# SECURE & EFFICIENT OTA UPDATES OF THE ENTIRE VEHICLE

Richard Kinder, HARMAN Connected Services

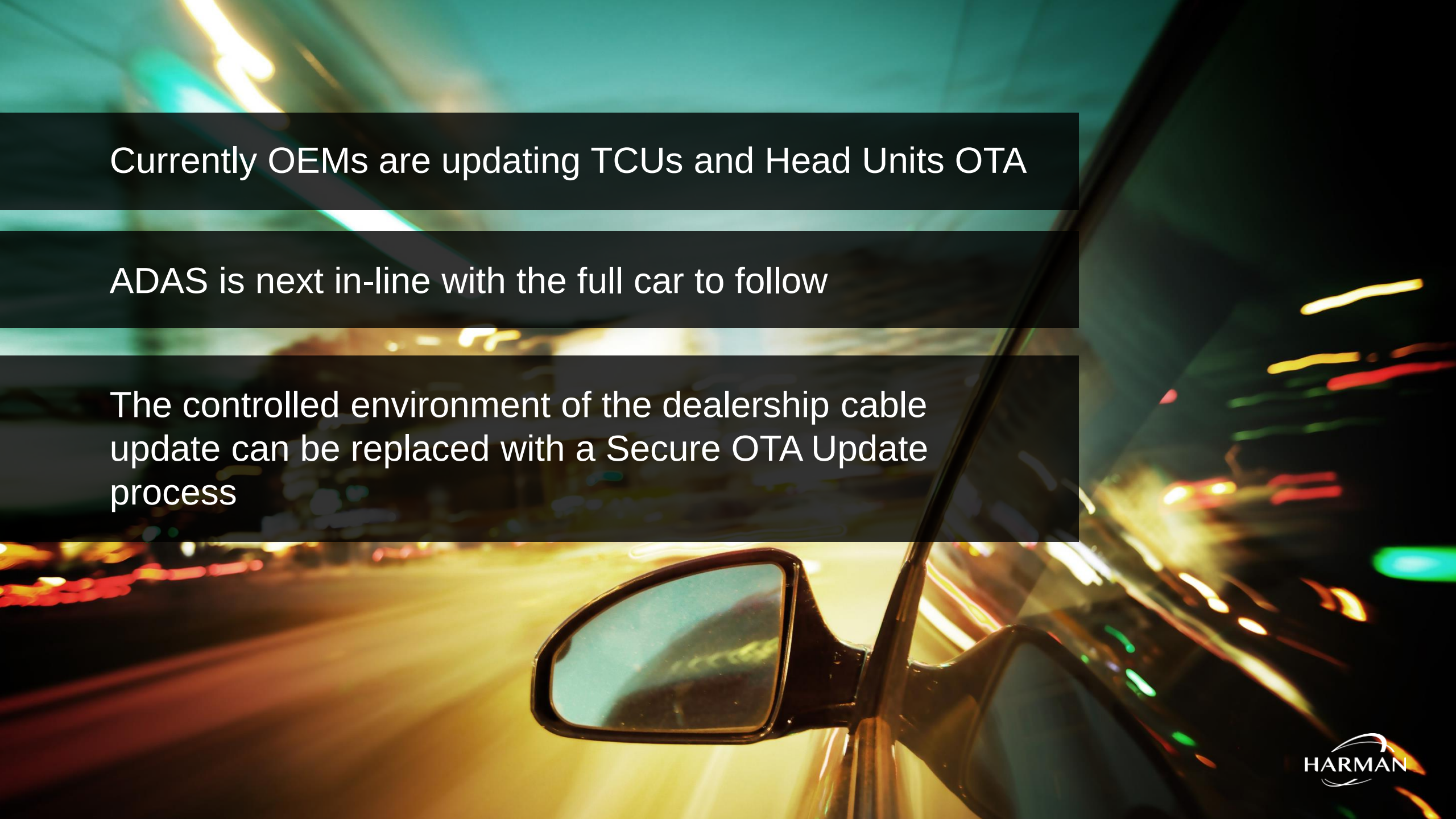
16th June 2016

HARMAN

# Agenda

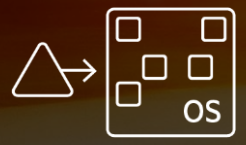
1. Market drivers
2. Introduction to OTA
3. Security goals for vehicle OTA
4. Complexity of the vehicle OTA
5. Secure OTA update of all ECUs

Car Connectivity
Software driving the automotive ecosystem evolution
Increased security and regulatory requirements
HARMAN


Currently OEMs are updating TCUs and Head Units OTA
ADAS is next in-line with the full car to follow
The controlled environment of the dealership cable update can be replaced with a Secure OTA Update process
HARMAN

# redbend

Installed on >15 million vehicles




>30 million successful updates

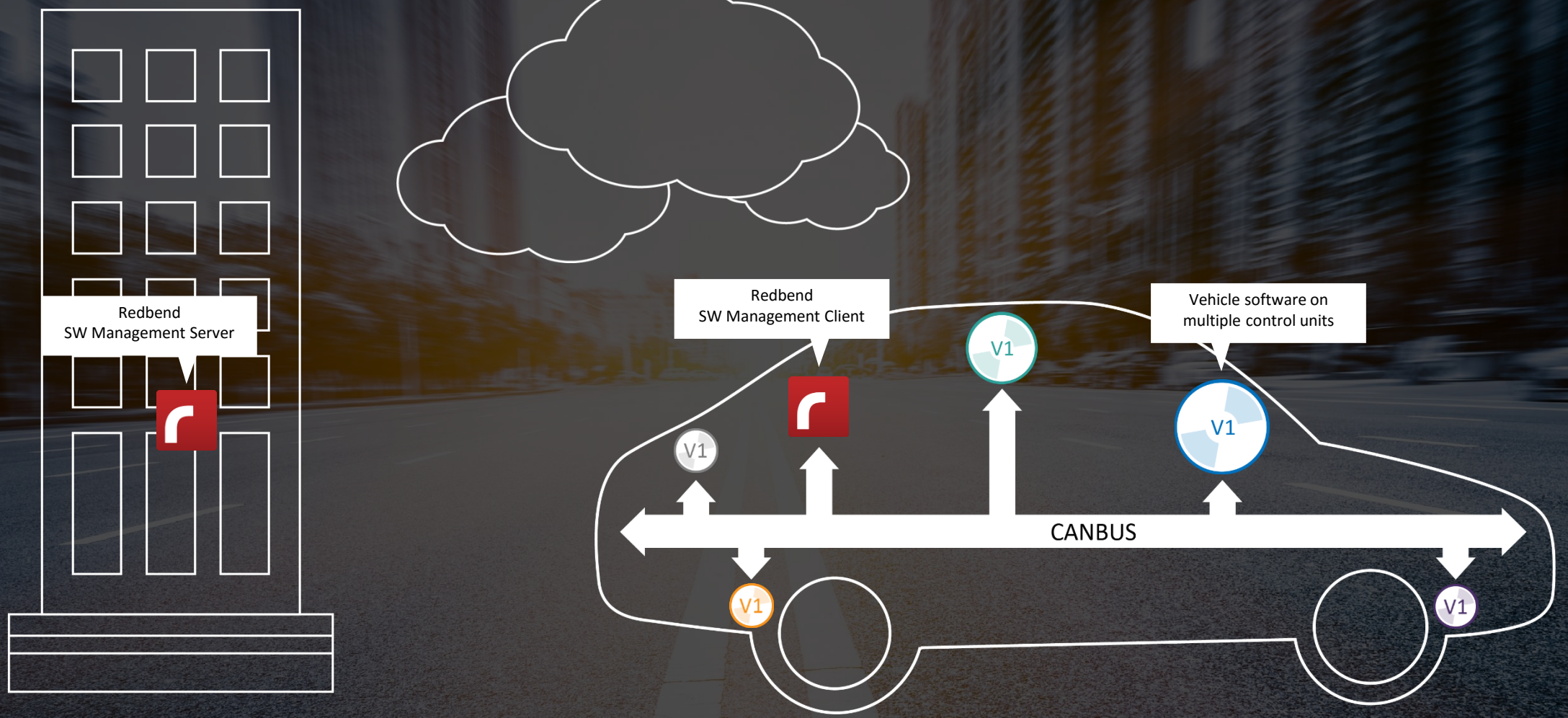
10 active automotive customers

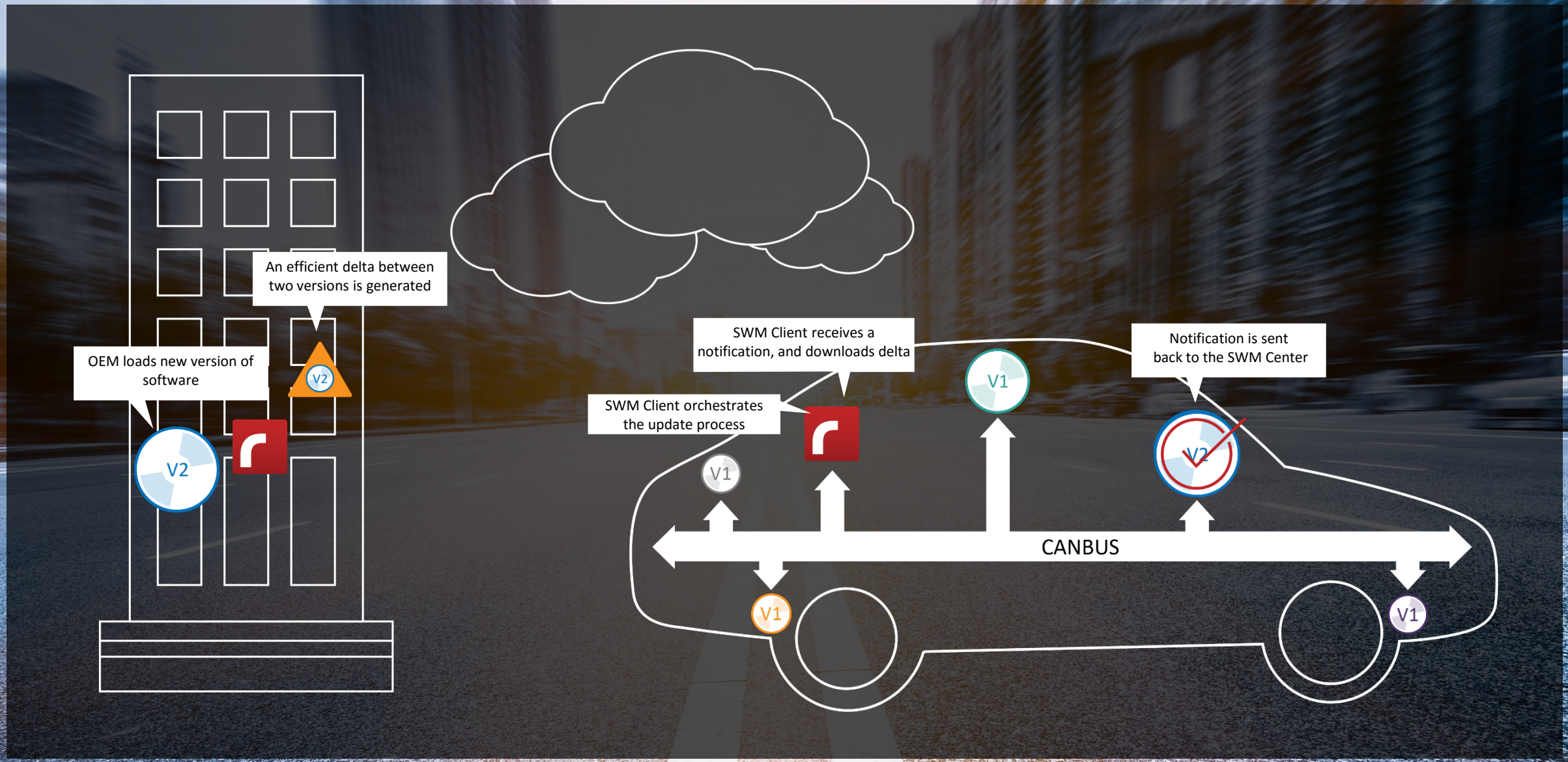
95% smaller updates; 100% update success rate

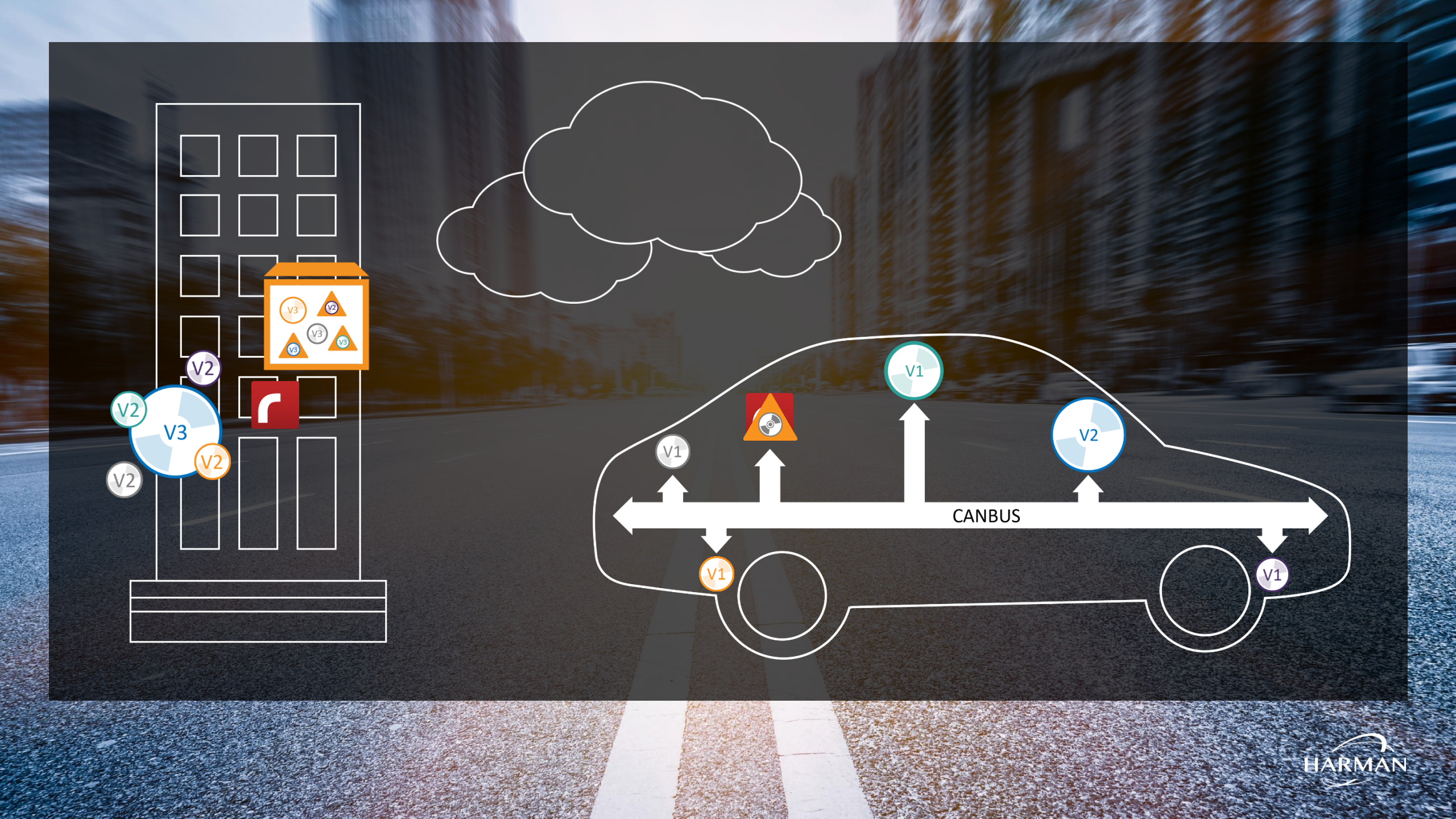
HARMAN

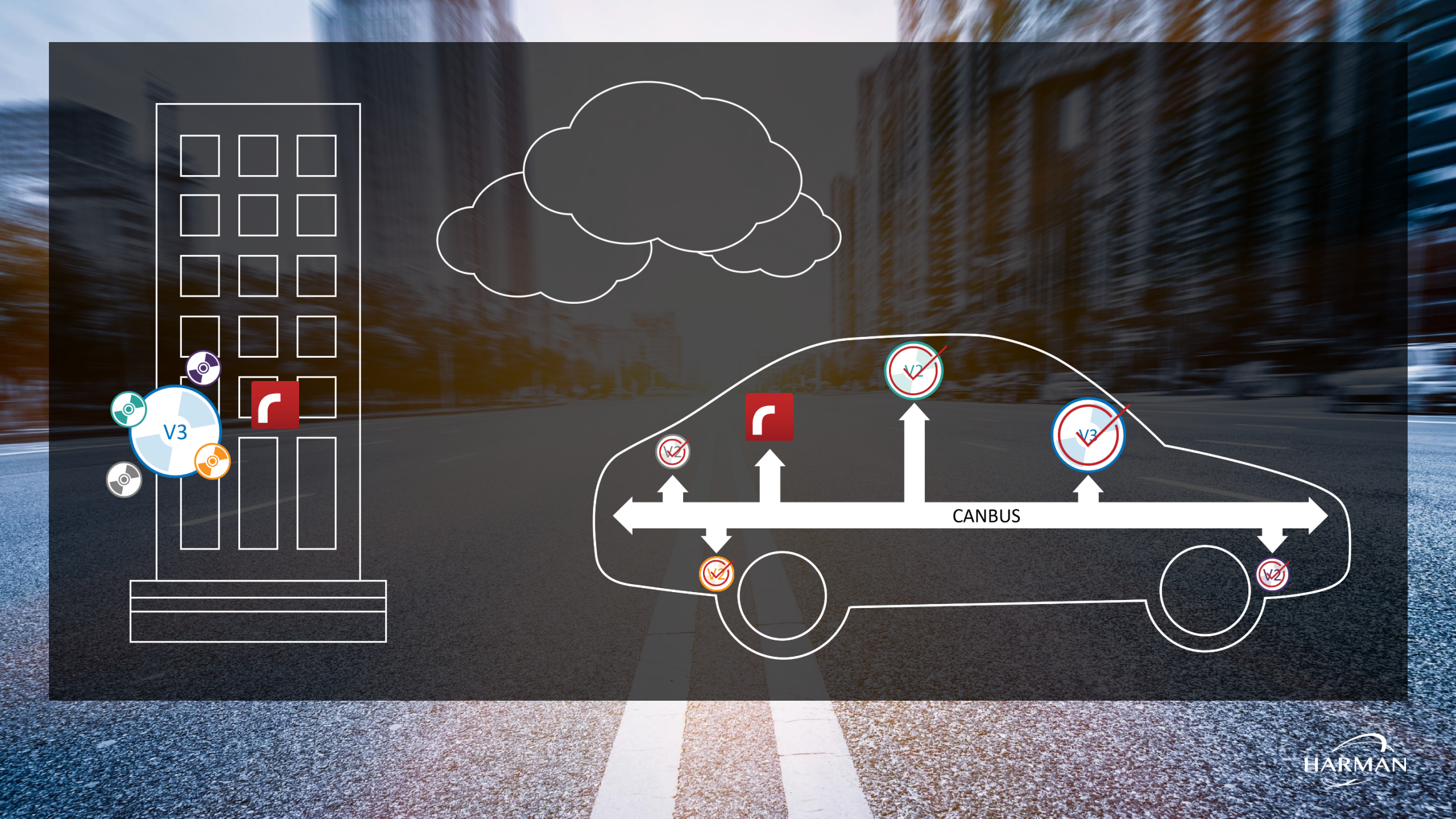
# Agenda

1. Market drivers
2. Introduction to OTA
3. Security goals for vehicle OTA
4. Complexity of the vehicle OTA
5. Secure OTA update of all ECUs


Redbend
SW Management Server
Redbend
SW Management Client
Vehicle software on
multiple control units
V1
V1
V1
V1
V1
CANBUS


An efficient delta between two versions is generated
OEM loads new version of software
V2
V2
SWM Client receives a notification, and downloads delta
SWM Client orchestrates the update process
V1
V1
Notification is sent back to the SWM Center
V2
CANBUS
V1
V1


V3
V2
V3
V3
V3
V2
V2
V3
V2
V2
V1
V1
V2
CANBUS
V1
V1


V3
V2
V3
CANBUS
V2
V2
V2

# Agenda

1. Market drivers
2. Introduction to OTA
3. Security goals for vehicle OTA
4. Complexity of the vehicle OTA
5. Secure OTA update of all ECUs

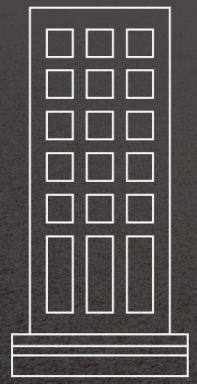
Admin Users

Unauthenticated user access

Unauthorized usage of system

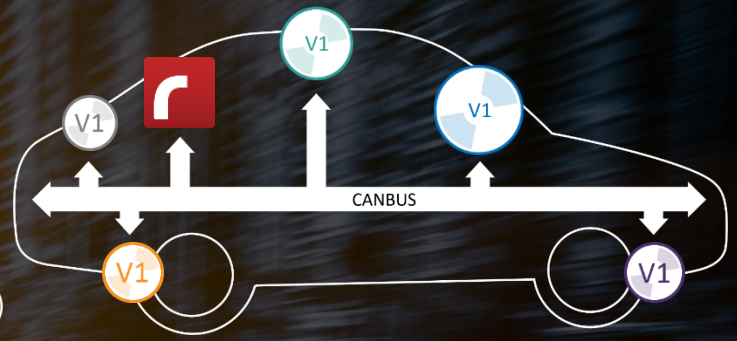
Hosted OTA Service

OEM Backend



Unauthorized access to OEM IP

Protection of OEM IP




Unauthorized SW installation

Unauthenticated SW installation

MITM

Spoofing

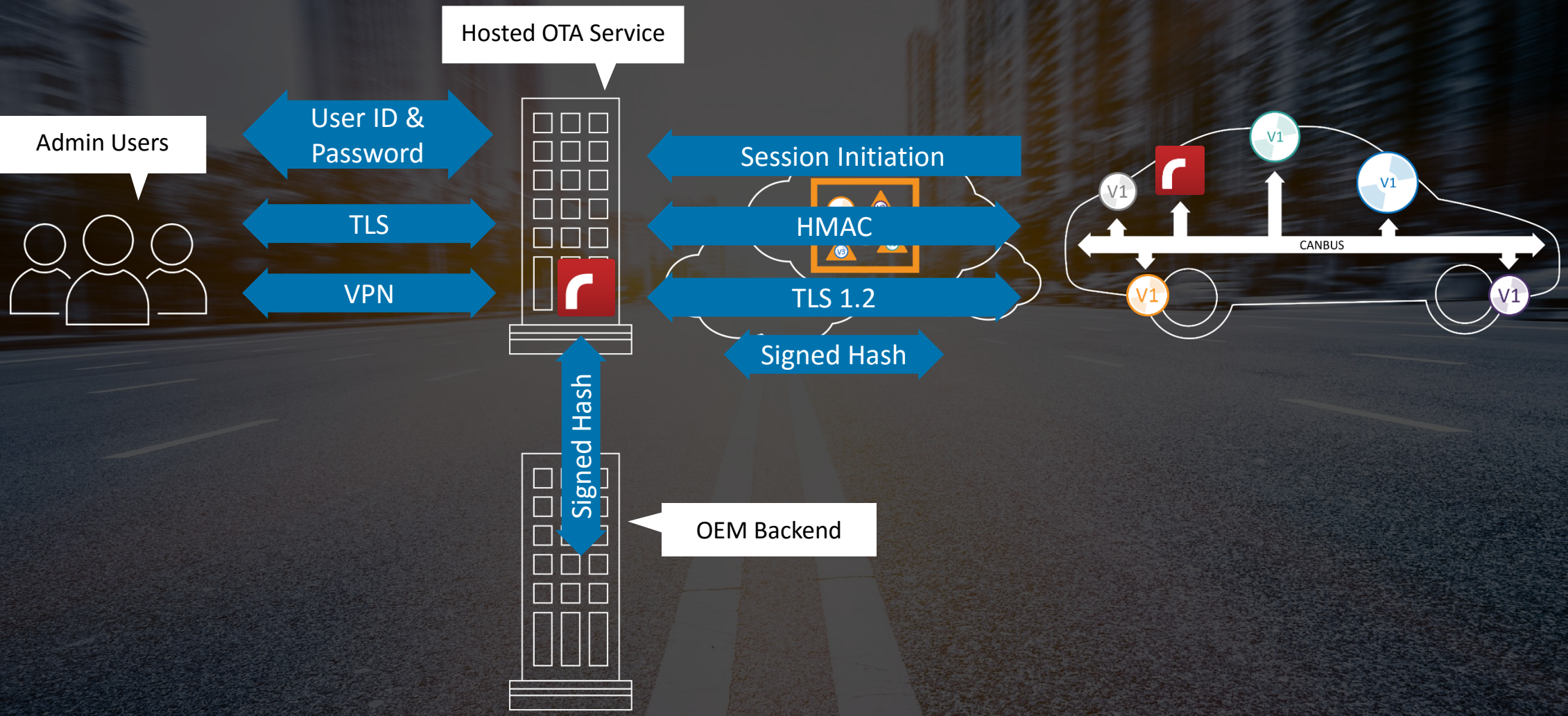
Snooping

Theft of secrets

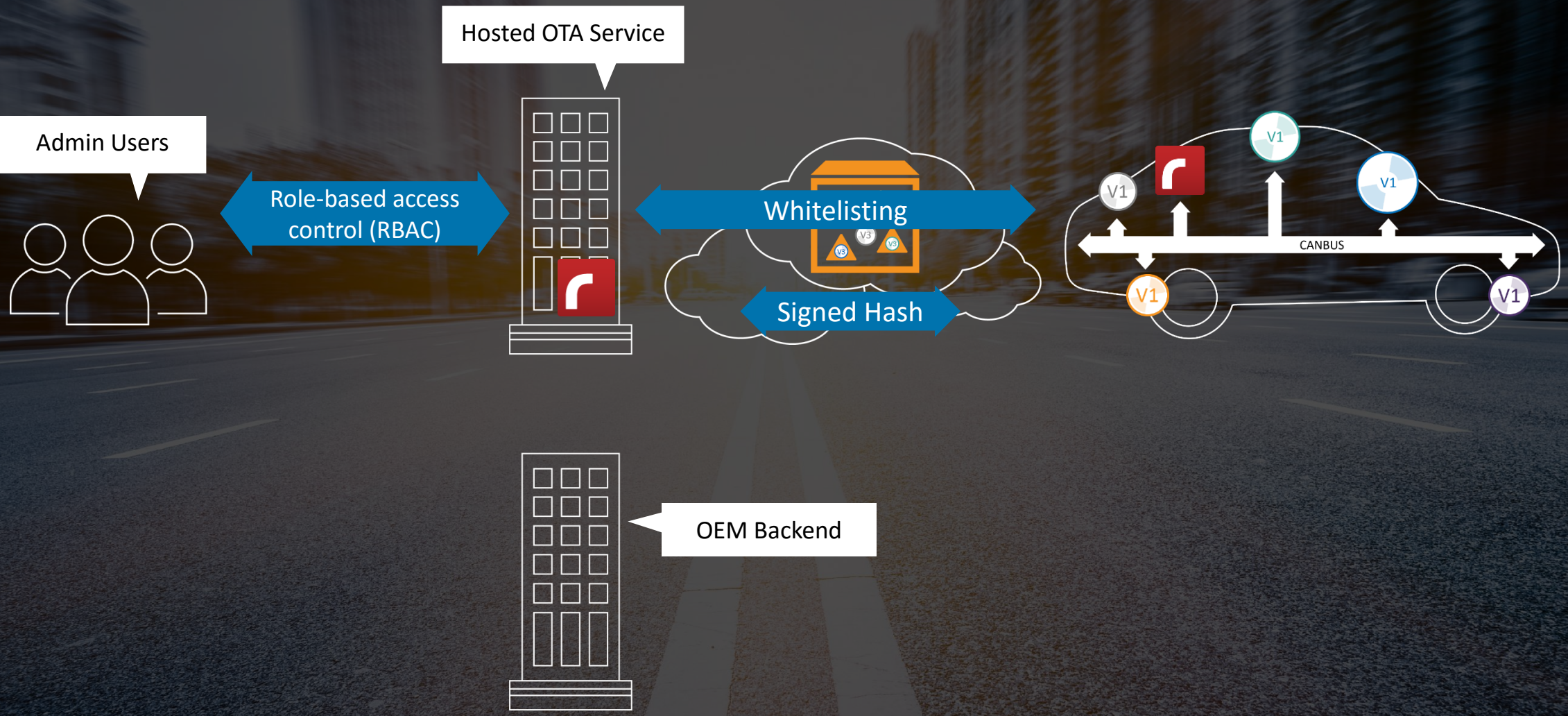
# TOP LEVEL SECURITY GOALS

| Authentication | Authorization | Confidentiality | Integrity |
| --- | --- | --- | --- |
| Trust establishment between relevant actors in the system | The requesting actor is authorised to use the requested resource | OEM proprietary data is not readily available to a malicious actor | Software updates cannot be tampered with or installed by a malicious actor |

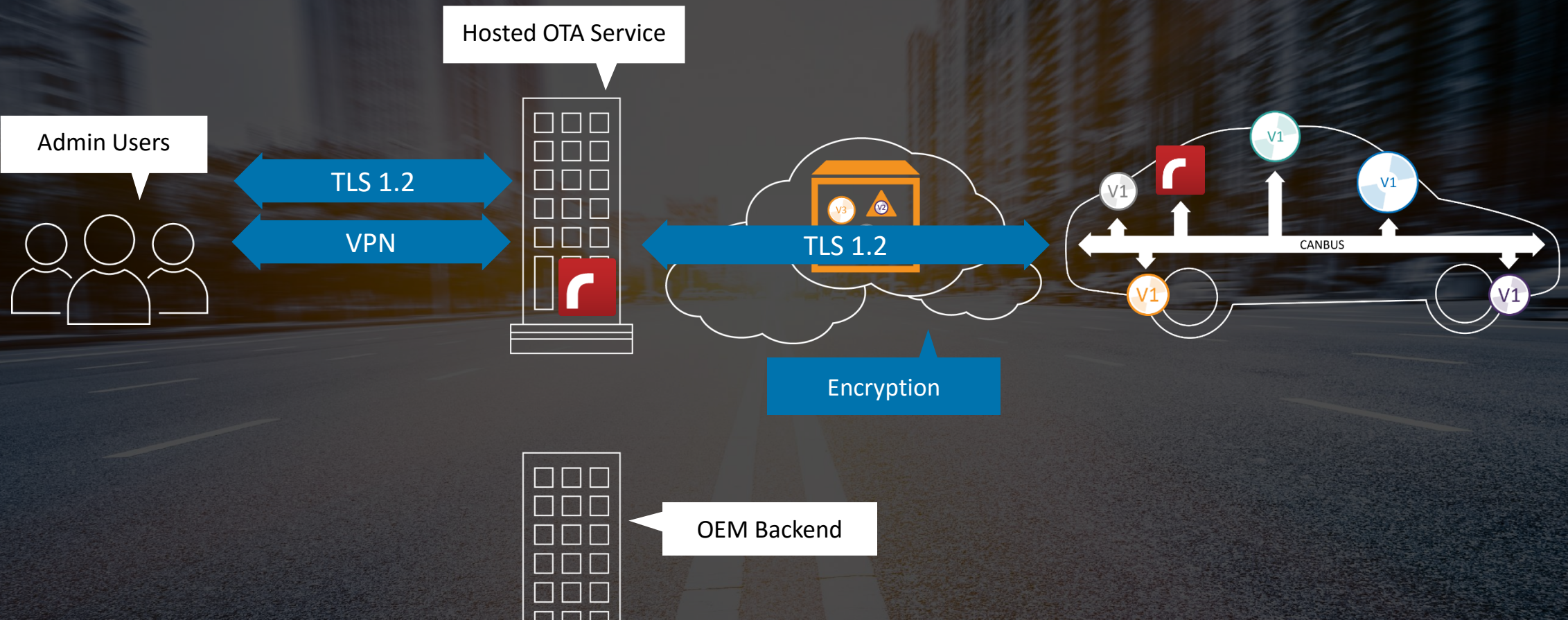
# AUTHENTICATION



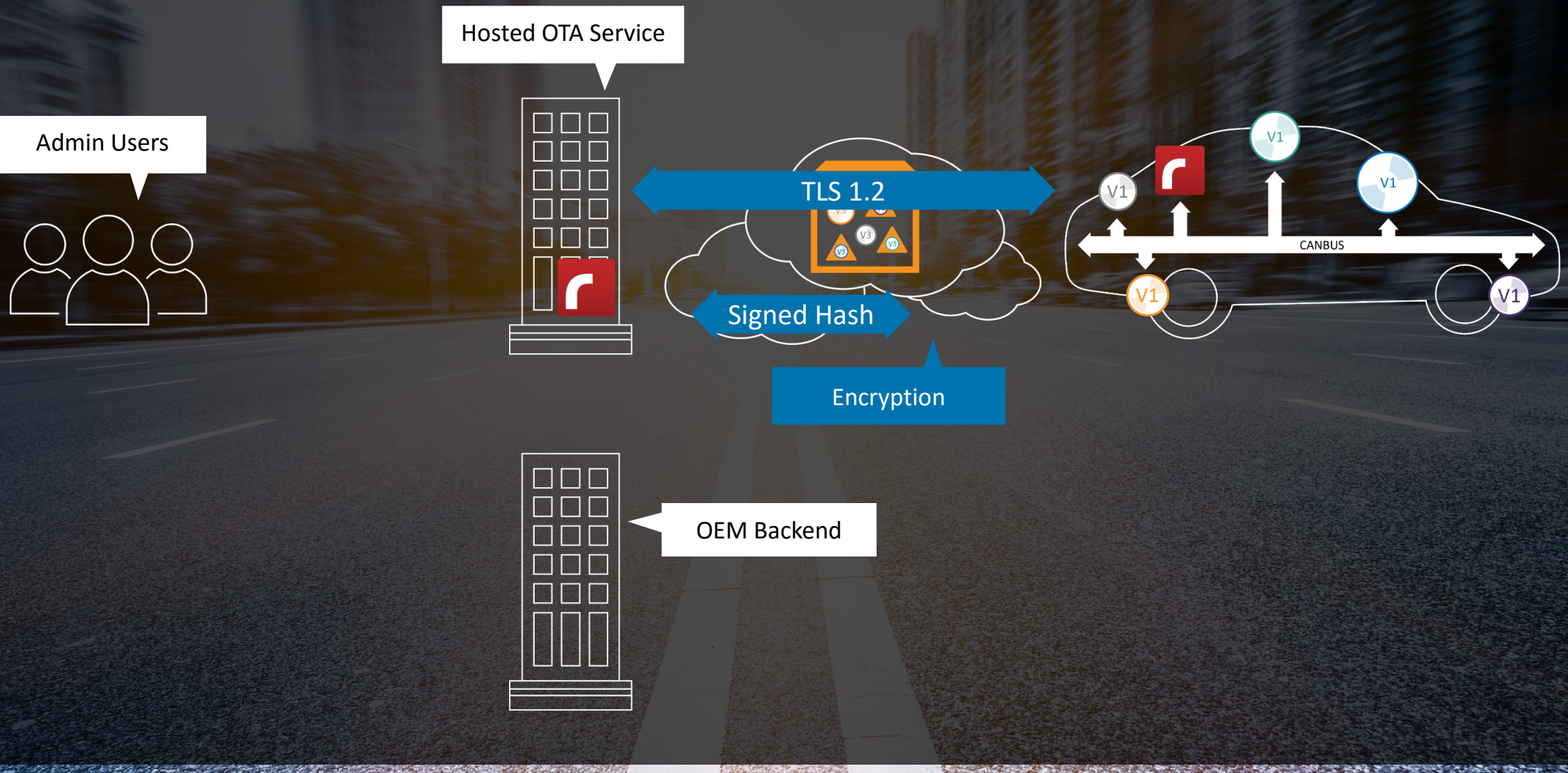
# AUTHORIZATION



# CONFIDENTIALITY



# INTEGRITY


Hosted OTA Service
Admin Users
TLS 1.2
Signed Hash
Encryption
OEM Backend
V1
V1
V1
V1
V1
CANBUS

# Agenda

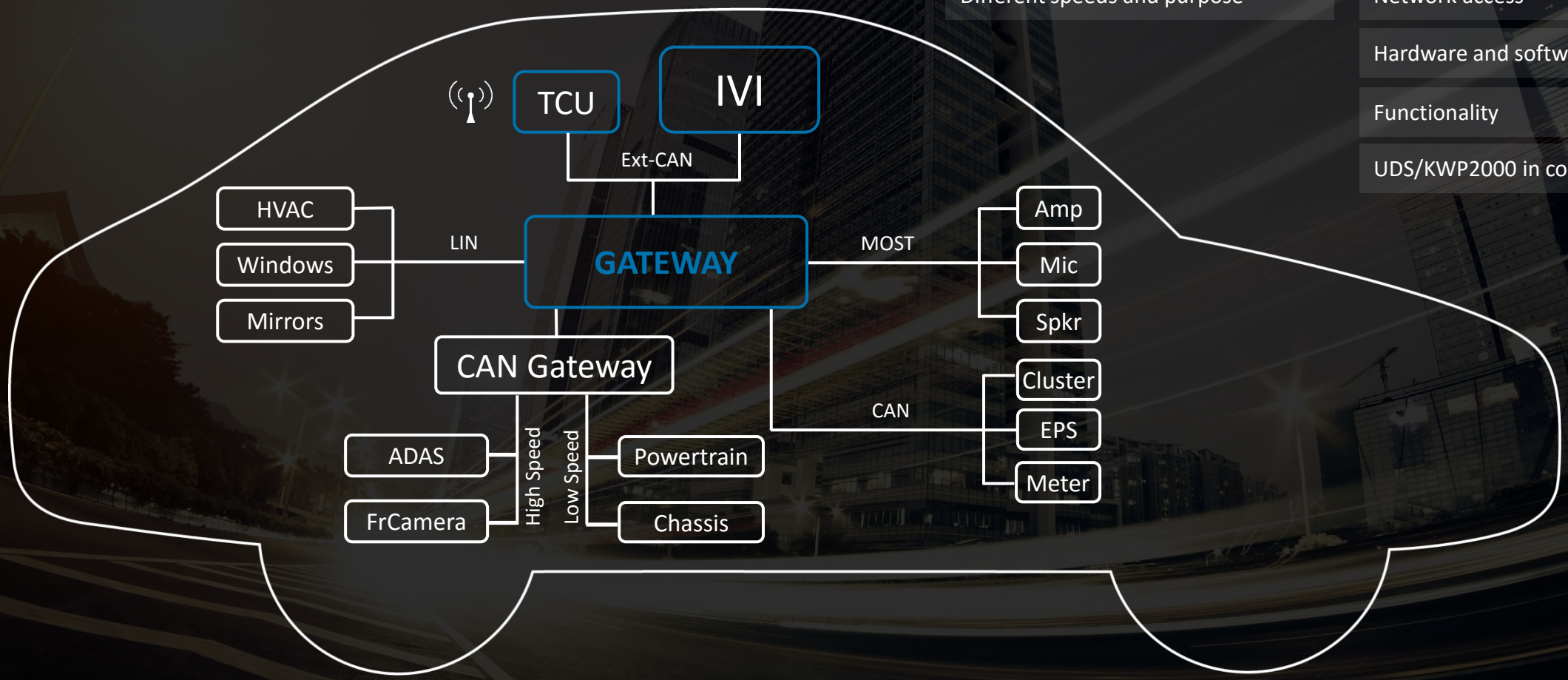
1. Market drivers
2. Introduction to OTA
3. Security goals for vehicle OTA
4. Complexity of the vehicle OTA
5. Secure OTA update of all ECUs

## Networks

- Complex network topology
- Different networks and sub-networks
- Different speeds and purpose

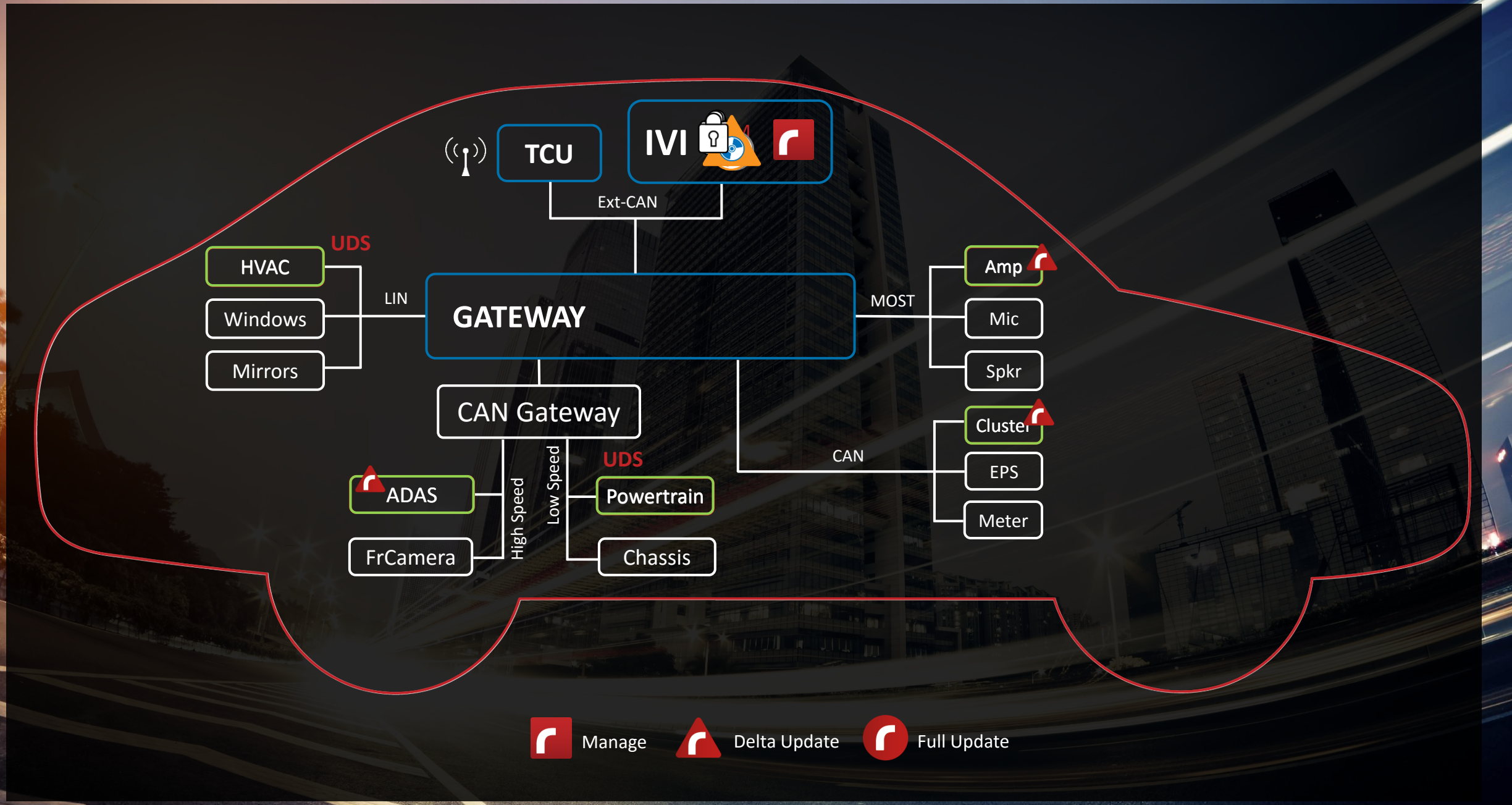
## ECUs

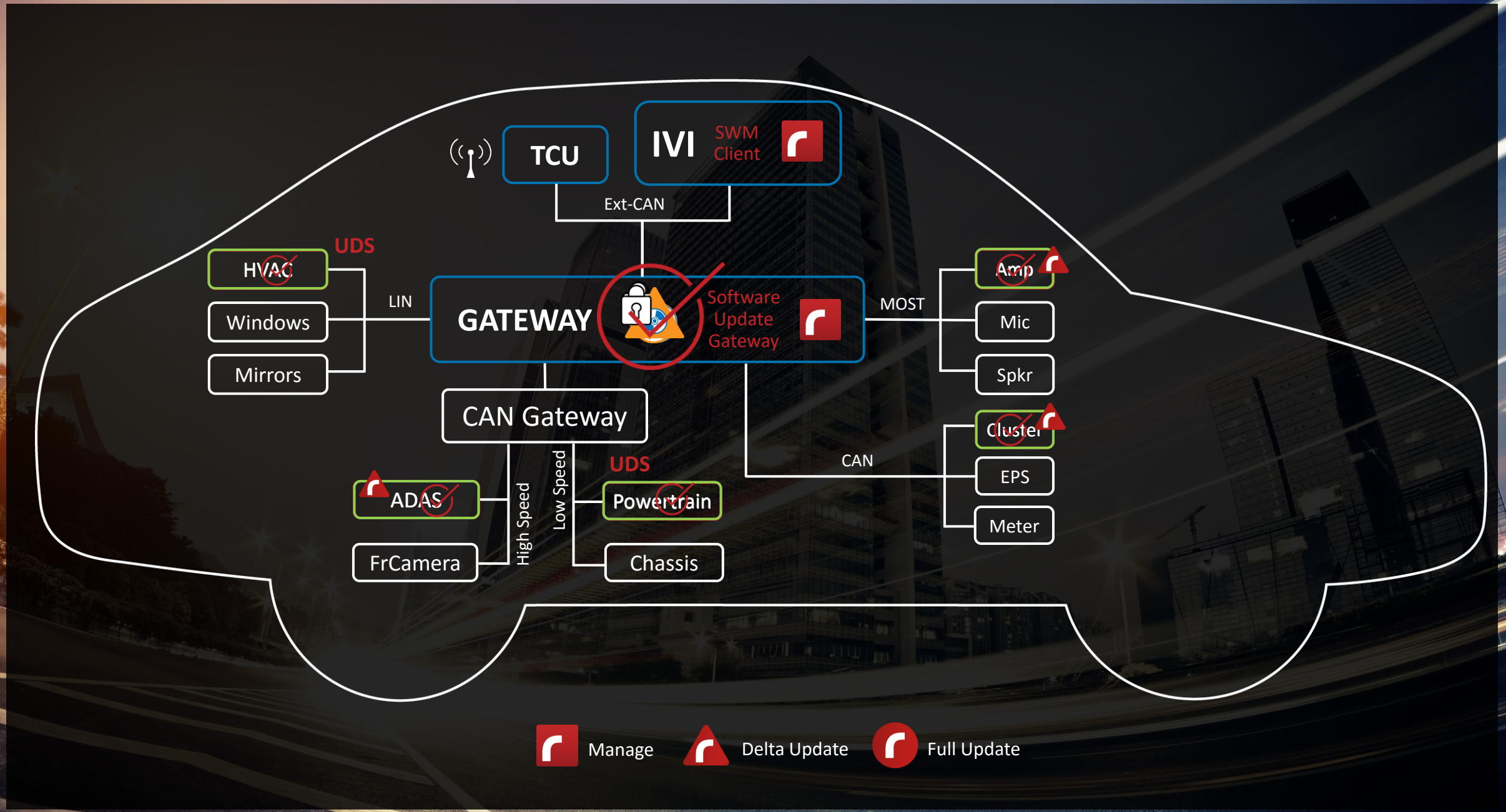
- RAM
- FLASH
- Network access
- Hardware and software architecture
- Functionality
- UDS/KWP2000 in common



# Agenda

1. Market drivers
2. Introduction to OTA
3. Security goals for vehicle OTA
4. Complexity of the vehicle OTA
5. Secure OTA update of all ECUs


TCU
IVI
Ext-CAN
UDS
HVAC
Windows
Mirrors
LIN
GATEWAY
MOST
Amp
Mic
Spkr
CAN Gateway
Cluster
EPS
Meter
CAN
UDS
ADAS
FrCamera
High Speed
Low Speed
Powertrain
Chassis
Manage
Delta Update
Full Update


TCU
IVI
SWM Client
Ext-CAN
UDS
HVAC
Windows
Mirrors
LIN
GATEWAY
Software Update Gateway
MOST
Amp
Mic
Spkr
CAN Gateway
Cluster
EPS
Meter
CAN
UDS
ADAS
FrCamera
High Speed
Low Speed
Powertrain
Chassis
Manage
Delta Update
Full Update

In summary, secure and efficient update of the entire car requires:

1. Comprehensive client-server architecture
2. Secure “In car entire update”
3. Cyber-secure analysis and system design
4. Strong capabilities in gateway controller MCUs

HARMAN

HARMAN Redbend's trusted expertise in OTA Software Management and Virtualization is used by the world's leading manufacturers and service providers to manage over 2 Billion connected devices.

richard.kinder@harman.com

Richard Kinder


HARMAN