Noble

Securing Data and Innovation in Connected Cars

An Automotive Industry Use Case

The future of the automotive industry looks mind-blowing with autonomous, electric engines, biometric car access, remote vehicle shut down, driver health monitoring and driver override technology as examples of ideas slowly transitioning from the engineers' drawing boards into reality.

The single constant across all these differing areas of automotive innovation is data. Data is a valuable resource for innovation and a valuable resource to lose; data which can be stolen and abused.

Data Challenges in the Automotive Industry

The automotive industry is charging ahead to have Level 5 autonomous vehicles (capable of generating data of 2 - 5TB per hour from its sensors) on the highways by 2020. This growth in transmittable and manipulative data increases personal risk for consumers and cyber targeting manufacturers in the industry. While on-board infotainment and telematics systems provide rich features desired by consumers, they also bring new legal and compliance risks in the form of potential privacy and security pitfalls and land-mines. Autonomous and highly automated vehicles only add to this complexity and risks. The modern-day car is a computer on wheels. Data is the oxygen for the innovation and there's no better example of how data is critical to the business than Formula 1. With 3,000 pieces of data collected from each car every second, which drives the consideration of over 1,000 new designs on average made for a Formula 1 car each week, the speed of innovation leaves no time to protect the intellectual property.

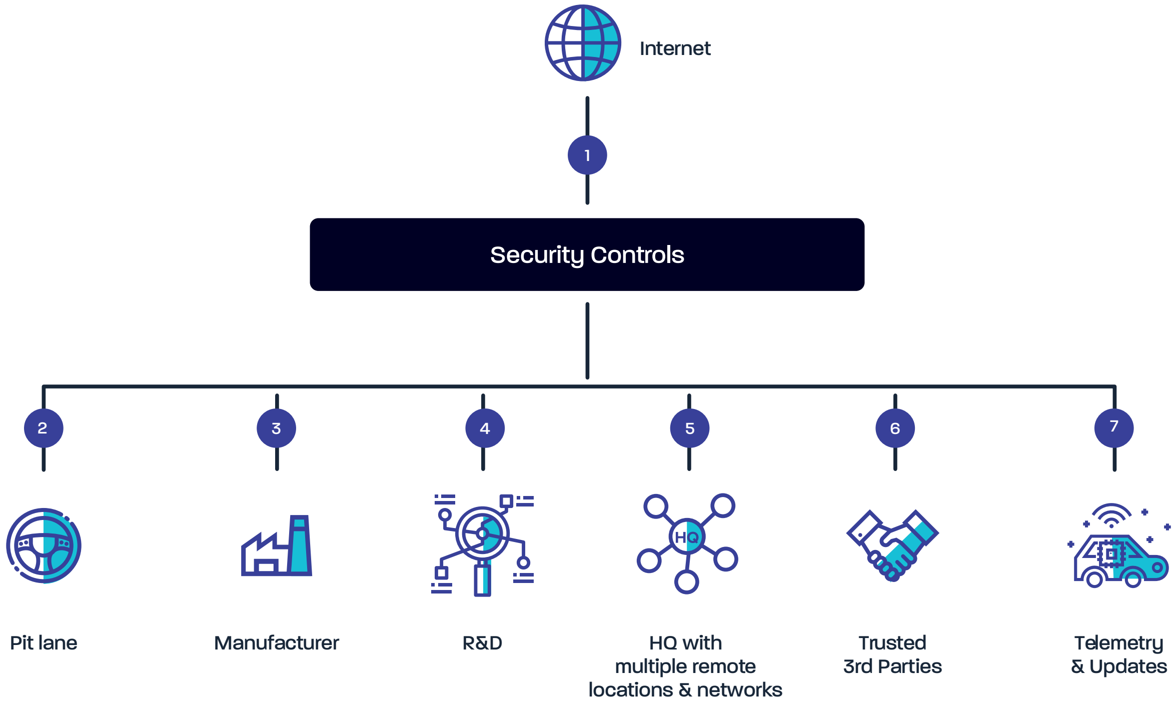
Risks of Anomalies in the Vehicle Data Network

In addition to the palpable safety concerns, researchers have also highlighted potential privacy invasions. By exploiting weaknesses in wireless communications systems or in devices that connect directly to cars (such as smartphones, insurance dongles, or diagnostic tools), hackers could conceivably gain access to data stored on a vehicle that describes its owner's driving habits, current location, entertainment preferences, or daily schedule. Businesses that offer company cars, operate fleets, and are considering the deployment of self-driving vehicles, are at risk, especially if they are liable for passenger safety. Typical businesses that fall into this category may include logistics providers, telecom providers, car rental agencies, construction firms, and delivery services (e.g., pizza, flowers). Logistics companies should confirm that companies which manufacture and maintain their trucks are on top of cyber risks.

Noble Vision alerts Automotive Data Driven Anomalies

With the vast increase of the attack surface and the potential impact of a cyber-attack, that is now a safety-critical matter, continuously monitoring the communication of automotive telemetry and decision data become critical, Noble Vision's advanced level of near real-time monitoring minimises the risk of unauthorised over-the-air updates, car intelligence manipulation or other malicious activities.

In addition to these layers of protection directly relating to a vehicle's connectivity, supply chain risk management is a critical element of the overall cybersecurity effort. Compromised physical components can jeopardise the integrity of a car's security architecture, making it imperative that the whole supply chain is completely and continuously analysed to reassess the trust of the suppliers.



1. Secure data flows from users, employees and partners
2. Secure race day data flows
3. Secure 2-way updates and performance stats
4. Secure manufacturing IP
5. Secure IP and real-time analysis
6. Secure supply chain policies
7. Secure operational and security data processes