CYMOTIVE
TRUSTED SMART MOBILITY

Cybersecurity in autonomen Fahrzeugen

Was der Markteinführung von autonomen Fahrzeugen noch im Wege steht

Cristian Ion, Head of Secure Engineering

Paradigmenwechsel bei der Fahrzeugsicherheit

Tod und Teufel – das sind die größten Herausforderungen bei der Absicherung autonomer Fahrzeuge. Wenn keine Person mit „gesundem Verstand" eingreifen kann und Fahrzeuge tagelang ohne Aufsicht böswilligen Akteuren ausgesetzt sind, gibt es wesentlich mehr Angriffspunkte als bei Fahrzeugen mit verantwortlichen Fahrern. Fahrzeugentwickler müssen daher an das Thema Cybersecurity ganz anders herangehen als bei manuell gesteuerten Autos.

In keinen Bereich der Automobil-Entwicklung ist in den letzten Jahren so viel Geld geflossen, wie in die autonomer Autos und Lastkraftwagen. McKinsey geht von 120 Milliarden US-Dollar allein bis zum Jahr 2019 aus. In den letzten Jahren hat die Entwicklungstätigkeit aber keinesfalls nachgelassen – eher das Gegenteil ist der Fall. Der Kapitalzufluss ist deswegen so groß, weil alle Marktbeobachter davon ausgehen, dass der erste Anbieter, der es schafft, autonome Fahrzeuge erfolgreich zu launchen und zu betreiben, damit übermäßig hohe Profite erwirtschaften wird.

Wie schwierig es ist, ein Auto tatsächlich autonom, also völlig ohne menschliche Eingriffe bei üblichen Geschwindigkeiten zu steuern, zeigen Beispiele aus jüngerer Vergangenheit. So haben sich ca. 30 autonome Taxis der Firma Cruise (einer General-Motors-Tochter) im Juni 2022 in San Francisco auf einer Kreuzung versammelt und den Dienst eingestellt. Das hat zu einem veritablen Verkehrschaos für viele Stunden geführt.

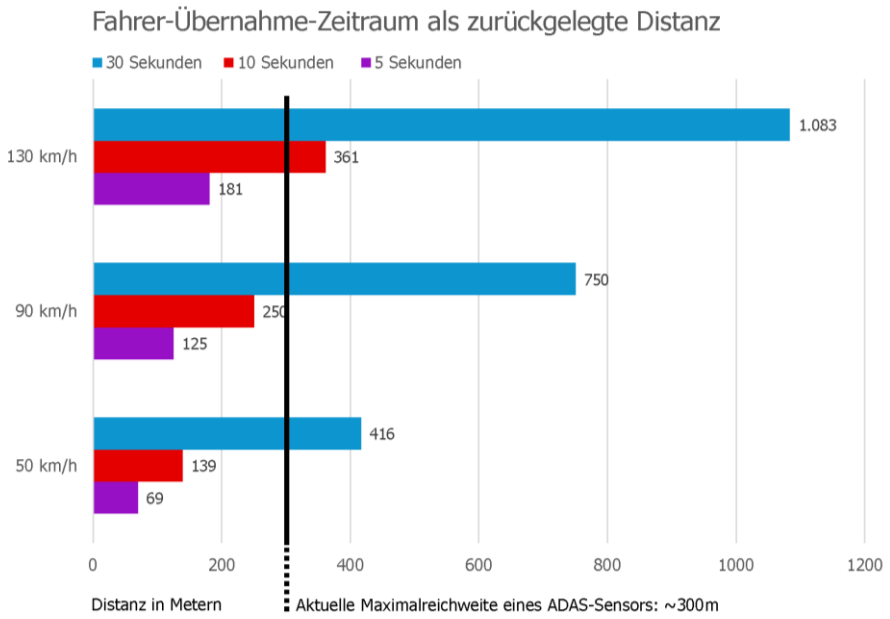
Bis auf den Imageschaden ist aber wenig passiert. Ganz anders erging es dem Taxi-Unternehmen Uber 2018 mit einem autonomen Fahrzeug, bei dem noch eine „Operatorin" zur Kontrolle mit im Auto saß. Die Autoelektronik konnte einen vorausfahrenden Fahrradfahrer nicht schnell genug klassifizieren, sodass das autonome Fahrzeug ihn ungebremst überfahren hat. Der Fahrradfahrer war tot. Für das Unternehmen Uber, das Unsummen in die Entwicklung gesteckt hatte, war das Engagement zur Entwicklung einer autonomen Taxiflotte damit beendet. Die Verantwortlichen hatten das Thema Sicherheit offensichtlich unterschätzt.

Die beiden Beispiele zeigen eindrucksvoll, was alles passieren kann. Ein sehr großes Problem lassen sie aber außer Acht: Es wird in Zukunft Akteure geben, die ein

Interesse daran haben, autonome Fahrzeuge zu kapern (um das Fahrzeug oder im Falle eines autonomen LKWs die Ladung zu stehlen), die Sensoren zu täuschen und Unfälle zu provozieren, um die Hersteller in Misskredit zu bringen, oder in besonders krassen Fällen Autos auch als Waffen einzusetzen (man denke beispielsweise an einen führerlosen 40-Tonner oder an das Science-Fiction-Buch „Daemon", das kaum mehr Fiktion ist).

Wenn es keinen Fahrer mehr gibt, der vor jedem Fahrtantritt überprüft, ob alles in Ordnung ist und der bei einem merkwürdigen Verhalten des Fahrzeugs selbst in das Geschehen eingreift, müssen dies Systeme übernehmen, die bisher nicht notwendig waren. Das Fahrzeug muss also selbst erkennen, dass etwas mit ihm nicht stimmt. Die Bedrohungslage ist damit eine völlig andere. Für ein Fahrzeug kann es schon schwierig sein zu erkennen, ob – platt gesprochen – jemand ein Bild vor die Kamera geklebt hat.

Ist kein Mensch mehr da, der das sieht, kann das schwerwiegende Konsequenzen haben. Für Automobilunternehmen ist es daher von entscheidender Bedeutung, eine



Schon Sekunden nach einem Sensorausfall fährt ein Fahrzeug im Blindflug. Bei autonomen Fahrzeugen darf das nicht passieren.

umfassende Risikoanalyse zu erstellen, welche Gefahren für ein bestimmtes Fahrzeug wie hoch sind.

Dies unterscheidet sich beispielsweise deutlich zwischen autonomen LKWs, die zwischen zwei Verteilerstationen nur auf der Autobahn unterwegs sind und so gut wie nie im öffentlichen Raum unbeaufsichtigt parken und den Fahrzeugen einer

Taxiflotte, die zu jedem Ort einer Stadt fahren können. Letztere könnten Kriminelle in einen Hinterhalt locken, die Mobilfunkverbindung stören, ungesehen Reifen stehlen oder in die IT des Fahrzeugs oder der Backend-Systeme eindringen.

Des Weiteren können sich autonome Systeme nicht über physische Gesetzmäßigkeiten hinwegsetzen: Wenn bei einem Auto bei 100 km/h wichtige Sensoren ausfallen, kann es viele Meter zurücklegen, bis es – ohne andere zu gefährden – sicher zum Stehen kommt. Wenn hierbei kein Mensch mehr eingreifen kann, wird der Ausfall von Sensorik schnell kritisch. Aber selbst wenn noch ein Mensch die Kontrolle übernehmen kann, ist das Auto bei 100 km/h nach 10 Sekunden schon 350 Meter weitergefahren. Aktuell reicht die Sichtweite moderner Sensoren nur 300 Meter weit. Muss der Fahrer erst geweckt und zur Übernahme bewegt werden, fährt das Fahrzeug bei defekten Sensoren eventuell bereits blind mit 100 km/h weiter.

Wo eine Sicherheitsarchitektur ansetzen muss

Die Komplexität der Sicherheit eines selbstfahrenden Fahrzeugs steigt insgesamt logarithmisch mit dem Grad der Autonomie. Dies ist etwas, was Fahrzeugentwickler teilweise immer noch unterschätzen. Es ist in der Regel nicht damit getan, noch ein Sicherheitslayer über bestehende Systeme zu legen. Die Datenmengen und Rechenleistungen, für die verschiedene Autonomie-Level notwendig sind, steigen exponentiell an.

Je unabhängiger ein Fahrzeug fahren soll, um so mehr Daten muss es verarbeiten und aus einem Sicherheitsblickwinkel auch in Echtzeit validieren. Soll es sich beispielsweise mit anderen Fahrzeugen in der näheren Umgebung über Verkehrsgegebenheiten (Eis auf der Straße, Unfälle, Ampelphasen) austauschen, kann es notwendig werden, Kommunikationsströme von beispielsweise 40 Partnern in der Nähe verschlüsselt zu verarbeiten. Das System muss in Echtzeit Angriffsversuche erkennen, Relevantes von Unwichtigem trennen, widersprüchliche Daten entwirren und Kommunikationsabbrüche adäquat verarbeiten (weil

Kommunikationspartner weitergefahren sind). Wenn dann pro Sekunde Gigabyte an Daten eintreffen, wird klar, was dafür an Rechenleistung nötig ist, um sie zu bewerten und zu verarbeiten.

Solche Systeme müssen tief in das Gesamtsystem des Fahrzeugs integriert werden und natürlich die eigenen Sensordaten in Echtzeit verarbeiten. Typischerweise sind das Kamera-Streams, LiDAR-Daten sowie Radar- und Positionsdaten von Satelliten. Sie müssen in Echtzeit bewertet und konsolidiert werden. Widersprechen sich einzelne Daten, gilt es, KI-Methoden anzuwenden, die falsche Daten erkennen und ignorieren können. So nutzen aktuelle autonome Fahrzeugsysteme auch Marker aus bereits erfassten (auch optischen) Daten, um die berechnete Position abzugleichen. Hierzu ist eine Bildanalyse im 3D-Raum notwendig.

Drei Ebenen der Sicherheit

Um etwas Licht und Struktur in die verschiedenen Risikoszenarien zu bringen, ist es sinnvoll, die Sicherheit von autonomen Fahrzeugen in drei Bereiche oder Ebenen aufzuteilen und getrennt zu betrachten:

- **Fahrzeugsteuerung** (Englisch: „Control")
- **Navigation**
- **Flottenorganisation & Einsatzplanung**

Fahrzeugsteuerung

Zur Fahrzeugsteuerung zählen alle technischen Systeme, die konkrete Komponenten wie Motoren, Lenkung, diverse Sensoren, Bremsen, Lichter, Positionsbestimmung und Beschleunigung betreffen.

Zu den größten Sicherheitsherausforderungen in diesem Bereich gehören:

Sensordaten-Validierung

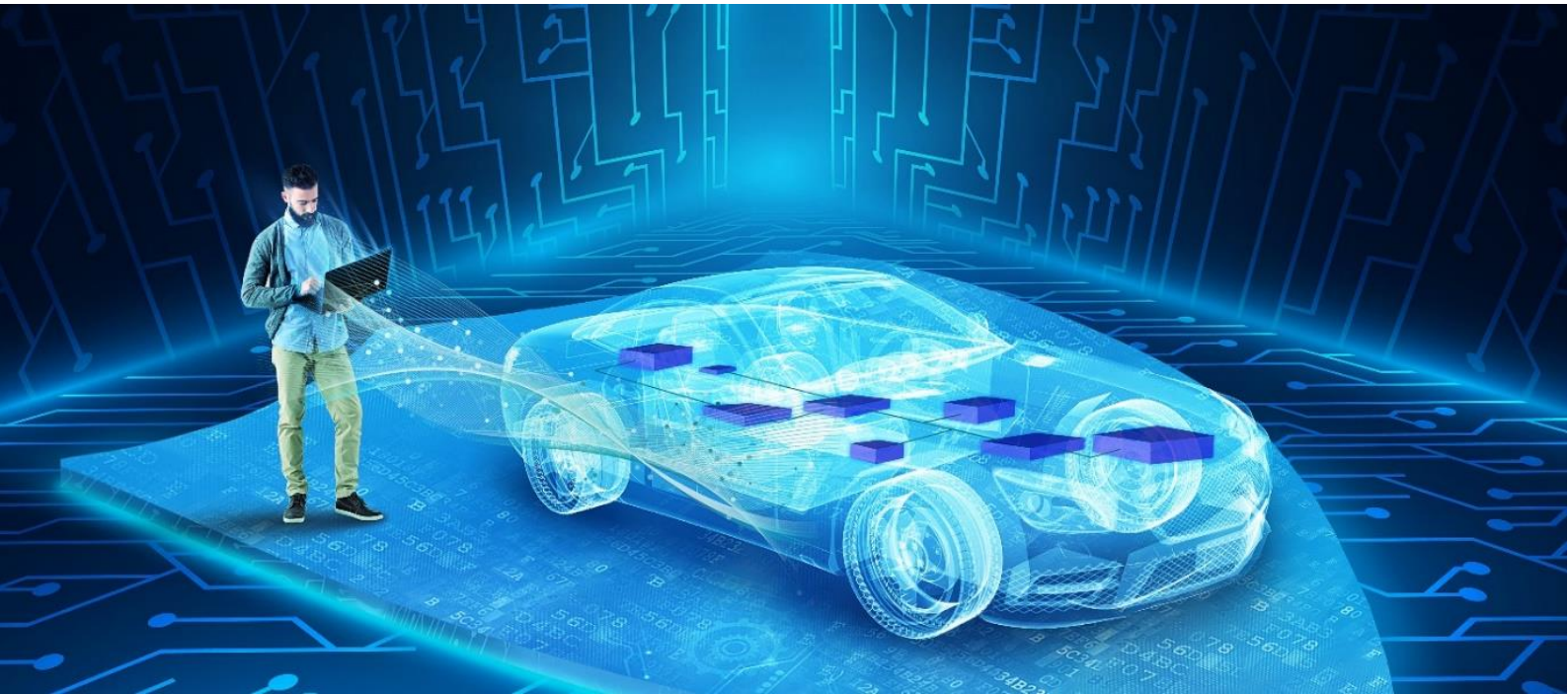
Ein autonomes Fahrzeug nutzt verschiedene Sensoren wie Kameras, LiDAR und Radar, um seine Umgebung zu erkennen und daraus ein internes Abbild der äußeren Welt zu erstellen. Die Sensoren können durch natürliche Störquellen (wie Spiegelungen in Fenstern oder auf Wasserflächen) und mutwillige Störungen irritiert werden. Es gibt auch die Möglichkeit, dass böswillige Akteure die Sensordaten nach der Erfassung manipulieren, bevor sie verarbeitet werden. Die Sicherheitssoftware in einem Fahrzeug muss also in der Lage sein, bei widersprüchlichen Sensordaten in Echtzeit Entscheidungen zu treffen, welchen Daten es vertraut und welchen nicht und daraus ein korrektes Abbild der äußeren Welt berechnen.

Präzise Positionsbestimmung

Das Fahrzeug muss seinen genauen Standpunkt ermitteln, um im Straßenverkehr beispielsweise die richtige Abbiegespur exakt anzusteuern oder präzise vor einer Haltelinie anzuhalten. Hierzu nutzt es auch Fotomaterial und Kameradaten, um etwa Straßenmarkierungen auszuwerten. GPS-Daten sind für eine exakte Positionsbestimmung nicht genau genug.

Valide Streckenführungsberechnungen

Das Fahrzeug ist für die Berechnung der zu fahrenden Strecke und Auswahl der richtigen Fahrbahn auf aktuelle Daten angewiesen, die eventuell auch erst von Fahrzeugen kommen, die vor wenigen Minuten an der gleichen Stelle vorbeigefahren sind. Häufig liefert eine Flottenzentrale zusätzliche Daten, die ebenfalls auf Manipulationen hin geprüft werden müssen. Problematisch können hier manipulierte Bilddaten sein, die das System zum Vergleich mit den erfassten Bilddaten der Sensoren abgleicht.



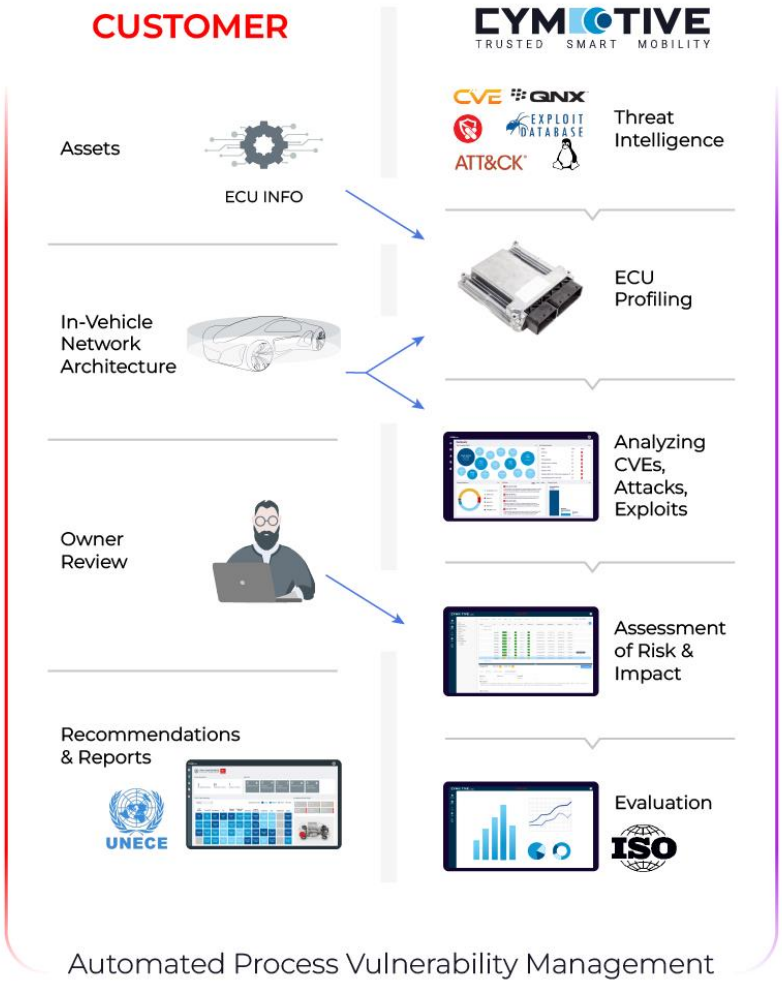
Robuste und sichere KI- und ML-Modelle

Die Beurteilung, ob Daten valide sein können, erfolgt in der Regel über Künstliche-Intelligenz-Algorithmen. Die Schwierigkeit hierbei ist, diese robust auch für seltene und außergewöhnliche Fälle zu gestalten, damit sie in diesen besonderen Situationen (sogenannten „Border Cases") vernünftige Entscheidungen treffen können. Es darf eben nicht passieren, dass die KI in einer unbekannten Situation einfach keine Entscheidung fällt und derweil den nicht erkannten Fahrradfahrer überfährt. Damit das nicht passiert, muss die KI in der Lage sein festzustellen, dass sie sich in einer für sie unbekannten Situation befindet.

Für Entwickler ist es auch unabdingbar, sicherzustellen, dass die KI die Umgebung nicht an Nebensächlichkeiten erkennt, die es zwar auf dem Trainingsgelände, aber nicht in der Realität auf der Straße gibt (das gilt insbesondere für Grenzfälle, die selten in der Realität eintreten).

Manipulationserkennung der Systeme und automatische Wiederherstellung eines sicheren Zustands

Besonders wichtig und herausfordernd ist die Erkennung, dass jemand die Systeme des Fahrzeugs manipuliert hat oder in die Systeme eingedrungen ist. Stellt das Fahrzeug ein solches Eindringen fest (sogenanntes „Intrusion Detection"), muss es darauf richtig reagieren, etwa in dem es die manipulierten Systeme wieder in ihren Ursprungszustand zurückversetzt. Dieses Thema ist besonders schwierig, weil es kaum möglich ist, alle denkbaren Angriffsversuche vorherzusehen und Angreifer natürlich versuchen werden, ihr Eindringen zu vertuschen.

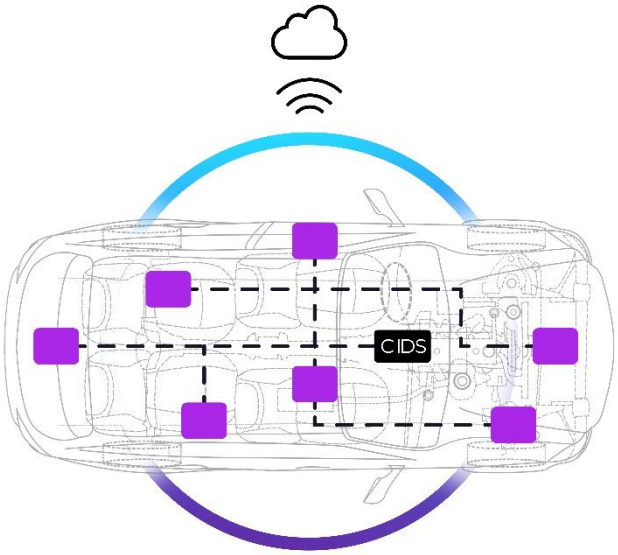


So können Menschen relativ leicht erkennen, dass eine

Bremse manipuliert wurde und sie beim Betätigen keine Reaktion zeigt. Für Fahrzeuge ist das schwierig, wenn diese Fälle nicht bereits vom Entwickler berücksichtigt wurden. Es reicht ja schon, die Blinker zu manipulieren, damit anderen Fahrzeugführer, die in die Kreuzung fahren, denken, man würde nach rechts abbiegen, obwohl das Auto geradeaus fahren wird.

Genügend Rechenleistung und Netzwerkbandbreite

Die Daten, die von den Sensoren kommen, und die Steuerungsbefehle müssen verschlüsselt übertragen und zur Verarbeitung entschlüsselt werden. Das ist nicht trivial, da üblicherweise Daten in der Größenordnung zwischen 5 und 10 Gbit/s anfallen und sicher über das Onboard-Netzwerk übertragen werden müssen. Bisher haben Komponenten wie eine Bremse, ABS oder eine Lenkung keine Krypto-Chips eingebaut und können die Verschlüsselung nicht leisten.



Navigation

Im Themenbereich Navigation und Guidance geht es darum, dass die Fahrzeuge sicher ihren Weg durch den Straßendschungel finden – auch wenn Ihnen wichtige Informationen fehlen oder manipulierte Daten vorliegen. Dabei gibt es besondere Herausforderungen zu beachten.

Verlässliche, robuste Positionsdaten

Wie überall gibt es auch in Europa Gegenden, in denen GPS-Daten gestört werden oder kaum zu empfangen sind (Tunnel, zwischen Hochhäusern, in Parkgaragen). Da das GPS-Signal relativ schwach ist (es muss erst circa 20.000 km zurücklegen), kann der Empfang leicht gestört werden (nicht nur in Kriegsgebieten). Dafür benötigt das Fahrzeug verlässliche, geprüfte Daten, die als Alternative eine sichere Ortsbestimmung ohne GPS möglich machen.

Authentifizierte Navigationsdaten

Auch das Kartenmaterial und die genauen Navigationsdaten muss das Fahrzeug prüfen können. Über einen Update-Mechanismus ist nicht nur theoretisch das Einspielen manipulierter Daten möglich. Da Informationen über Bauarbeiten

regelmäßig ausgetauscht werden und diese von anderen Fahrzeugen stammen können, ist eine Validierung und ein Abgleich mit der realen Umgebung notwendig.

V2X-Daten-Validierung

Tauscht ein Fahrzeug viele Daten mit den Fahrzeugen, Smartphones, Polizei und Feuerwehr oder Verkehrsinfrastruktur in der Umgebung aus (Vehicle-to-Vehicle (V2V) und Vehicle-to-Infrastructure (V2I)), müssen diese Daten geprüft und verarbeitet werden. Das können enorme Datenmengen sein, die alle ver- und entschlüsselt werden müssen. Der Datenaustausch erfolgt auf Basis von 5G direkt zwischen den Teilnehmern (also ohne Funkmast dazwischen). Durch die Vielzahl unterschiedlicher Teilnehmer (in der Stadt können das durchaus 50 bis 100 sein) ist die Gefahr an dieser Stelle sehr groß, dass das Fahrzeug Fake-Daten übernimmt. Es muss daher selbst auch ohne externe Unterstützung in der Lage sein, die Daten als valide oder unsicher einzustufen.

Integration in Smart-Mobility-Anwendungen

Zu Smart-City-Lösungen gehören natürlich auch Fahrzeuge, die mit der smarten City kommunizieren und Daten austauschen. Auch hier gilt es, auf höchste Sicherheit zu achten, um nicht über diese Schnittstelle Malware oder kriminellen Akteuren ein Einfallstor zu öffnen.

Verarbeitung großer Datenmengen

Die Verarbeitung der großen, meist verschlüsselten Datenmengen für die Navigation und Guidance des Fahrzeugs erfordert hohe Netzwerkbandbreiten und vor allem einen hohe Rechenleistung im Fahrzeug. Diese lässt sich nicht in eine Cloud auslagern und muss auch ohne Funkverbindung zur Flottenzentrale sicher funktionieren. Die geforderte Rechenleistung übersteigt selbst die Leistungsfähigkeit moderner Workstations. Oft lässt sie sich nur durch spezialisierte Hardware erreichen.

Flottenorganisation und Einsatzplanung

Betrachtet man die aktuellen Entwicklungen bei autonomen Fahrzeugen, werden diese nicht zuerst für Privatanwender zur Verfügung stehen. Wahrscheinlicher ist der Einsatz als selbstfahrende LKWs für Transportunternehmen und bei Taxiflotten (auch weil hier ein großer Fachkräftemangel oder hoher Kostendruck herrscht). In San Francisco hat mit „Cruise" das erste Taxi-Unternehmen seinen kommerziellen Dienst mit fahrerlosen Fahrzeugen aufgenommen.

Hinter der Steuerung der Flottenfahrzeuge durch eine Fleet-Control-Zentrale stehen komplexe Anwendungen, die neben dem On- und Offboarding von Fahrzeugen, dem Billing, der Auftragserteilung und Positionsauswertung auch eine Kapazitätsplanung sowie eine Unfall- und Ausfallbehandlung durchführen müssen.

Sicherheitsmängel können schnell zu Störungen und damit zu schlechter Presse und wirtschaftlichen Schäden führen. Die Sicherheitsherausforderungen in diesem Bereich sind:

Authentifizierte Backend-Kommunikation

Die Kommunikation zwischen Fahrzeug und Flottenmanagement muss abgesichert und verschlüsselt erfolgen. Hier darf sich kein anderer Akteur zwischenschalten können (Man-in-the-Middle-Attack), um die Fahrzeuge in die Irre zu leiten. Ebenso müssen die Telemetrie-Daten vom Fahrzeug zur Zentrale vor Manipulationen geschützt sein. Die Kommunikation muss garantieren, dass sich kein böswilliger Akteur als ein bestimmtes Fahrzeug ausgeben und Daten liefern kann.

VSOC – Unfallerkennung und Reaktion

Das Erkennen von Unfällen und die angemessene, richtige Reaktion auf den Unfall kann komplex und schwierig werden. Dafür benötigen Flottenbetreiber ein Vehicle Security Operation Center (VSOC). Das gilt auch, wenn das Fahrzeug selbst feststellen muss, wie groß die Schäden sind. Manipulationsversuche an den Flottenfahrzeugen müssen ebenfalls verschlüsselt an das VSOC übertragen werden, um adäquat darauf reagieren zu können.

Sicherheitslücken-Management und OTA-Updates

Ein Fahrzeug besteht aus vielen Einzelkomponenten mit eigenen Softwareplattformen, die ihrerseits häufig modular aus mehreren Software-Komponenten bestehen. Hält man diese Software nicht aktuell, nimmt die Sicherheit Stück für Stück ab, weil Angreifer mehr Zeit haben, Sicherheitslücken zu entdecken und auszunutzen. Flottenbetreiber müssen daher die Software-Stände und -Versionen der eingesetzten Software kennen und gefundene oder bekannt gewordene Fehler und Sicherheitslücken per Update over-the-air (OTA) beheben können. Steht noch kein Update bereit, müssen sich gefährdete Systeme temporär deaktivieren lassen.

Absicherung des VSOC

Ein erfolgreicher Angriff auf die Flottensteuerungszentrale kann leicht eine ganze Flotte ausschalten. Da diese Zentrale meistens eine Vielzahl an Systemen und Diensten betreibt, die alle voneinander abhängig sind, ist die hermetische Absicherung der Zentrale eine sehr komplexe Aufgabe.

Fernsteuerung von Fahrzeugen

Aktuell bringen vor allem Mobilfunkprovider das Thema „Remote-Control" von Fahrzeugen in die Diskussion. Das ist in mehrfacher Hinsicht eine besondere Herausforderung, da sowohl das Mobilfunknetz in Deutschland dafür zu viele Lücken aufweist und eine Fernsteuerschnittstelle neue Angriffspunkte eröffnet (die für Angreifer sicher lohnenswert erscheinen).

Aktueller Entwicklungsstand

Letztlich zeigt die Vielfalt der beschriebenen technischen Herausforderungen, dass eine 100-prozentige Absicherung enorme Anstrengungen erfordern.

Aktuell fehlt es den Komponenten in heutigen Fahrzeugen an der notwendigen Rechen- und Kommunikationsleistung, um die Sicherheit eines vollautonomen Autos zu gewährleisten. Deswegen sind Prototypen und experimentelle Fahrzeuge heutzutage häufig eingeschränkt unterwegs, beispielsweise was die Geschwindigkeit oder die Größe des Terrains angeht. Wenn in kritischen Situationen Fahrer kurzfristig noch die Kontrolle über das Fahrzeug übernehmen können, reicht die aktuelle IT-Infrastruktur im Fahrzeug meist noch aus.

Ab einem Autonomie-Level 4, bei dem kein Fahrer mehr aktiv eingreift und das Fahrzeug in allen Situationen autonom fährt, sind die Anforderungen an die Fahrzeugsteuerung inklusive redundanter Sensoren und die Verarbeitungskapazitäten um Faktoren höher. So muss in einem solchen Fahrzeug eine Rechenleistung verfügbar sein, die weit über das hinausgeht, was aktuell

verbaut wird. Dies wird insbesondere klar, wenn man bedenkt, mit wie vielen Akteuren das Auto gleichzeitig kommuniziert, wie viele Sensoren es auswertet und auch konkurrierende, nicht stimmige Daten validieren und verarbeiten muss. Die durchgängige Verschlüsselung aller Kommunikationswege und die Berechnung eines internen 3D-Abbilds der externen Welt kostet zusätzliche Rechen-Power. Wenn man die dafür benötigte Rechenleistung in traditioneller IT-Technik aufbaut, braucht es dafür mehrere Server-Racks.

Damit ist auch klar, dass für tatsächlich autonome Fahrzeuge ein „Aufbohren" der bestehenden Fahrzeugtechnik nicht ausreicht und kein gangbarer Weg ist. Autonome Fahrzeuge erfordern eine radikale Anpassung der IT-Infrastruktur des Fahrzeugs und hohe Investitionen in die Entwicklung solcher Plattformen, um die Sicherheit im Straßenverkehr gewährleisten zu können.

Hinzu kommt der Aufbau von Rechenzentren, die für das Flottenmanagement und die Steuerung notwendig sind. Diese müssen ebenfalls höchsten Sicherheitsanforderungen genügen und die Flotten aktiv managen und steuern. Sie müssen qualitativ hochwertige Navigationsdaten bereitstellen und perfekt gegen Angriffe abgesichert werden.

Auch die Gesetzgeber haben das Thema IT-Sicherheit in Fahrzeugen erkannt: Mit den beiden Normen UNECE R155 und GB/T gibt es umfangreiche Richtlinien für alle Fahrzeuge im Straßenverkehr (also auch autonom fahrende), die Vorgaben machen und Prüfungen festlegen. Die GB/T für den chinesischen Markt ist diesbezüglich sehr ausführlich und präzise, die UNECE R155 bleibt in vielen Fällen vage und überlässt es teilweise den Mitgliedstaaten, die Norm auszulegen und deren Umsetzung zu prüfen.

Professionelle Beratung sorgt für Sicherheit

Autohersteller waren in der Vergangenheit Unternehmen mit vielen Ingenieuren und kleinen Softwareabteilungen. Für die Entwicklung komplexer, sicherer Systeme müssen die Entwicklungsprozesse sauber designt und kontinuierlich überwacht werden. Die Expertise, diese Prozesse aufzusetzen und einzuführen, entsteht nicht über Nacht und erfordert einiges an Know-how.

Cymotive ist seit Jahren bei etlichen großen Automobilherstellern in die Entwicklung autonomer Fahrzeuge involviert – unter anderem als ausgewählter Cybersecurity-Partner der Volkswagen-Gruppe. Das 2016 in Israel gegründete Unternehmen unterstützt sowohl beratend als auch als Software-Entwickler OEMs und Zulieferer bei der Absicherung von Fahrzeugen.

Mit der Cybersecurity-Expertise und dem Know-how zu den Anforderungen an die IT- und Fahrzeugsicherheit von autonomen Fahrzeugen kann Cymotive Hersteller

umfassend unterstützen. Dies ist häufig notwendig, weil der radikale Wandel der Autoarchitektur beim Übergang zum vollautonomen Fahrzeug Kompetenzen erfordert, die bisher bei Autoherstellern kaum vorhanden waren.

Suchen Sie noch nach Unterstützung für Ihre Zukunftspläne? Dann nehmen Sie gerne Kontakt auf: office@cymotive.de

Cymotive auf einen Blick

Das Unternehmen ist ein Cybersecurity-Player mit Beratungs, Ingenieurs- und Prüfungsdienstleistungen ausschließlich für die Automobil-Industrie. Wir unterstützen OEMs und Zulieferer bei der Konzeption, Implementierung und Entwicklung autonomer Fahrzeuge und beim langjährigen Betrieb bin zum Ende des Auto-Lifecycles. Dazu gehören Prozess-, Compliance- und Beratungsleistungen, Schaffung von technischer Infrastruktur und Dokumentation sowie der Integration einer durchgehenden Security-Schicht über die gesamte Fahrzeug-Steuerung und -IT hinweg. Cymotive kann darüber hinaus Zulieferer coachen und deren Ergebnisse auf Sicherheitslücken hin überprüfen.

Cymotive entwickelt eigene Software, die Hersteller in die Fahrzeuge integrieren können. Dazu gehört ein Intrusion Detection System, das Manipulationsversuche am Fahrzeug (zum Beispiel bei den Sensoren) erkennt und meldet, ein Vulnerabilitäten-Management und Software, die Malwareangriffe erkennen kann. Damit begleiten wir Autohersteller von der Konzeption, über die Entwicklung bis hin zum Roll-Out und Betrieb der Fahrzeuge „in the wild".

Seit mehr als fünf Jahren ist Cymotive auf mehreren Plattformen für unterschiedliche Hersteller aktiv und hat auch ein Kompetenzzentrum für IT-Entwicklung von autonomen Fahrzeugen inklusive Kommunikation und Back-End.

Kontakt

Deutschland

Major-Hirst-Str. 5
38442 Wolfsburg
+49 5361 897 8775

office@cymotive.de

Israel

94 Yigal Alon St. Tower 1
Tel Aviv, Israel, 6789155
+972 79 5729960

office@cymotive.com