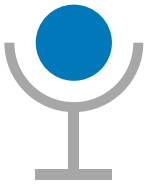
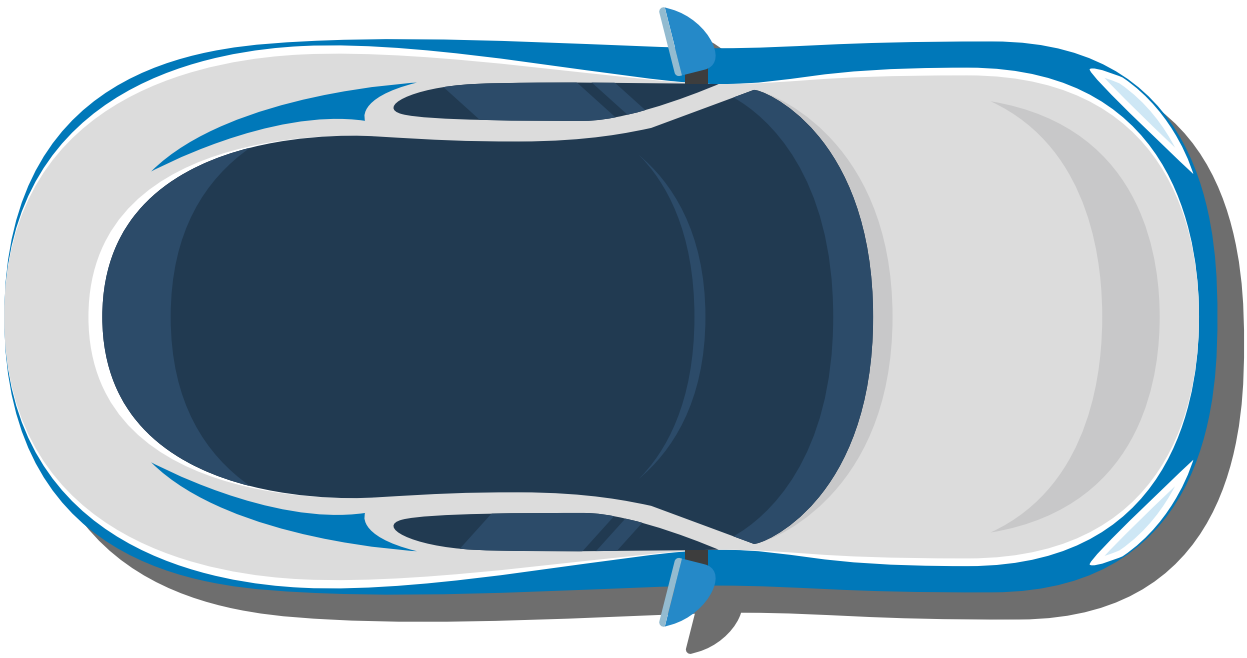
V-to-X-Sicherheit
Kombination von mehreren Mechanismen





AUTOR

Onn Haran
ist Gründer und CTO von Autotalks in Kfar Netter (Israel).

Um die Vision der Vehicle-to-X-Technik zu realisieren, müssen Fahrzeuge in der Lage sein, den empfangenen Nachrichten zu vertrauen. Die Bedrohungsszenarien und Arten der Bedrohung steigen. Es gilt, aktuelle Verteidigungsstrategien anzupassen und neue zu entwickeln, um die Herausforderung zu meistern. Vorschläge und Lösungen kommen von Autotalks.

START-UP AUF DEM WEG IN DIE SERIENFERTIGUNG

Autotalks beschäftigt sich seit über zehn Jahren mit Vehicle-to-X(V-to-X)- Kommunikation – überzeugt von der Idee, eine große Anzahl verschiedenster Unfälle im Straßenverkehr zu vermeiden. Das israelische Unternehmen zählt nach Aussagen unabhängiger internationaler Experten zu den am schnellsten wachsenden Start-Ups im Themenfeld V-to-X weltweit, mit der Entwicklung und Fertigung von dafür notwendigen automobilspezifischen Chipsätzen.

Im Jahr 2016 stellte Autotalks die 2. Generation seines Chipsatzes vor. Er erfüllt die strengsten Anforderungen an die Fahrzeugsicherheit, mit mehreren Verteidigungsschichten. Die Ebenen beinhalten einen sicheren Boot, geringe Latenzzeiten, eine Zeilenratenüberprüfung der gesamten V-to-X-Kommunikationsverbindung und eine V-to-X-Firewall, die die Kommunikation absichert. Die kryptografisch-agile Sicherheits-Engine unterstützt Upgrades mit weiterentwickelten Algorithmen und ist somit für Jahrzehnte zukunftsfähig. Darüber hinaus ist der Chipsatz für das autonome Fahren konzipiert und unterstützt den Standard WIFI, IEEE 802.11a/b/g /ac, der den Einsatz von ergänzenden Mehrwertdiensten ermöglicht.

Autotalks erhielt mehrere Design-Auszeichnungen. Das Unternehmen wurde von dem Automobilzulieferer Denso, einem V-to-X-ECU-Pionier, als Lieferant für die Großserienproduktion ausgewählt. 2019 ist mit ersten Serienfahrzeuge mit einem V-to-X-Gerät von Autotalks zu rechnen.

V-TO-X-KOMMUNIKATION

V-to-X-Kommunikation vernetzt Fahrzeuge (V-to-V), Infrastruktur (V-to-I) und Fußgängern (V-to-P). Sie sammelt die Informationen und sendet Warnungen bei bevorstehenden Gefahren. V-to-X-Kommunikation hilft so den Fahrern, Autounfälle zu verhindern, insbesondere in Situationen mit eingeschränkter Sicht, beispielsweise durch andere Verkehrsteilnehmer, bei schlechter Wetterlage oder ungünstigen Lichtverhältnissen.

Dank der V-to-X-Kommunikation werden weitere Verbesserungen ermöglicht: Zum einen hilft sie bei der Optimierung der Verkehrskoordination und erhöht damit die Straßenauslastung, zum anderen ist es möglich mit ihrem Einsatz die Emissionen und damit verbundene Kosten zu verringern.

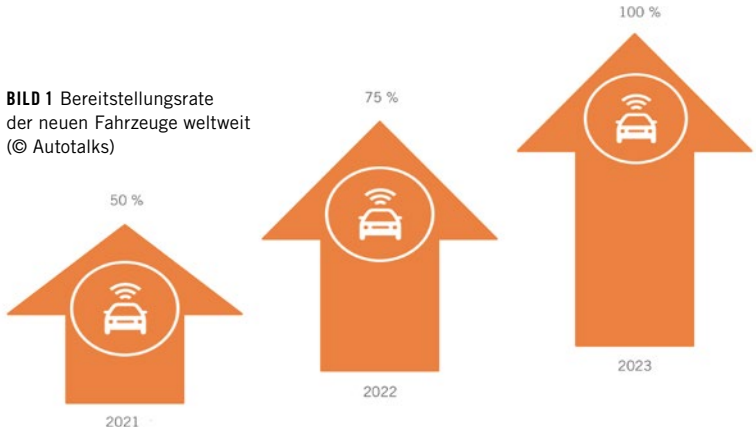


BILD 1 Bereitstellungsrate der neuen Fahrzeuge weltweit (© Autotalks)

Im Dezember 2016 veröffentlichte die US NHTSA (National Highway Traffic Safety Administration) ein NPRM (Notice of Proposed Rulemaking), dass die DSRC (Dedicated Short Range Communication)-basierte V-to-V-Kommunikation in allen Neuwagen von 50 % im Jahr 2021 auf 75 % im Jahr 2022 ansteigen soll/wird. Die NHTSA rechnet damit, dass mithilfe von V-to-X-Kommunikation bis zu 80 % der Unfälle vermeidbar sind, **BILD 1**.

SAFETY: ALLGEMEINE ASPEKTE

NPRM hat allgemeine Anforderungen an die DSRC-Kommunikationsgeräte auf V-to-V-Basis aufgestellt, dabei ist die Sicherheit besonders wichtig. Das wachsende Risiko von Cyber-Attacken hat das USDOT dazu bewegt, die Sicherheitsanforderungen zu steigern. Die Anforderungen sehen eine mehrschichtige, holistische Herangehensweise mit Hardware Security Module (HSM) und Manipulationserkennung vor, die zur Speicherung sensitiver Daten angefordert wurden.

V-to-X-Spezifikationen und Einsatzrichtlinien wurden im Hinblick auf die spezifischen Herausforderungen von V-to-X entwickelt. Die Algorithmen der Elliptischen-Kurven-Kryptographie (ECC) wurde von den Standardisierungsgremien aufgrund der kleinen Größe der Signaturen und Schlüssel ausgewählt.

Die Signaturen werden mit dem Elliptische-Kurve-Digitalsignatur-Algorithmus (ECDSA) und 256-Bits-Keys berechnet. Die Standard-ECC-Kurven basieren auf NIST, in Deutschland werden sogenannte Brainpool-Kurven hinzugefügt, um den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu entsprechen. Die Brainpool-Kurven sollten 256- und 384-Bit Keys unterstützen.

Jedes Fahrzeug hat viele privat-öffentliche Schlüsselpaare, die häufig zum Schutz der Privatsphäre des Fahrzeugs geändert wurden. Jeder öffentliche Schlüssel wird in einem Zertifikat verteilt. Die Zertifikate werden von einer Zertifizierungsstelle (CA) unterzeichnet. Die gleichen kryptografischen Lösungen können in den USA und Europa mit nur geringen Unterschieden angewendet werden. Jedes Fahrzeug verfügt über zahlreiche öffentlich-private Keys, die häufig wechseln und so die Privatsphäre der Autofahrer schützen. Jeder öffentliche Schlüssel wird mit einem Zertifikat verkauft. Die Zertifikate sind durch eine Zertifizierungsstelle signiert. In USA und Europa können dieselben kryptografischen Lösungen mit wenigen Abwandlungen verwendet werden.

Autotalks setzt entsprechend der Empfehlungen von NPRM auf mehrschichtige Sicherheit, um mehrfache Gefahren besser abzuwehren, **BILD 2**. Das Sicherheitsschema kann analog zu einem Schloss aufgebaut sein. Ein einfacher Sicherheitsmechanismus ist nicht ausreichend. Eine Firewall ist notwendig, um das System abzusichern, da ein System nur so stark ist, wie sein schwächstes Bestandteil. Zum Beispiel kann der V-to-X-Sicherheitsspeicher einen perfekten Schutz bieten, aber ein System wäre gehackt, wenn Malware das HSM zum Signieren einer gefälschten Nachricht steuern kann. Der Zugriff auf kritische Systemressourcen

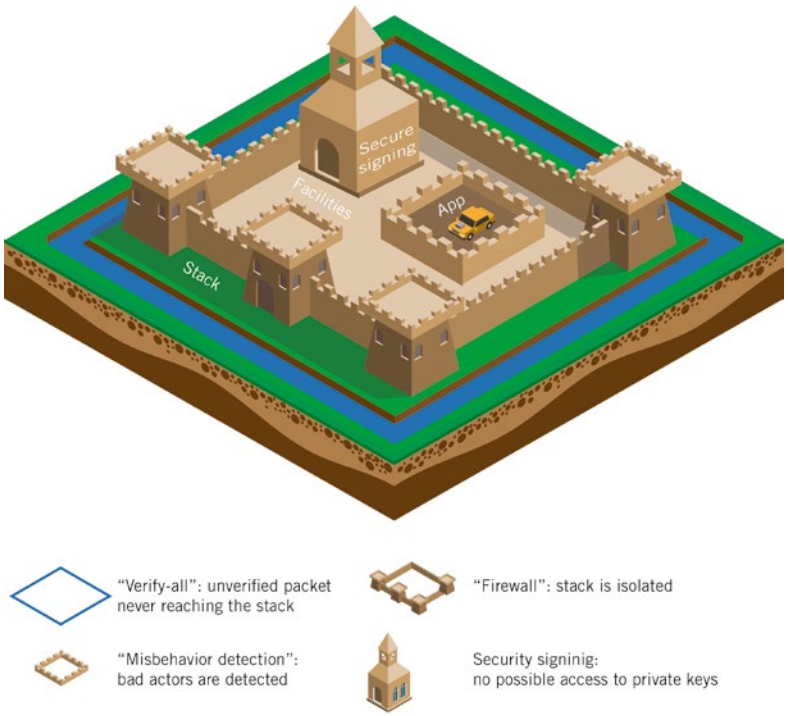


BILD 2 Autotalks setzt den Empfehlungen von NPRM folgend auf mehrschichtige Sicherheit, um mehrfache Gefahren besser abzuwehren; das Sicherheitsschema kann analog zu einem Schloss aufgebaut sein; ein einfacher Sicherheitsmechanismus ist nicht ausreichend (© Autotalks)

wie Konnektivität und HSM wird durch die Firewall überwacht, um Mißbrauch zu vermeiden. Datenverkehr wird vorautorisiert. Potenzielle Malware wird blockiert und kann die CPU-Ausführung nicht übernehmen. Kurz gesagt, die Firewall stellt sicher, dass die V-to-X-Anwendungen nur vertrauenswürdige Nachrichten erhalten.

SICHERHEIT – LÖSUNGEN

BILD 3 zeigt die Firewall eines Verifying-All-Messages-Systems („Verify-All“, links) und ein System mit einer begrenzteren Verifizierungskapazität, bei dem die Pakete zur Verifizierung ausgewählt werden („Verify-on-Demand“ rechts).

Verify-All ermöglicht eine deterministische Firewall. Der Datenfluss ist definiert und kann deshalb streng befolgt werden, damit können die Schwachstellen der Software nicht ausgenutzt werden. Die Angriffsfläche für eine Attacke ist minimal. Die Leistung von Verify-on-Demand ist begrenzt und zwingt den Einrichtungslayer zum Empfang von unsicheren Daten zum Parsing. Die Verifizierung wird basierend auf einem Auswahlalgoritmus durchgeführt. Der Einrichtungslayer und der RX-Pfad sind unsicher. Die Angriffsfläche für eine Attacke ist nicht quantifizierbar. Der freiliegende Einrichtungslayer kann den TX-Pfad und die Apps angreifen. Der Datenfluss ist nicht deterministisch und deshalb ist nur eine begrenzte Durchsetzung möglich.

Ein weiterer Vorteil der Verifizierung aller übermittelten Informationen ist das deterministische Vorgehen und eine kurze Verifizierungslatenz. Das Modul ist stets zur Datenverarbeitung bereit. Verify-on-Demand nutzt nur ein limitiertes Modul. Standardmäßig ist bei der Bündelung der Pakete eine Warteschlange notwendig. Die Latenz ist unbegrenzt. V-to-V hat sicherheitsrelevante Entscheidungen in Echtzeit zum Ziel, eine unbegrenzte Latenz würde den Zweck nicht erfüllen.

Die maximale Menge der Pakete pro Sekunde wird zur quantitativen Definition der „Verify-All“ berechnet. Die Paketlänge wird mit der Gleichung 1 berechnet:

GI. 1
$$T_{premable} + T_{PHY\ header} + T_{symbol\ length} \cdot \text{ceil}\left(\frac{(16+6+8\cdot<\text{data length}>)}{\text{NDBPS}}\right)$$

Aufeinander folgende Pakete werden durch mindestens DIFS (58µS) getrennt. Vorausgesetzt mit 250-Bytes-Daten kann das ECDSA-Modul zwei Pakete empfangen, Gl. 2:

GI. 2
$$32u + 64u + 8u \cdot \text{ceil}\left(\frac{(16+6+8\cdot250)}{48}\right) + 58u = 498uSx$$

Deshalb erfordert „Verify-All“ die Bearbeitung von >2000 Verifizierungen pro

ATZ live

Automotive Acoustics Conference

4th International ATZ Conference Vehicle Acoustics

11 and 12 July 2017
Zurich/Ruschlikon | Switzerland

LIGHTWEIGHT STRUCTURES AND NVH
Design & Material Technologies

NVH OF HEVs & BEVs
Challenges and E-Sources Characterization

VEHICLE EXTERIOR NOISE
Legislation, NVH Solutions, Tools and Diagnostic Methods

/// SCIENTIFIC DIRECTOR
Dr. Davide Caprioli
Autoneum

/// KINDLY SUPPORTED BY

autoneum

ATZ live
Abraham-Lincoln-Straße 46
65189 Wiesbaden | Germany

Phone +49 611 7878-131
Fax +49 611 7878-452
ATZlive@springer.com

PROGRAM AND REGISTRATION
www.ATZlive.com

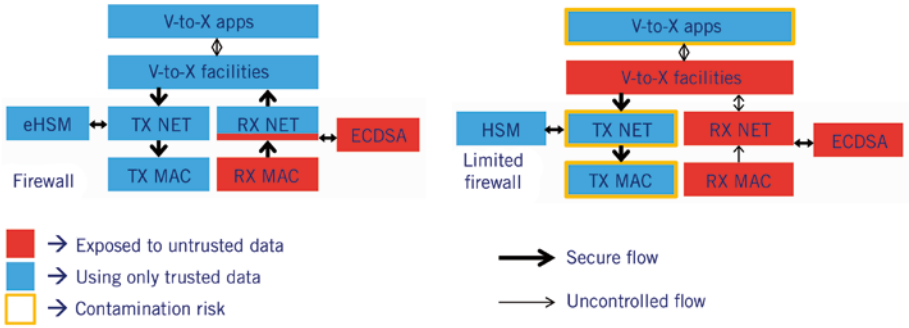


BILD 3 inführung einer Firewall eines Verifying-All-Messages-Systems („Verify-All“, links) und ein System mit einer begrenzten Verifizierungskapazität, bei der die Pakete zur Verifizierung ausgewählt werden („Verify-on-Demand“, rechts) (© Autotalks)

Sekunde. In der Praxis kann ein kabelloses Medium eine 100 %-Nutzung nicht erreichen und 1200 Verifizierungen pro Sekunde können bereits als „Beinahe-Verify-All“ betrachtet werden. Eine niedrigere Zahl ist ein Kompromiss -– ein Sicherheitssystem sollte aber für den schlimmsten Fall und nicht für ein optimistisches Szenario gerüstet sein.

Mit der Zeit wird ein Update der geschützten Firmenware erforderlich, um die Sicherheit zu verbessern. Die Lebensdauer eines Fahrzeuges ist länger als die Lebensdauer anderer kommerzieller Produkte. Stellen Sie sich nur einmal die Sicherheitsalgorithmen, die vor 20 Jahren benutzt wurden, in der heutigen Welt vor. Geräte von Autotalks haben die Kapazität zur Nutzung stärkerer Algorithmen, wenn die derzeit definierten Algorithmen zukünftig nicht stark genug sein sollten.

Die öffentlich-privaten Schlüsselpaare sollten gegen böswillige Angriffe geschützt sein. Das Hardware Security Module (HSM), das in Zahlsystemen eingesetzt wird, bietet den größten Schutz gegen physische und logische Attacken. Gemäß den Anforderungen von NPRM müssen Geräte entsprechend FIPS140-2 Level 3 zertifiziert sein. Der größte Unterschied zwischen der Stufe 2 und Stufe 3 der physischen Sicherheit besteht in der Fähigkeit zur Aufdeckung von Manipulationsversuchen durch den versuchten Zugriff auf das HSM und zur Annullierung aller Kritischen Sicherheitsparameter (CSPs) und aller Klartextdaten. Einfachere und „billigere“ Attacken, die sogenannten “Side-Channel-Attacken” zielen auf die verschlüsselte Quellendatei ab, dabei werden die Ausführungszeiten der kryptografischen Funktionen und die differenziale Leistungsaufnahme überwacht. Die Robustheit gegenüber solchen Side-Channel-Attacken ist von größter Bedeutung. Die gängigsten Attacken versuchen die Schwachstellen der HSM-Software auszunutzen; deswegen sollte die HSM-Software unter strengster Befolgung von Methodologie und Standards entwickelt und getestet werden.

ECDSA-Signaturlatenz kann beachtlich sein, da das ECDSA-Signaturmodul auf Sicherheit und nicht auf Geschwindigkeit ausgerichtet ist. In manchen Fällen kann die Latenz sogar 30 ms überschreiten, schnellere Lösungen signieren in 10 ms und weniger.

Die allgemeine V-to-V-Latenz ist kritisch. Die Aktualität der Daten steht im direkten Verhältnis mit ihrer Verwendbarkeit. NPRM setzt eine Grenze von 150 ms für das maximale GNSS-Alter. GNSS-Receiver aktualisieren die Position alle 100 ms, die herkömmlichen GNSS-Receivers sind aber für Latenz nicht optimiert und eine hohe Schwankung der Latenz ist üblich. Kürzere ECDSA-Signaturlatenz kann höhere GNSS-Latenzen und Schwankungen ausgleichen.

Während zehn Cooperative Awareness Messages (CAM)/Basic Safety Messages (BSM) in 1 s ausgetauscht werden, kann eine weitere Nachricht, Decentralised Environmental Notification Message (DENM) mit einer Warnung über situative Gefahren wie Eis auf der Straße, übertragen werden. Eine hohe HSM Signaturlatenz kann zu unnötigen Verzögerungen in der Übertragung von kritischen DENM führen.

NPRM betrachtet die Erkennung von Fehlverhalten als eine zwingend erforderliche Sicherheitsfunktion. Erkennung von Fehlverhalten ist nur ein Mechanismus zur Erkennung von scheinbar legitimen Daten, die von angegriffenen oder defekten Geräten stammt. Die kompromittierten Geräte werden aufgespürt und fortlaufend an einen zentralen Server übertragen. Da der Server für längere Zeiten unerreichbar sein könnte, sollte das HSM eine hohe Datenmenge über mehrere Wochen speichern können. Die

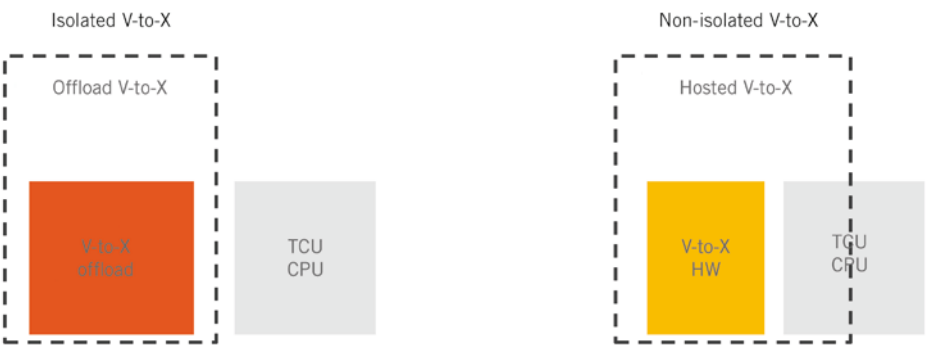


BILD 4 Telematikeinheit mit isoliertem und nicht isoliertem V-to-X (© Autotalks)

Speicherkapazität des HSM sollte entsprechend angelegt sein und kann mehrere MB betragen.

Der zentralisierte Server prüft Berichte von mehreren Fahrzeugen. Technologien zur Erkennung von Fehlverhalten stecken noch in Kinderschuhen und es wird sehr spannend zu sehen sein, ob sie die NPRM-Bewertungsphase überdauern. Ihre Bedeutung ist unbestritten und sollte zukünftig eine nachrüstbare Technologie sein, die zur V-to-X-Sicherheit beiträgt.

Die V-to-X-Funktionalität kommt bei Fahrzeugen entweder als eine dedizierte V-to-X ECU (Electronic Control Unit) oder wird der bestehenden ECU, typischerweise einer Kommunikations-Unit (CCU) oder einer Telematics Unit (TCU) hinzugefügt. Die Nutzung einer dedizierten V-to-X ECU ist am sichersten, da die Schnittstellen gut getestet und analysiert sind. Die Integration der V-to-X innerhalb anderer ECUs kann wünschenswert sein, um Kosten zu reduzieren, aber ohne eine strickte Domain-Isolierung kann die V-to-X-Sicherheit schwer beeinträchtig werden.

BILD 4 zeigt ein Telematics-Einheit mit isolierter und nicht isolierter V-to-X-Einheit. Im rechten Block mit nicht isolierter V-to-X ECU kann der TCU-Host über „Nicht-V-to-X-Kommunikationskanäle angegriffen werden, da dieselbe CPU V-to-X hostet, und ein Angriff auf die CPU gleichzeitig auch V-to-X gefährden würde. Die Verbindung von ungesicherten Kommunikationskanälen mit V-to-X ist eine konstruktiv schlechte Entscheidung. Im linken Block stellt das Offload-V-to-X-Modell die Isolation sicher.

ZUSAMMENFASSUNG

Zusammenfassend lässt sich sagen, dass die V-to-X-Sicherheit eine gut durchdachte Kombination mehrerer Mechanismen zur Systemsicherung ist. Autotalks geht an die V-to-X-Sicherheit mit größtem Respekt heran und zieht keine Kompromisse in Betracht, Risikominimierung steht immer im Vordergrund. Autotalks ist als Sicherheitsexperte auf dem V-to-X-Markt anerkannt und die Sicherheitsfunktionen der Chipsets wurden von den bestens ausgebildeten israelischen Ingenieuren und Cyber-sicherheitsexperten entwickelt.