High Level Connected/Smart Vehicle Threats

1. Vehicle

- External hacking/contamination of:
  - safety-critical functions;
  - non-safety functions;
  - information systems;
- Illegal/unauthorised changes to vehicle's electronic ID;
- Hacking/tampering to circumvent monitoring systems or falsify data;
- Jamming (via natural or unnatural interferences) of radio based (wireless) systems including navigation systems;
- Spoofing of sensor data;
- Interference with control units, master data and firmware/software;
- Unintended impact caused by mistaken action by owner, operator or maintenance engineer;
- Unintended impact caused by owner, operator or maintenance engineer being tricked into taking an action;
- Misuse of functions designed to remotely operate systems;
- Components, or software, engineered or altered to enable an attack;
- Use of a vehicle as means to compromise connected devices etc.;
- Use of a vehicle as a weapon;
- Compromise of back-end/supporting servers;
- Compromise of software update procedures, including over-the-air updates.

2. Vehicle-to-vehicle

- Transmission/communication of false/unreliable/contaminated data to other vehicles;
- Interference with wireless systems or sensors;
- Use of vehicle-vehicle communications to compromise other vehicles systems.

3. Vehicle-to-Infrastructure

- Use of vehicle to infrastructure connections as attack vector against infrastructure systems;
- Transmission of false/unreliable/contaminated data to infrastructure;
- Compromise of external connectivity.

4. Infrastructure-to-vehicle

- Transmission of false/unreliable/contaminated data to vehicles;
- Unintended impact caused by mistaken action by infrastructure maintainer;
- Misconfiguration of equipment by maintenance community during installation/repair;
- Local physical attack/compromise on the roadside infrastructure:
- Components engineered to enable a potential attack on roadside infrastructure;
- Failure of equipment – systems must have sufficient resilience to withstand the harsh roadside elements e.g. severe weather;
- Spoofing/Impersonation of roadside infrastructure messages;
- Compromise of external connectivity;
- Compromise of back-end/supporting servers.