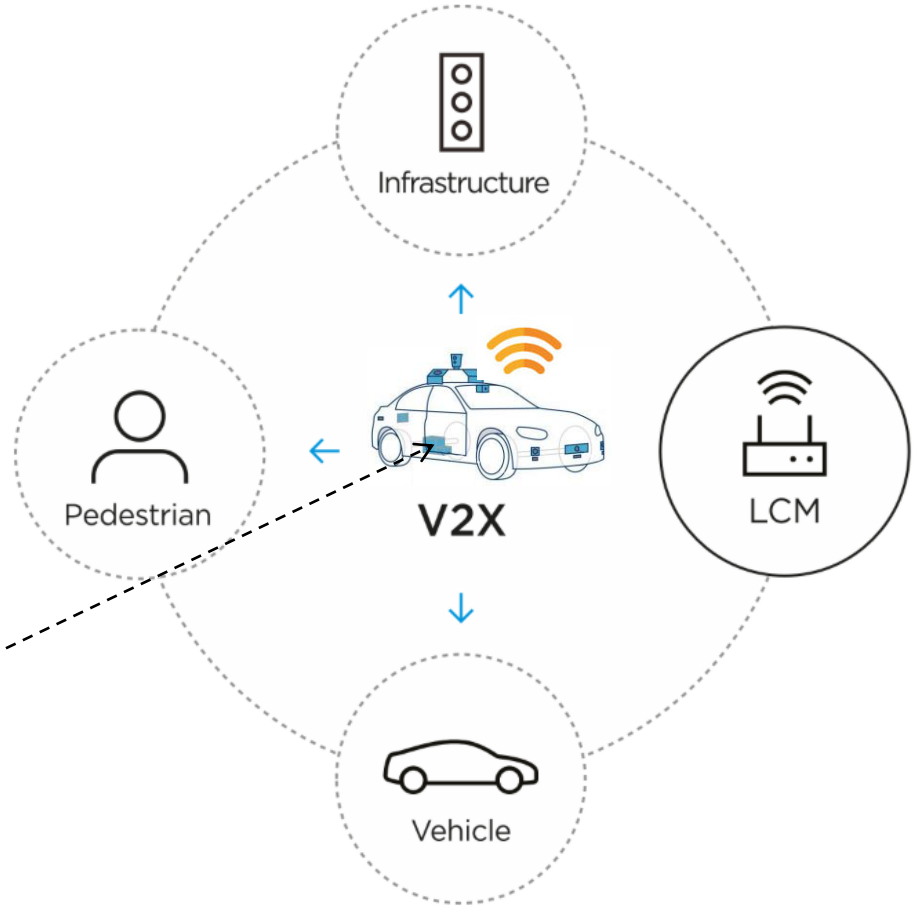


Technologies

AI-DRIVES: V2X communications secured by federated machine learning

1) Security as a Service: V2X anomaly detection engine with federated learning
   - Quicker: reduce V2X communications
   - Data privacy: learning on own data
   - Scalable: local knowledge shared globally
2) AI data platform: V2X communications data
   - Knowledge on anomaly of different severities
   - Standards: DSRC | C-V2X | hybrid

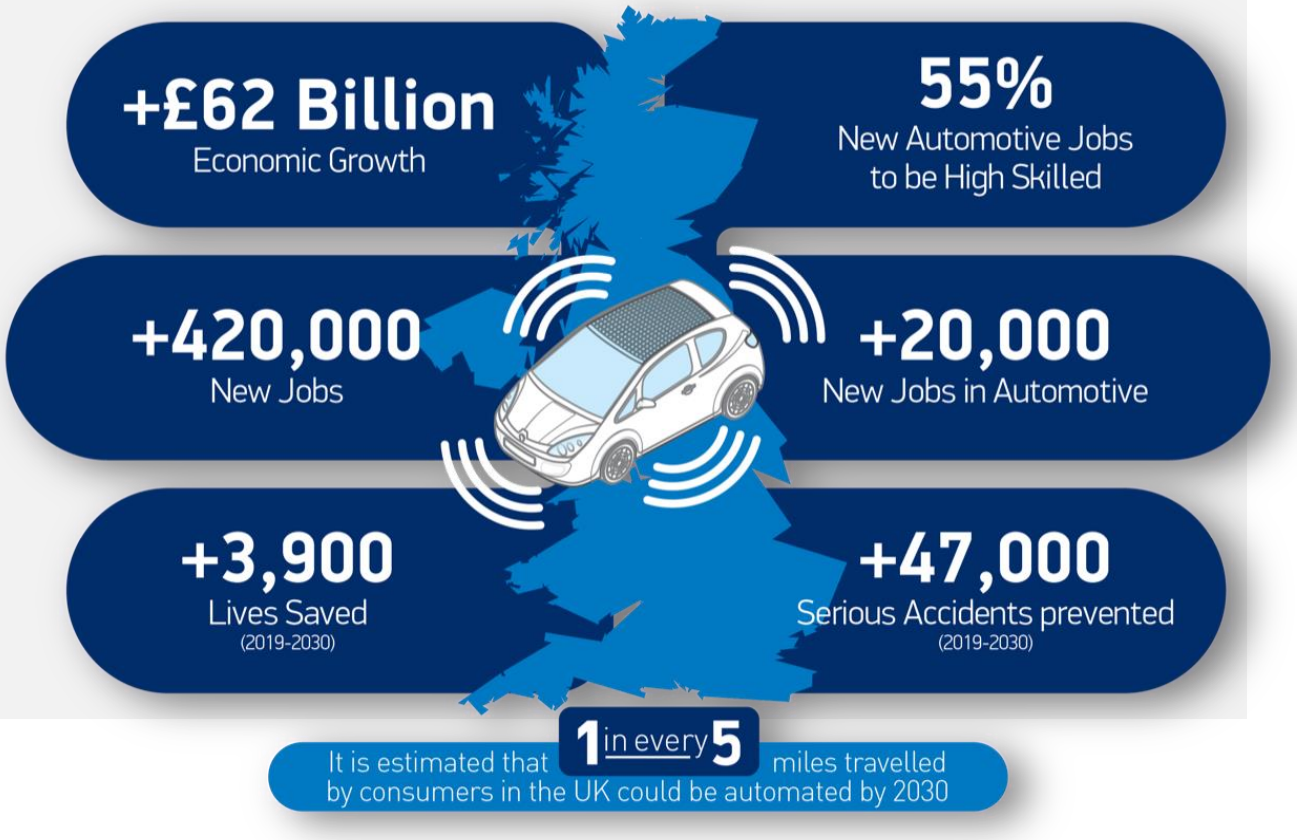




Market Drivers

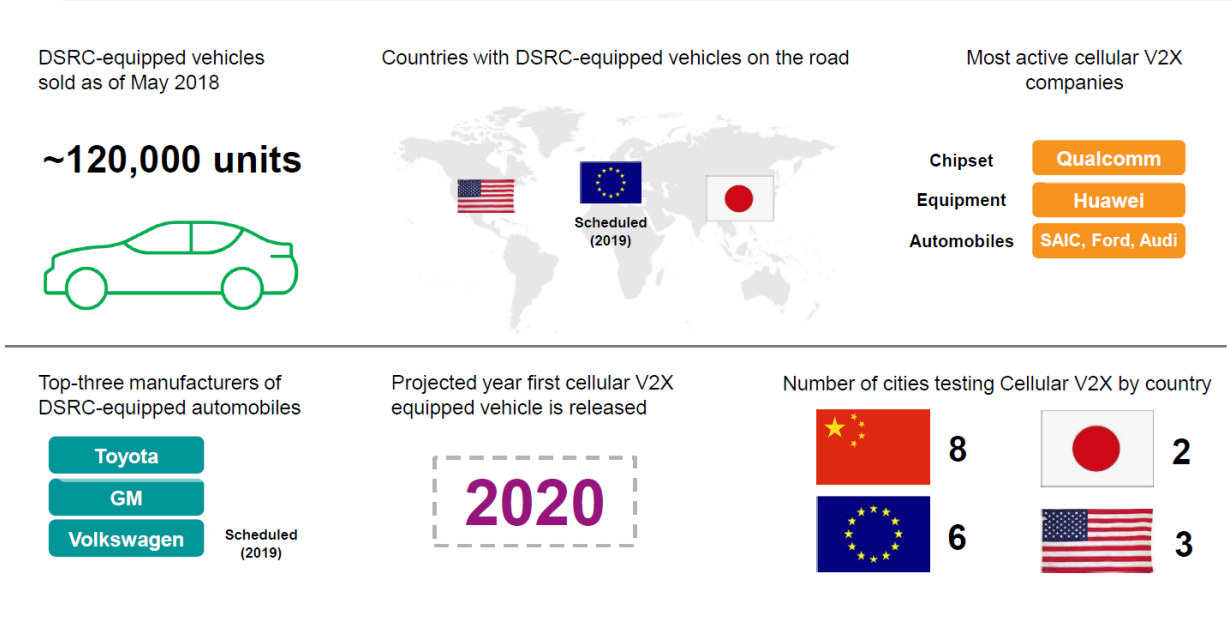
- Efficiency & productivity
  - 237% increased highway capacity if all cars use sensors and V2V comms.
  - On demand Mobility As a Service

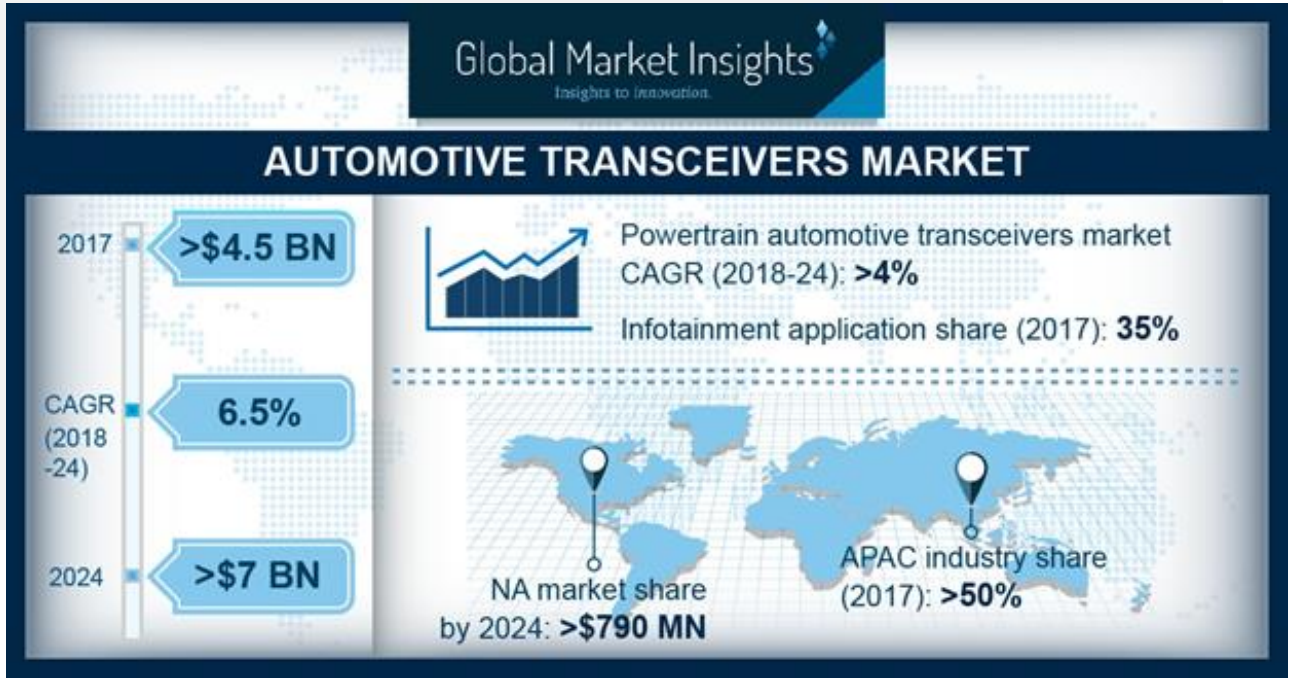
- End users
  - With CAVs: reduce traffic deaths by 90% (McKinsey & Company)
  - With V2V: reduce 13% accidents, 439k fewer crashes a year (US DoT)



Market Size

- CAVs globally
  - Overall £907bn by 2035 (Transport Systems Catapult, 2017)
- Automotive transceiver market
  - More than $7bn by 2024





Next Steps

- Validate AI-DRIVES solution and clarify technical specifications
  - Customers/channels: approach Tier 1 providers via UbiPOS network
  - Commercial model
- IP position: being assessed
- Routes to commercialisation

- Funding
  - SIGKDD, June 2020
    - Data collection: simulations
    - MVP: simulations within six months
  - Innovate UK, Cyber Security in IoT, next round

CYBER + ASAP

Marke

Components	Value at L3 (at scale)	Value at L4/5 (at scale)
LIDAR	$800	$900
Cameras	$300	$255
Embedded controls	$200	$200

CAV TECHNOLOGIES

For CAV technology sales to automotive sector: market value is £63bn.

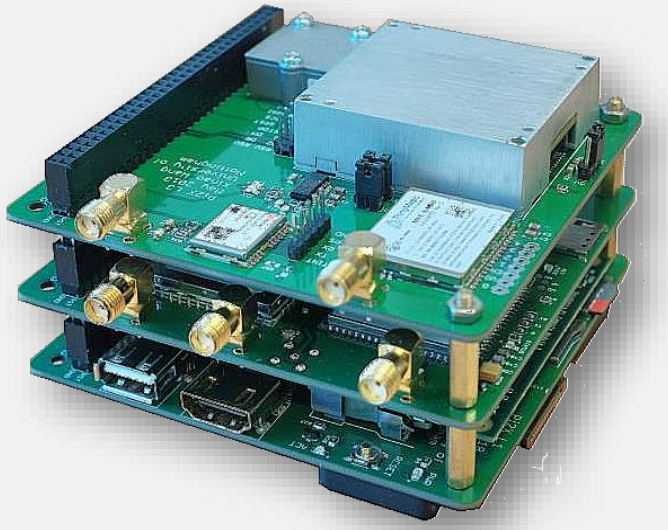
Value based on CAV technology sales values (before 50% OEM mark-up)

TABLE 3.7 Assumed share of autonomy package value by component. At L3, 35% of the total value is assumed to be software, and at L4/5 this is assumed to rise to 50%. Assumptions are described in full in Appendix B.

Component	Percentage of value at L3	Percentage of value at L4/5
LIDAR	25%	24%
Radar	12%	8%
Cameras	9%	7%
V2X hardware	3%	1%
V2X software	12%	14%
Embedded controls hardware	2%	1%
Embedded controls software	7%	9%
Mapping hardware	2%	1%
Mapping software	6%	9%
Data security software	5%	12%
HMI hardware	2%	2%
HMI software	6%	6%
Actuators	2%	2%
[illegible]ture	3%	3%
[illegible]	2%	1%
[illegible]	0.3%	0.1%
Embedded modem	0.3%	0.3%
Passive components	0.5%	0.7%

UoN: Ongoing Research

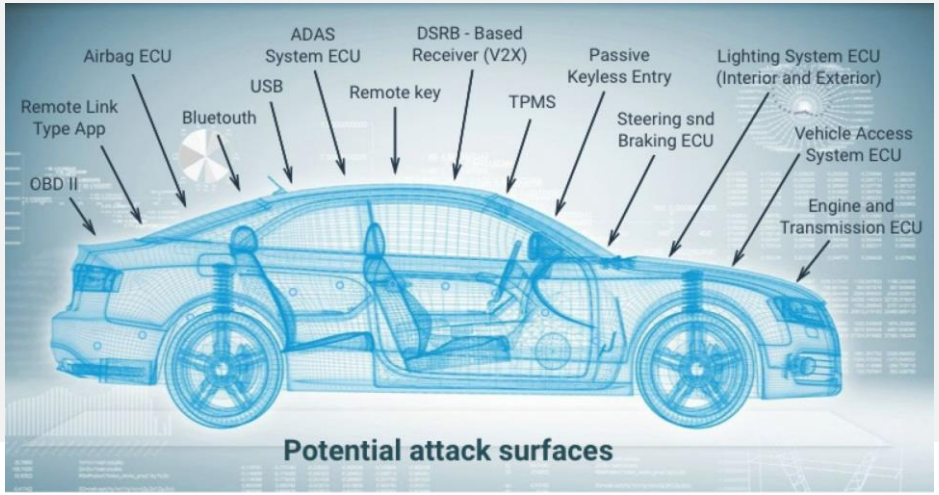
- Collaborator:
  - NGI: GNSS/INS sensor integrated board, with DSRC/Cellular enabled device for collaborative navigation
  - UbiPOS UK Ltd

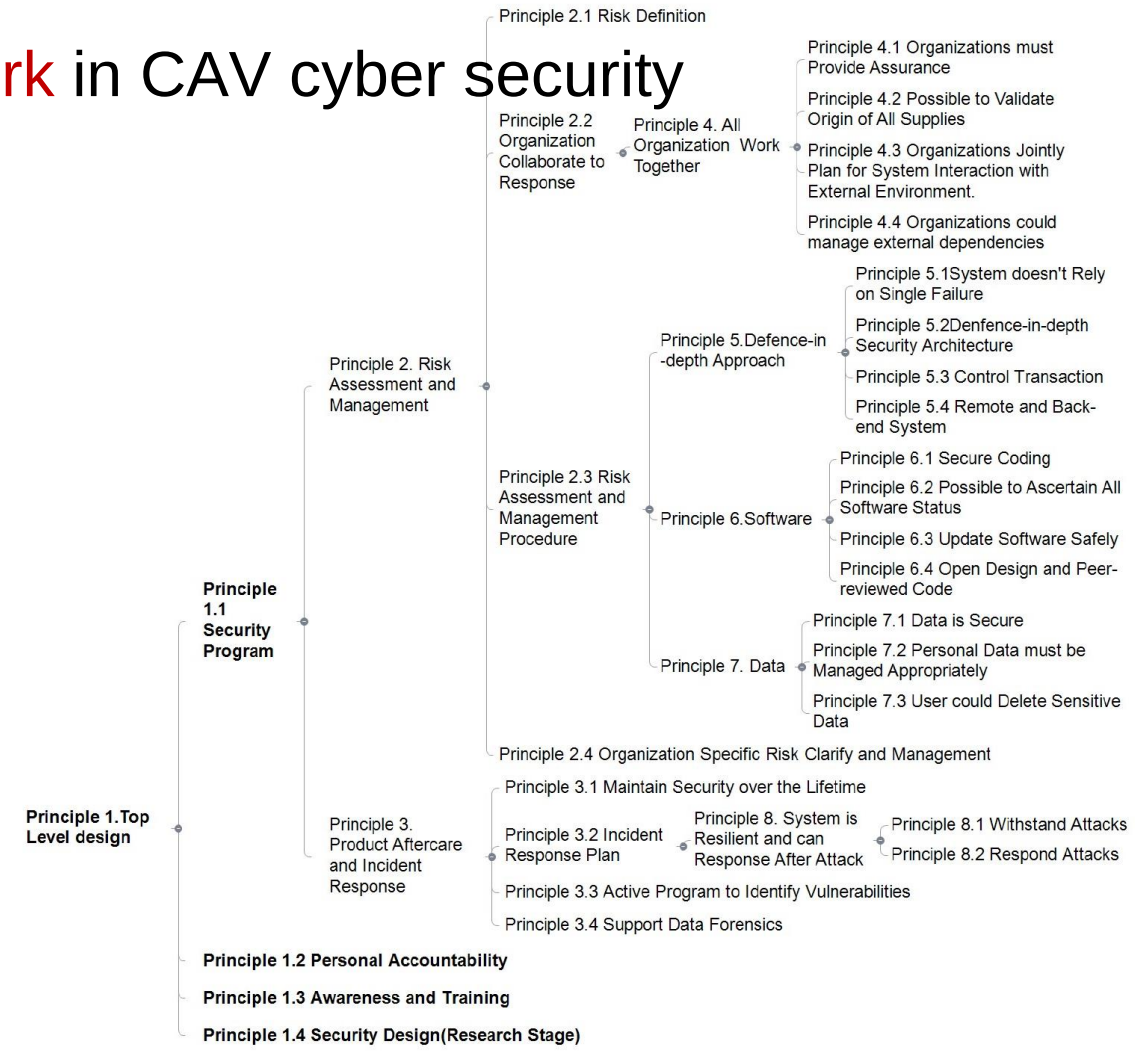


UoN: Ongoing Research

- Current: lack of commonly used framework in CAV cyber security
  - CAV attacks types defined
  - CAV attack points classified
  - Prevention mechanisms conducted

- A common framework of CAV security
- A database of CAV cyber-attacks





Qiyi He, Xiaolin Meng, Rong Qu, Ruijie Xi, Design A New Framework for Assessing Cyber Security Attacks to Connected and Autonomous Vehicles, 2019

UoN: Ongoing Research

The University of Nottingham
UNITED KINGDOM · CHINA · MALAYSIA

- CAV cyber-attacks
  - Passive: eavesdropping, traffic analysis
  - Active: spoofing, replay, modification, DOS

- Derived CAV-KDD dataset
  - Four major types
  - 39 sub-attacks
  - 39 CAV atrributes
  - 14 comm.-based sub-attacks

- Machine learning
  - Decision tree vs. SVM

Category	Attack points
Physical Parts	Sensors(LiDAR, Radar, Camera), GNSS device, vehicle system (OBD, CAN-bus, power system) etc.
Software	Mobile applications installed on the vehicle, in-vehicle system (entertainment system), data processing system, decision making system etc.
Data	local data (vehicle ID, payment information, userś personal information), Exchange data (Vehicle's speed, brake status) etc.
Communication Channel	V2I (Vehicle to Infrastructure), V2V (Vehicle to vehicle), V2C (Vehicle to Cloud), V2X (Vehicle to everything) etc.

Q. He, X. Meng, R Qu. Towards a Severity Assessment Method for Potential Cyber Attacks to Connected and Autonomous Vehicles. Journal of Advanced Transportation, 20, 2020
Q. He, X. Meng, R Qu, R. Xi. Machine Learning-Based Detection for Cyber Security Attacks on Connected and Autonomous Vehicles. Mathematics, 8(8): 1311, 2020