GUARD KNOX

# Mitigating Cybersecurity Risks for Connected Vehicles

## Introduction

In 2015, researchers simulated the first hack of a connected vehicle. If they had succeeded only in controlling the air conditioning and radio, we might dismiss the hack as a prank that makes us uncomfortable but no more than that. However, the white-hat hackers went much further—they were able to disable the brakes and the steering remotely. At that moment, the concept of the connected car changed forever.  Cyberattacks could kill.

By the next year, malicious high-tech carjackers stole 100 cars via key code databases that they were able to reprogram to gain entry to the vehicles and actually start them and drive them off. We learned that cyber attackers could now steal our vehicles in numbers that were previously unthinkable.

By 2017, another set of researchers showed the world that they could exploit the internal networks within vehicles to shutdown airbags and automatic door locks. Suddenly, the connected car was exposed and vulnerable and the passengers inside were at risk.

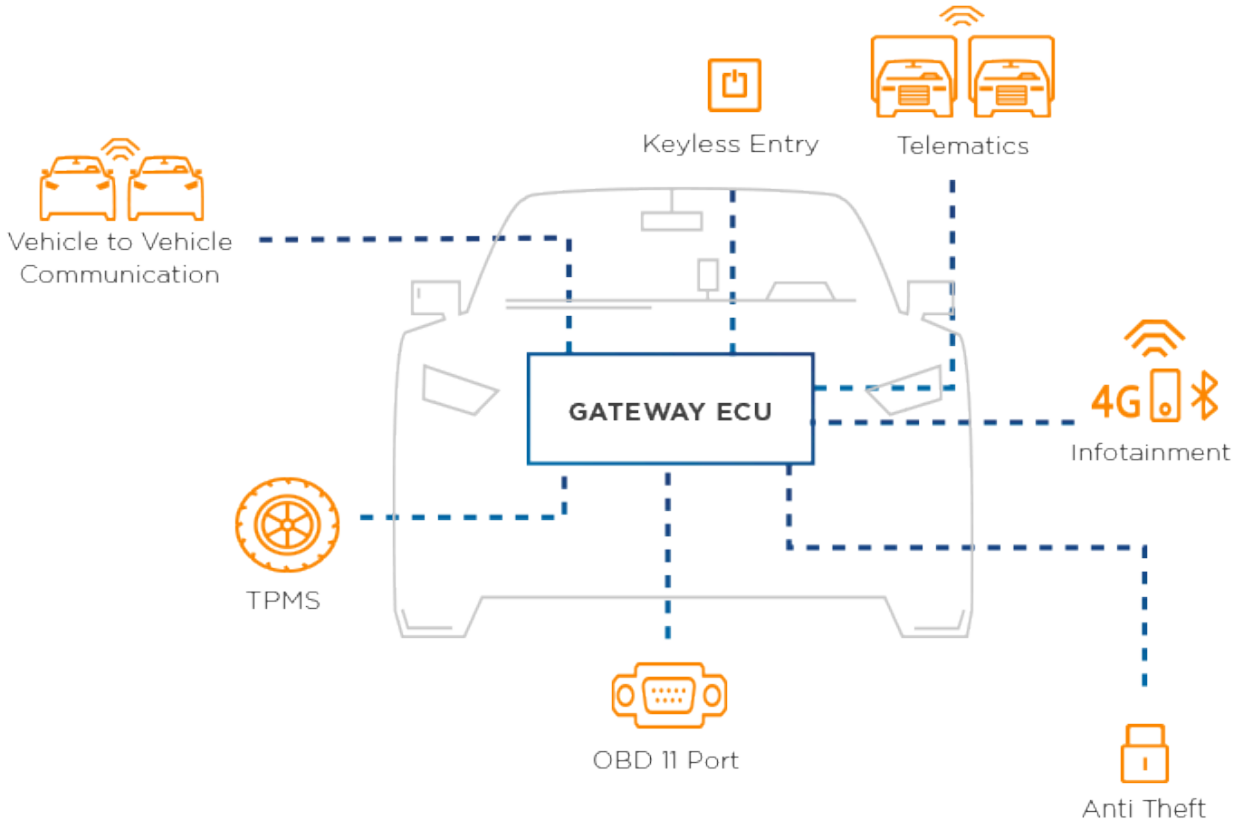
We at GuardKnox maintain that cybersecurity is the foundation of the connected car. Without the Communication LockdownTM approach and full network protection that can keep us and our cars safe at all times, further progress in vehicle connectivity, Advanced Driver Assistance Systems (ADAS) and autonomous vehicles (AVs) will not be practical.

## In-Vehicle and External Cybersecurity

Today's cars, trucks and buses host hundreds of sensors and Electronic Control Units (ECUs) powered by more than 100 million lines of software code. Cameras, LiDAR and other high-fidelity sensing devices stream gigabytes of data in real time. A typical vehicle might also host several different types of local area networks such as CAN bus, Ethernet, Local Interconnect Network (LIN), and Media Oriented Systems Transport (MOST). Since manufacturers' source hardware and software from many different suppliers, no single player controls, or is familiar with, all of the possible attack vectors within any vehicle. As such, vehicles constitute a massive attack surface even greater than fighter jets.

Connected cars are increasingly communicating with external systems. Vehicles communicate with the internet, satellites, road infrastructure, as well as other vehicles over numerous protocols such as WiFi, Bluetooth, Dedicated Short Range Communications (DSRC), and 4G Mobile. Each of these is beyond the control of the car manufacturer and can potentially be compromised. The security situation beyond the vehicle is no more optimistic than within.

## Vehicles must be protected from cyber attack both internally and externally



# IT Methods are Inadequate for Many Aspects of Automotive Cybersecurity

Many people in the automotive industry are looking to Information Technology (IT) for guidance on cybersecurity. IT has been dealing with hackers for more than two decades and has developed a number of best tools and practices for dealing with cyberattacks in the internet space. There are not many similarities between the two worlds of IT and automotives. We believe that the two worlds are so different that widely practiced IT methods are inadequate for protecting us in our connected vehicles. Here's why:

## Resilience

There is a certain resilience level in the IT network that doesn't exist in the world of intelligent transportation and if existed might cause a substantial risk. In the former, most cyber problems can be solved with a quick install, update or configuration change. In cases where data is lost or corrupted, it can be restored from a backup. Even in the worst-case scenario of total system failure, automatic failover to a disaster recovery site is available. This is not the case with connected vehicles. While an input error on an IT endpoint might result in the storage of an incorrect address or an error in payment amount, a simple mistake in a command in one of a vehicle's ECUs could cause a dangerous system failure. This can result in a collision or worse. In case of total system failure, a car can't "fail over" to another car. Passengers don't enjoy the luxury of a "do-over" when the brakes go out.

## Reaction

Traditional IT cybersecurity measures are reactive, often discovering and reporting on events that have already happened. The open-system world of the IT network admittedly cannot stop all attacks. As heuristic systems that learn as they work, IT cybersecurity solutions are in constant need of threat-intelligence updates. Always a step behind the latest hack attacks, they can achieve only, at best, a 98% reliability rate.

While this level is adequate in the IT context, it is unacceptable in closed-system moving-vehicle operation. You can tolerate the automatic identification and mitigation of 98% of cyberattacks on your data, but would you consent to driving a vehicle whose brakes work only 98% of the time?

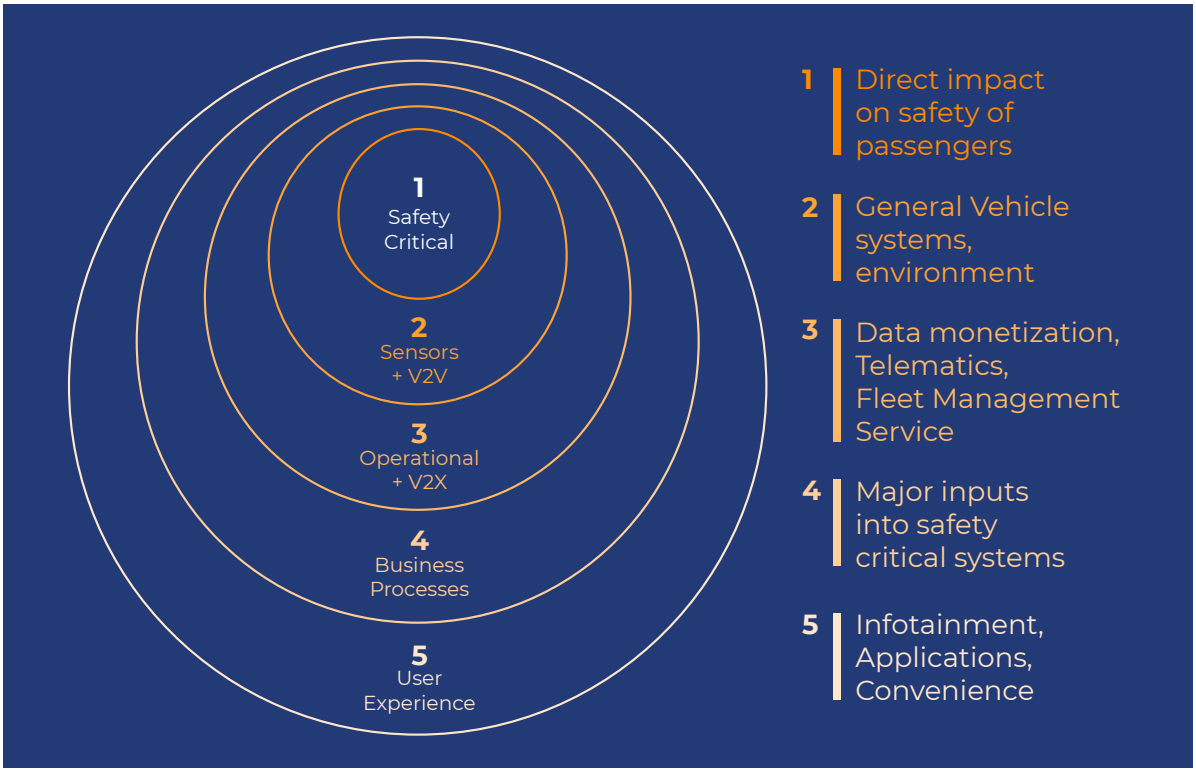
### False Positives

IT cybersecurity approaches typically generate multitudes of 'false positives'—conditions that are outside the understanding of the approach and are flagged as potential problems but, in reality, are not. False positives absolutely inundate IT cybersecurity systems and lead them security personnel on countless goose-chases that take up significant time and computer cycles. This is completely unacceptable for the security requirements of moving vehicles where false positives must be eliminated.

**IT cybersecurity approaches address issues that differ from the requirements of vehicles**

## Protecting the Systems in the Vehicle: Layered Approach

NHTSA (National Highway Traffic Safety Administration, a US government agency) promotes a multi-layered approach to cybersecurity that reduces the possibility of a vehicle cyberattack and mitigates the potential consequences of an intrusion. Taken from the worlds of aviation and defense systems, the most critical systems (safety) must be "air-gapped" (isolated) from the most exposed systems. For example, physical separation of the infotainment system from critical control systems such as braking and steering.




GuardKnox identifies 5 types of systems in the vehicle. Each type has identifiable characteristics and must be protected in accordance with its risk level.

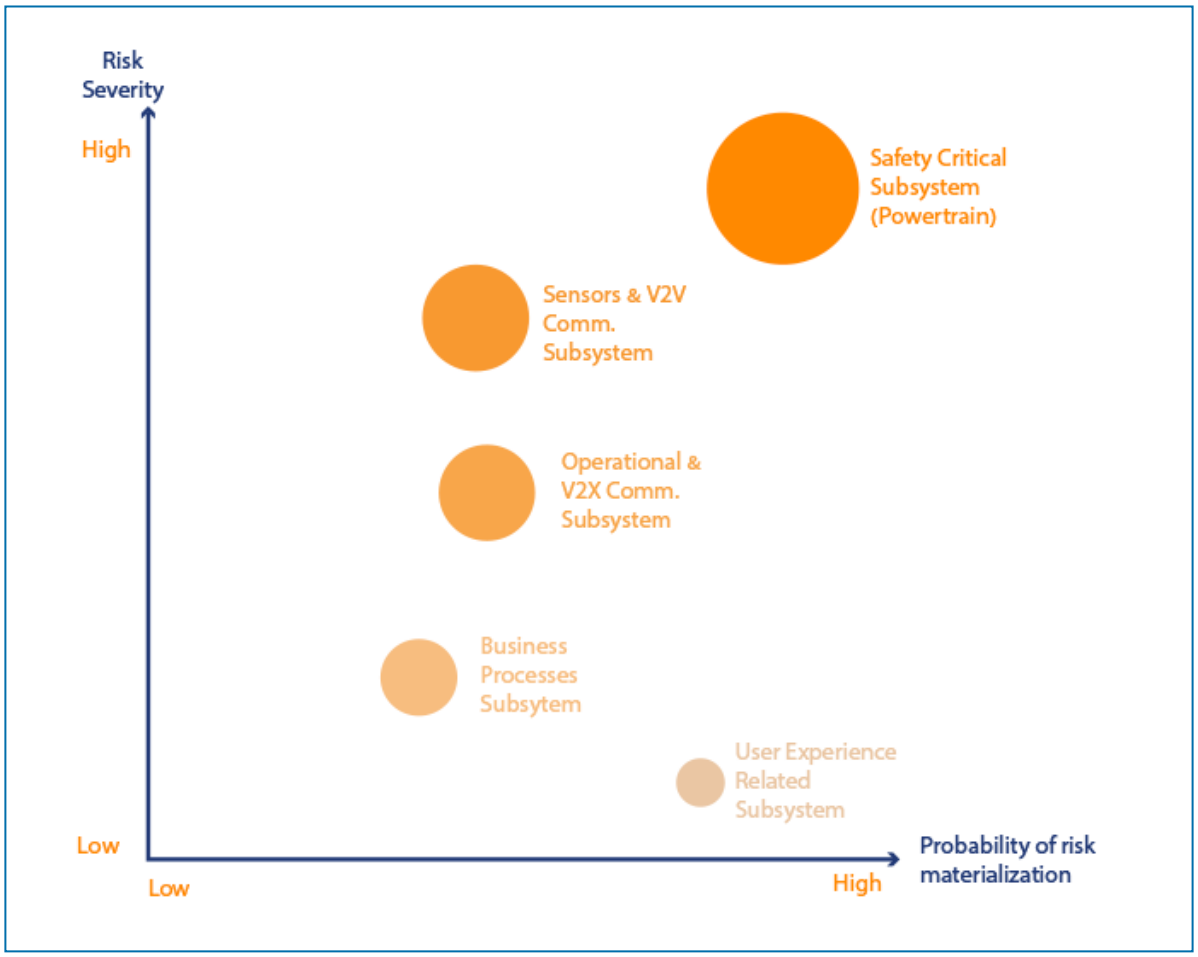
1. Safety critical subsystem (i.e. powertrain components) with direct impact on the safety of vehicle passengers and others
2. Sensors and V2V Communication provides major inputs to the safety critical subsystem
3. Operational and V2X Communication includes general and non-critical vehicle systems, safety subsystems and vehicle environment-control components
4. Business Processes include components related to data monetization as well as Telematics and Fleet Management System (FMS)
5. User experience (UE) includes infotainment, apps, and convenience components

Each system-type must be air-gapped with the most critical, Safety, isolated from the rest.

**Each system layer must have the cybersecurity approach that is appropriate to it: Safety is the most critical**

## Protecting the Most Critical Component: Safety

Non-safety-related systems, e.g., secure data storage and communications with the cloud, behave much like they do in the open-system IT world. They are subject to similar types of attacks and therefore respond to similar types of mitigation provided by IT solutions. As a result, to protect these systems, we can usually adopt and rely on IT best practices.



However, the most critical layer is within the vehicle itself—where we sit. Safety issues within the closed-system vehicle cannot tolerate after-the-fact remediation nor false positives. In fact, for these very reasons, no fighter jet today relies on the IT approach. In the closed systems of fighter jets and the safety-related areas of the connected car, the security level must operate at 99.99999% reliability. We cannot tolerate less.

Therefore, for safety-critical systems, we cannot rely on IT solutions. Instead, a vehicle-specific approach to cybersecurity is necessary: a deterministic methodology that ascertains that all ECUs within the car behave within acceptable parameters at all times; a methodology that does not embark on reactive attempts to identify and mitigate attacks, but is agnostic to attack; a solution that is not overwhelmed by false positives, but is, in fact, impervious to them.

**Safety-critical functions in the vehicle must be protected by a deterministic approach**

## Communication Lockdown™ Secures Safety-Critical Functions

The connected car is rapidly reshaping the automotive landscape, turning drivers into subscribers and presenting all sorts of exciting new revenue-generating and subscriber-satisfaction opportunities. But to take advantage of the vast potential just down the road, OEMs, Tier 1s and other players in the industry need to make a sharp turn in their approach to connected vehicle vulnerabilities and security.

Our physical safety, as well as the dependable performance of the vehicle that transports us, depend on reliable instructions between ECUs and sensors, across ECUs and over myriad data buses regardless of whether they originate within the vehicle or from external sources. GuardKnox's patented Communication Lockdown™ technology guarantees the security of data transmissions and guards the confidentiality and integrity of the growing accumulation of performance and personal data generated by the connected vehicle.

Unlike IT cybersecurity, Communication Lockdown™ is deterministic and attack-agnostic—well-suited to protect safety-critical functions in connected vehicles, providing these advantages:

- One central lockdown security device can manage the security for the entire vehicle
- A dedicated lockdown device can be easily installed for any segment or ECU for new and existing vehicles
- All ECU-to-ECU and ECU-to-HEU traffic are validated and authenticated
- Proper performance of the vehicle within its acceptable limits is enforced using a state machine
- Maintenance messages for the OEM usage and user data are protected within the vehicle and transmitted securely

Communication Lockdown™ provides the deterministic[1] approach that delivers proper cybersecurity for safety-critical functions

Communication Lockdown™ enables progress in vehicle connectivity, Advanced Driver Assistance Systems (ADAS) and autonomous vehicles (AVs)

[1] This methodology allows to maintain stringed protection without any updates as long as the OEM does not changes vehicle CANdb file, which is rarely done.