Die Communication Lockdown™-Technologie:

Höchste Cybersicherheit für vernetzte Fahrzeuge

Übersicht

Dieses E-Book gibt einen technischen Überblick über die Communication Lockdown™-Technologie von GuardKnox. Es erklärt, inwiefern diese patentierte Technologie per Hardware- und Software-Implementierung der Automobilindustrie helfen kann und welche Möglichkeiten sie für die gesamte automobile Wertschöpfungskette bietet.

Zunächst werden kurz die Architektur und der Konnektivitätsumfang vernetzter und autonomer Fahrzeuge beschrieben und grundsätzliche Gedanken zu deren Cybersicherheit aufgestellt.

Es wird dargestellt, wie sich die GuardKnox-Methode von typischen IT-basierten Lösungen unterscheidet. Zudem wird auf die Feinheiten der Communication Lockdown™-Technologie eingegangen – wie etwa die drei Prüfschichten, die „Zustandsmaschine“ zur Kommunikationsüberprüfung sowie die flexible Hardware-Implementierung.

Zum Schluss werden die Methodik, die Vorteile sowie die Integrationsmöglichkeiten beschrieben.

Die Notwendigkeit automobiler Cybersicherheit

Vom Auto zum Computer auf Rädern

Vor etwas mehr als 50 Jahren verbesserte Volkswagen die Fahrzeugleistung drastisch, indem die Einspritzung elektronisch gesteuert wurde. Seitdem kamen fast 150 Computer und Steuergeräte hinzu, die in 5-10 verschiedenen Netzwerken betrieben werden. Diese steuern die technischen Features des Fahrzeugs, einschließlich der Motor- und Getriebeleistung, Klimatisierung, Fensterhebern, Displays, ABS und des Parkassistenten. Außerdem verbessern sie das Fahrerlebnis durch Infotainmentsysteme, Nachrichten sowie moderne Technik wie Keyless Entry und vielem mehr.

Stand heute sind weltweit mehr als 110 Millionen Fahrzeuge ständig mit dem Internet verbunden. Dieses wird zur Unterhaltung, Navigation, für Notdienste sowie drahtlose Softwareaktualisierungen (OTA) von OEMs und Aftermarket-Anbietern genutzt.

Mit mehr als 150 Millionen Codezeilen pro Fahrzeug – mehr als dreimal so viel wie die modernsten Kampfflugzeuge – birgt diese Technologie computerähnliche Cyberrisiken, einschließlich des Diebstahls persönlicher oder finanzieller Daten, Ransomware, Remote-Hijacking, heimlicher Überwachung der Fahrzeuginsassen, böswilliger Änderungen an der Firmware / Software und vieles mehr.

Cyberangriffe können zu Daten- sowie finanziellem Verlust und sogar zum Verlust von Menschenleben führen. Neben den Risiken für die Verbraucher bestehen auch erhebliche operative, markenbezogene und finanzielle Risiken für OEMs, Subunternehmer und andere beteiligte Unternehmen im Automobilökosystem.

Den richtigen Cyberschutz finden

Moderne Fahrzeuge basieren auf einer gut strukturierten Kommunikation zwischen den Steuergeräten und benötigen einen wirksamen Schutz, um diese Kommunikation zu überwachen. Klassische Lösungen der Computerindustrie wie Intrusion Detection / Intrusion-Prevention-Systeme (IDS / IPS) und / oder Firewalls sind naheliegende Möglichkeiten, um Fahrzeuge zu schützen. Jedoch reichen sie häufig nicht aus, um die Cybersicherheitsanforderungen der Automobilindustrie zu erfüllen:

- Sie bieten keine Echtzeit-/ Sofortmaßnahmen auf neue Bedrohungen oder sich verändernde Malware
- Die Algorithmen basieren auf statistischen Durchschnittswerten
- Sie benötigen viel Zeit, um neue Bedrohungen zu analysieren und um entsprechende Updates zu entwickeln
- Sie bieten keinen Support für ein externes Security Operations Center (SOC) an, um Fahrzeuge kontinuierlich zu überwachen und mit dem Halter oder Fahrer zu kommunizieren

GuardKnox begegnet diesen Herausforderungen mit der patentierten Communication Lockdown™-Technologie. Diese wird bereits zur Abwehr von Cyberangriffen auf Waffensysteme wie Kampfflugzeuge oder Raketenabwehrsysteme verwendet. Communication Lockdown™ erzwingt eine formal verifizierte und deterministische Konfiguration der Kommunikation zwischen den verschiedenen Netzwerken des Fahrzeugs und eliminiert alle bekannten und unbekannten Cybersicherheitsrisiken in Echtzeit.

Diese Cybersicherheitsmethode erfüllt die Anforderungen des sicherheitskritischen Subsystems vernetzter Fahrzeuge. Der vollständig deterministische Ansatz besteht nicht darin, nach Angriffen zu suchen, sondern sicherzustellen, dass das Fahrzeug weiterhin so funktioniert, wie es konzipiert wurde. Die Zustandsmaschine erzwingt vorgegebene Zustände mit einem dedizierten Regelsatz. Cloud-Konnektivität oder laufende Updates sind nicht erforderlich, so dass sich keine Malware einschleichen und die Sicherheit des Fahrzeuges beeinträchtigen kann.

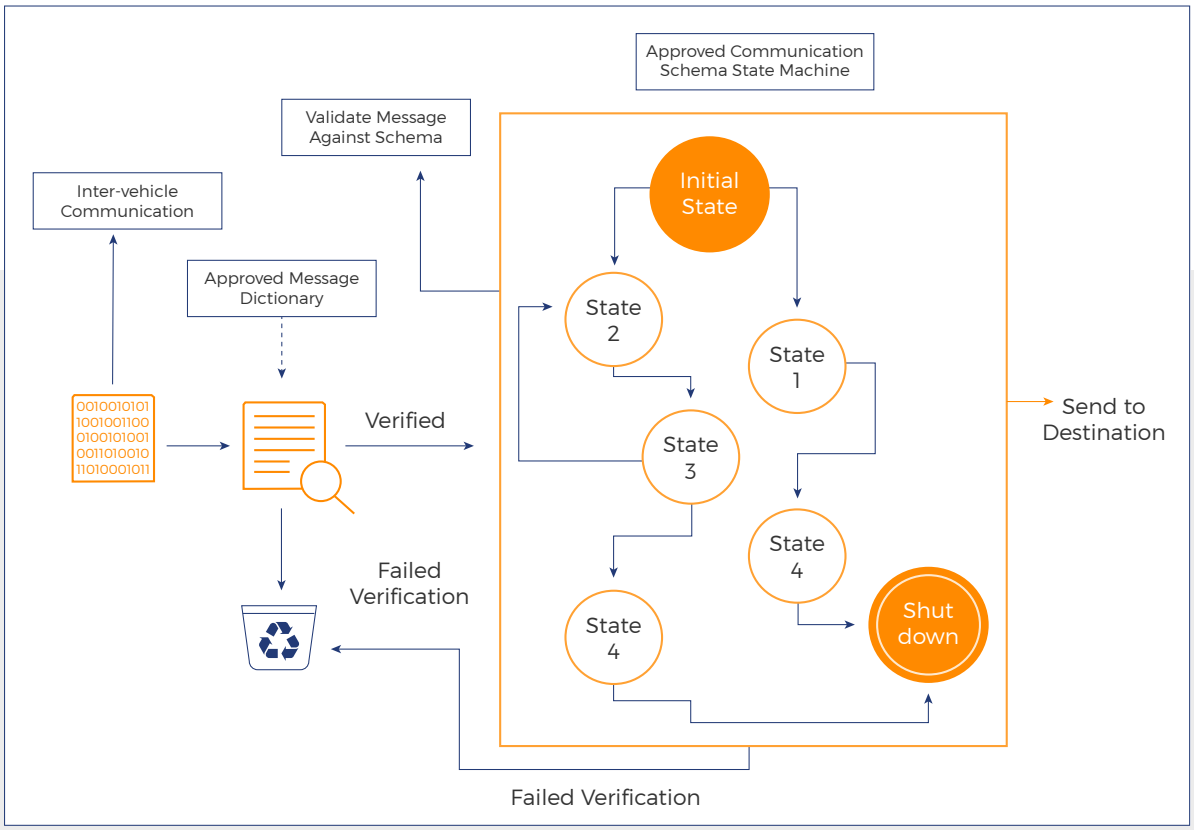
Im Folgenden werden die Unterschiede der GuardKnox-Methode zu herkömmlichen IT-Lösungen aufgezeigt.

Fähigkeit	Communication Lockdown™	Firewall	IDS/IPS	Anti-Virus
Sicherheit-mechanismus	• Formal verifizierte Zustandsmaschine • Agnostisch gegenüber Angriffen • Zertifizierbar (Sicherheit) • Sperrbarkeit der zugelassenen Konfiguration	• Statische, regelgebundene Firewall • Muss aktualisiert werden, sobald neue Angriffe auftreten	• Heuristische Erkennung von Angriffen (Anomalien) • Zuverlässigkeit kann nicht nachgewiesen werden	• Lokaler Virenschutz • Signatur-Updates erforderlich
Abwehrfähigkeit	• Alle Fahrzeugnetze • Prävention auf Bit-Ebene	Mehrere Auto-Netzwerke	Keine Prävention	1 Steuergerät
Zuverlässigkeit	• 100% - geprüft und getestet hinsichtlich der Anforderungen im Automobilbereich • Keine „False Positives“	Kann nach Automobilstandards geprüft, aber nicht formal verifiziert werden	• 98% Erkennungsrate • 5% Falsch-positiv-Rate	Zuverlässigkeit kann nicht nachgewiesen werden
Wartung	• Keine Cloud-Konnektivität erforderlich • Keine Updates erforderlich	Erfordert Cloud-Konnektivität und regelmäßige Updates	Erfordert Cloud-Konnektivität und kontinuierliche Updates	Aktualisierung bei jeder Änderung des Steuergeräts
Physische Trennung	Trennung von Hardware-, Software- und Firmware-Ebene zwischen den Netzwerken	Keine	Keine	Keine
Integration	• Minimaler Integrationsaufwand • Durchlässig für andere Steuergeräte	Erfordert die Integration in ein Steuergerät eines Drittanbieters (Tier 1)	Erfordert die Integration in mehrere Steuergeräte von Drittanbietern (Tier 1)	Erfordert Integration in Steuergerät / Entwicklungsumgebung
Skalierbarkeit	• Sichere Full-Service-Hosting-Plattform • Vollständige Unterstützung von virtuellen und serviceorientierten Umgebungen	• Feste Funktionalität • Erfordert neue Integration in die jeweilige Umgebung	• Feste Funktionalität • Erfordert Integration in die jeweilige Umgebung	Das Steuergerät muss neu kompiliert und zertifiziert werden
Kostengünstige Hardware	Keine Notwendigkeit, die Architektur der Fahrzeug-Hardware für zusätzliche Softwareerweiterungen / Anwendungen zu ändern	Keine	Keine	Keine
Einhaltung von Normen	• Funktionale Sicherheit: ISO 26262 • Technische Sicherheit (ISO 15408)	Keine	Keine	Keine
Physische Sicherheit	Manipulationssicher: Löscht Informationen bei einem Manipulationsversuch	Keine	Keine	Keine
Eignung für die automobile Wertschöpfungskette	Volle Anpassung an die Hardware-Wertschöpfungskette, keine Integration	Benötigt Software-Integration	Umfassende Integration	Umfassende Integration

Die Communication Lockdown™-Methode

Die Verbreitung von bösartigem Code verhindern

Die Communication Lockdown™-Technologie erkennt und verhindert die Einschleusung und Verbreitung bösartiger Nachrichten zwischen den verschiedenen Steuergeräten. Alle eingehenden Nachrichten werden überprüft und nur genehmigte / legale Nachrichten werden an ihren Zielort weitergeleitet. Alle Angriffsversuche werden protokolliert und können über einen drahtlosen Kommunikationskanal an ein Security Operations Center (SOC) zur weiteren technischen und statistischen Analyse gemeldet werden.



Communication Lockdown™ ist in der Lage, die technischen Spezifikationen der OEMs, insbesondere die Kommunikationsmatrix, die Datenbank mit den spezifizierten Nachrichten auf den Datenbussen und die funktionalen Spezifikationen zu nutzen, um ein Kommunikationsschema zu erstellen, das das ordnungsgemäße Verhalten des Fahrzeugs modelliert. Alle bekannten und unbekannten Bedrohungen und Cyberangriffe werden in Echtzeit abgewehrt, ohne die Gefahr einer Ausbreitung auf andere Netzwerke oder sicherheitskritische Komponenten.

Dies ist unter der Patentnummer 9.899.563B2 mit dem Titel "Specially Programmed Computing Systems with Associated Devices Configured to Implement Secure Commmunication Lockdowns and Methods of Use Thereof" näher beschrieben.

Eine unabhängige Lösung ohne ständige Updates

Da das korrekte Verhalten aller Nachrichten durch das GuardKnox-Kommunikationsschema vollständig definiert und vom OEM zertifiziert wurde, ist die Communication Lockdown™-Technologie völlig agnostisch für alle Arten von bekannten sowie unbekannten Cyberangriffen. Aus diesem Grund ist die GuardKnox-Lösung nach der Installation vollständig autonom und kann deterministisch ohne häufige Software- oder Firmware-Updates arbeiten - im Gegensatz zu Intrusion Detection- / Intrusion Prevention-Systemen (IDS / IPS) oder anderen herkömmlichen IT-basierten Lösungen.

Ein neues Communication Lockdown™-Schema muss nur dann generiert, zertifiziert und über ein OTA-Update installiert werden, wenn der OEM die Kommunikationsspezifikationen oder die Konfiguration des Fahrzeugs ändert.

Drei Schichten für Kommunikationssicherheit

Die Wirksamkeit der Communication Lockdown™-Methode basiert auf der patentierten Fähigkeit, Nachrichten auf mehreren Schichten zu überprüfen und zu verifizieren. Auf diese Weise wird sichergestellt, dass bei einer Kompromittierung durch eine externe Nachricht aus dem Ökosystem des Fahrzeugs das interne Fahrzeugnetzwerk vollständig vor der Verbreitung bösartiger Aktivitäten geschützt bleibt.

Alle eingehenden Nachrichten werden von GuardKnox auf drei Schichten geprüft:

Routingschicht

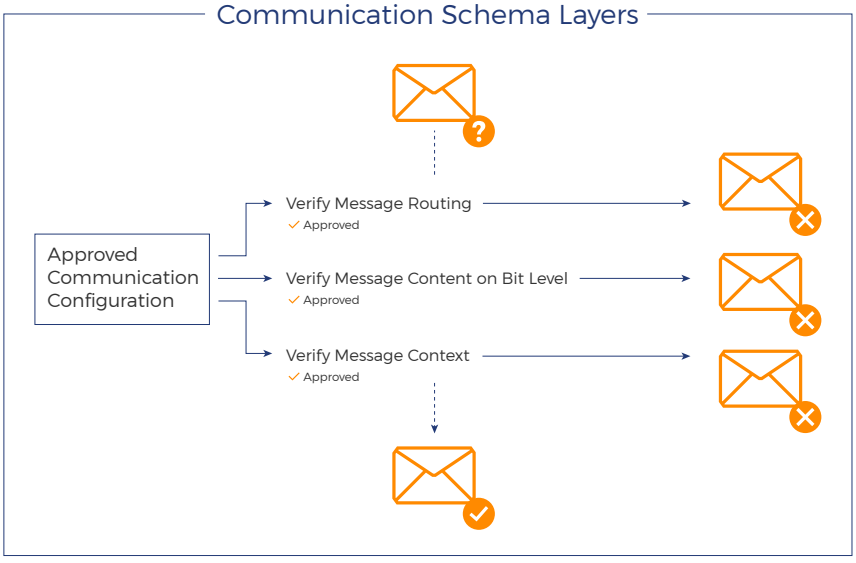
Der Ursprung und das Ziel jeder eingehenden Nachricht (Typ) werden vom Communication Lockdown™-Schema überprüft, um sicherzustellen, dass sie zulässig oder „legal“ sind. Beispielsweise sind Nachrichten vom Infotainmentsystem an die Antriebsstrangkomponenten (Lenkung, Bremsen usw.) unzulässig und werden daher sofort verworfen.

Inhaltsschicht

Der Inhalt jeder eingehenden Nachricht wird bis auf die Bitebene hin überprüft, um sicherzustellen, dass das zulässige Format gemäß den technischen Spezifikationen eingehalten wird. Nachrichten, die nicht dem definierten Format entsprechen, werden verworfen.

Kontextschicht

Der Inhalt jeder eingehenden Nachricht wird auf Rechtmäßigkeit im spezifischen Funktionszustand des Fahrzeugs, des Teilsystems, der ECU usw. überprüft. Nachrichten von einem bestimmten Ursprung zu einem bestimmten Ziel sind je nach Kontext/Funktionsstatus des Fahrzeugs zulässig oder werden verworfen.



Verifizierung des Nachrichtenkontextes mit einem Zustandsautomaten

Für jedes Steuergerät im Fahrzeug wird die GuardKnox Communikation Lockdown™-Technologie verwendet. Dahinter steht das theoretische Modell einer Zustandsmaschine zur Bestimmung des tatsächlichen Kontexts (Zustand) des Fahrzeugs sowie der Auswirkungen der eingehenden Nachrichten.

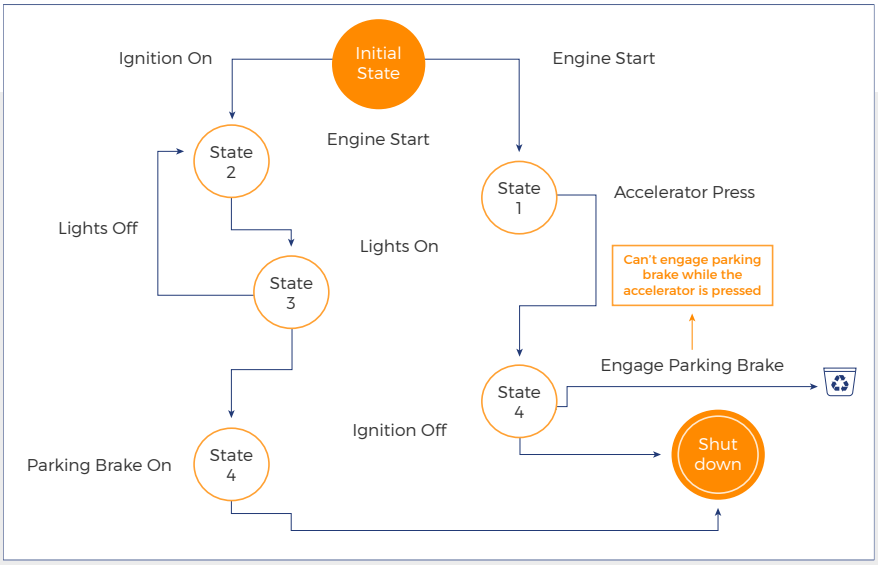
Der Fahrzeugzustand besteht aus einer beliebigen Anzahl von Variablen, z. B.:

- Fahrzeugzustand (geparkt, in Bewegung, etc.) Motorzustand (Ein, Aus, etc.)
- Aktuelle Geschwindigkeit
- Status des Gaspedals
- Status des Bremspedals
- Status des Lenkrads
- Status der verschiedenen Steuergeräte
- Status der verschiedenen Systemkomponenten (funktionsfähig, ausgefallen)

Jede neu eingehende Nachricht wird daraufhin überprüft, wie sie die Zustandsvariablen des Fahrzeugs ändert und wie sich diese Änderungen auf den Gesamtfahrzeugstatus auswirken. Abhängig von dem durch den Zustandsautomaten definierten Kontext und den zuvor empfangenen Nachrichten wird bestimmt, ob die neue Nachricht weitergeleitet oder gelöscht werden soll.

Beispiel: Betätigen der elektronischen Parkbremse während das Fahrzeug in Bewegung ist

Wenn ein Fahrzeug bei gedrücktem Gaspedal mit 90 km/h fährt und eine Nachricht zum Betätigen der Parkbremse empfängt, erkennt die Zustandsmaschine, dass diese Nachricht im Kontext eines schnell fahrenden Fahrzeugs unzulässig ist, und verwirft diese Nachricht sofort.



Verifying Message Content Using a Finite-State Machine
(Simplified View with Sample Message)

Beispiel: Öffnen eines Cabrioverdecks bei 90 km/h

Nehmen wir an, dass Cabriolets verlangen würden, dass das Auto unter 25 km/h fährt, um den Dachöffnungsmechanismus betätigen zu können. Bewegt sich ein Fahrzeug deutlich schneller, könnte der Wind die Mechanik beschädigen oder sogar das Dach abreißen. Sollte ein Fahrzeug bei einer Fahrt mit 90 km/h einen Befehl zum Öffnen des Verdecks erhalten, würde die Zustandsmaschine erkennen, dass die Nachricht unzulässig ist und die Meldung sofort verwerfen.

Beispiel: Nachricht vom OBD-II-Wartungsstecker während der Fahrt

Wird eine Nachricht vom OBD-II-Wartungsstecker empfangen, während das Fahrzeug in Bewegung ist, würde die Zustandsmaschine erkennen, dass sie sich nicht in einem gültigen Wartungsmodus befindet, da das Fahrzeug in Bewegung ist. Alle OBD-II-Nachrichten würden in Folge verworfen.

Verwendung mehrerer GuardKnox-Cybersicherheitsgeräte

GuardKnox implementiert die Communication Lockdown™-Technologie auf zwei verschiedenen Hardware-Sets oder Plattformen:

- GuardKnox Central Secured Network Orchestrator™ Gateway ECU/Domain Controller

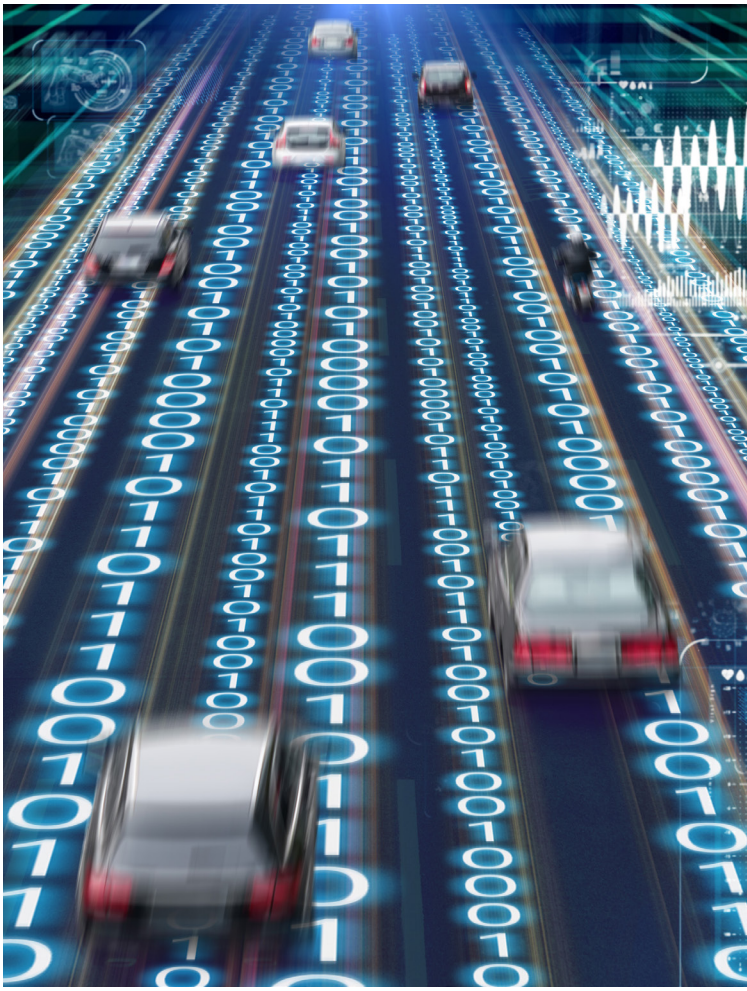
  Dieses Gerät bietet als sichere Plattform für jede Kommunikation und Anwendung einen zentralen Schutz des internen Fahrzeugnetzwerks und wird von OEMs während des Herstellungsprozesses installiert.

- GuardKnox Local Secured Network Orchestrator™ Controller

  Dieses Gerät schützt ein einzelnes Steuergerät oder eine Schnittstelle vor Datenverkehr von außen. Es wird vom Aftermarket als Cybersicherheitsmaßnahme installiert oder als Teil eines von Tier-1- oder Tier-2-Zulieferern erstellten Fahrzeug-Upgrades integriert. Die lokale Lösung kann als mobiles Internet-Gateway, Bluetooth-Gateway oder als Gateway für jede andere drahtlose Verbindung dienen.

Die Installation von mehr als einem Gerät kann erforderlich sein, wenn beispielsweise ein Aftermarket-Infotainmentsystem mit einem lokalen SNO-Controller in ein Fahrzeug eingebaut werden soll, das bereits seitens des Herstellers durch ein zentrales SNO-Gateway geschützt wird.

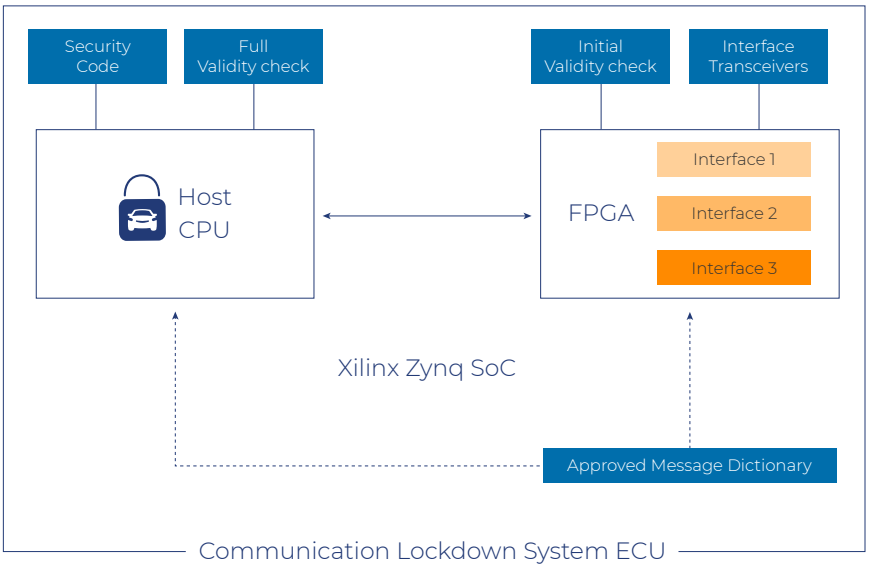
Obwohl jedes Gerät nur einen Teil des Netzwerkverkehrs im Blick hat – entweder den internen Netzwerkverkehr oder den ein- und ausgehenden externen Verkehr – arbeiten sie synergetisch zusammen, indem sie miteinander Metadaten über den weitergeleiteten oder verworfenen Verkehr austauschen. Durch diese patentierte Zusammenarbeit wird die Effektivität der Communication-Lockdown™-Technologie weiter gesteigert.



Flexible Hardware-Implementierung auf FPGAs

Die Verwendung von Field Programmable Gate Arrays (FPGAs) anstelle von ASICs oder anderen Prozessoren erhöht die Leistung und Zuverlässigkeit der GuardKnox Communication Lockdown™-Methode.

Programmierbare Logik ermöglicht die Virtualisierung oder Verwendung von virtuellen Prozessoren (Prozessoren, die einer virtuellen Maschine zugeordnet sind), um die Leistung zu steigern und leichzeitig die Software auf einem einzigen Steuergerät aufzuteilen.



Dies ermöglicht eine nahtlose Integration und flexible Aufteilung zwischen Hard- und Software.

Darüber hinaus kann die Systemverantwortung zwischen dem verarbeitenden System (z. B. Software) und der programmierbaren Logik (z. B. Hardware) verteilt werden. Sowohl die Software als auch die Hardware können ganz oder teilweise rekonfiguriert werden.

In der GurardKnox Implementierung der Lockdown™-Technologie werden die Datenanalyse und Entscheidungen über Weiterleitung oder Verwerfen einer Nachricht sowie die busspezifische Protokolllogik direkt im FPGA implementiert. Durch diese hardwarebasierte Inspektion mit reduzierter Abhängigkeit von Software erhöht sich sowohl die Durchleitungsgeschwindigkeit als auch die Zuverlässigkeit der Kommunikation.

Zusätzlich ermöglicht die Reprogrammierbarkeit von logischen Verbindungen und Rechenelementen nach der ECU-Produktion, dass rechnerisch anspruchsvolle neue oder aktualisierte Software verarbeitet werden kann, ohne die Hardware ersetzen zu müssen. Dies erhöht die Nutzungsdauer der ECU und reduziert deren Gesamtkosten über die gesamte Lebensdauer der Fahrzeugproduktion.

Integration der Cybersicherheitslösungen von GuardKnox

Die Communication Lockdown™-Technologie von GuardKnox wird auf die individuellen Bedürfnisse jedes Herstellers und jeder Applikation im Fahrzeug zugeschnitten. Die Integration erfordert lediglich die technischen Spezifikationen (Kommunikationsmatrix, Datenbank der Busnachrichten, funktionale Spezifikationen).

Der Prozess umfasst folgende Schritte:

1. Der OEM liefert GuardKnox die technischen Spezifikationen (Kommunikationsmatrix, Datenbank der Busnachrichten, funktionale Spezifikationen)
2. GuardKnox erstellt ein Kommunikationsschema aller Fahrzeugdaten
3. Der OEM überprüft und genehmigt das Schema
4. Das Schema wird vom OEM evaluiert und die Sicherheit zertifiziert
5. Das Schema wird in die Firmware der jeweiligen ECU geschrieben
6. GuardKnox produziert die kundenspezifisch angepasste ECU
7. Das Steuergerät wird direkt an den OEM geliefert

Zusammenfassung

Die Communication Lockdown™-Technologie von GuardKnox bietet einen patentierten Cybersicherheitsansatz, der auch den hohen Anforderungen vernetzter Fahrzeuge gerecht wird. Sie beruht auf den gleichen Methoden, wie sie zur Abwehr von Cyberangriffen auf Waffensysteme wie Kampfflugzeuge oder Raketenabwehrsysteme verwendet werden. GuardKnox stellt sicher, dass das Fahrzeugnetzwerk permanent gemäß den Vorgaben des Herstellers arbeitet.

GuardKnox bietet ein deterministisches Cybersicherheitskonzept, ein Zero-Trust-Modell, das keinen Spielraum für unvorhergesehene Kommunikation im Fahrzeugnetzwerk lässt, da alle Daten über Routing-, Inhalts- und Kontextschichten geleitet werden. Unplausible Daten werden vom GuardKnox-System sofort abgelehnt. Dabei wird weder eine Verbindung nach außen benötigt noch sind manuelle Eingriffe oder regelmäßige Software-Updates notwendig. Kurz gesagt, GuardKnox ist eine einzigartige Lösung für die heutigen „Computer auf Rädern“.

Über GuardKnox

GuardKnox bietet Automobilherstellern umfassende Cybersecurity-Lösungen, die perfekt in automobile Wertschöpfungsketten passen. Die einzigartige, von GuardKnox entwickelte Lockdown™-Methode, wurde bereits erfolgreich in Israels Raketenabwehrsystemen Iron Dome und Arrow III sowie der israelischen Version des US-Kampfjets F-35 eingesetzt. GuardKnox entwickelte ein deterministisches Cybersicherheitskonzept, ein Zero-Trust-Modell, das keinen Spielraum für unvorhergesehene Kommunikation im Fahrzeugnetzwerk lässt, da alle Daten über Routing-, Inhalts- und Kontextschichten geleitet werden. Unplausible Daten werden vom GuardKnox-System sofort abgelehnt.

Die GuardKnox-Familie bietet höchste Sicherheit mit einem zentralen Gateway-Steuergerät, einem sicheren Domain Controller und einem lokalen SNO für extern angeschlossene Steuergeräte.

- Infotainment- und Nachrichten-Apps, um ein Fahrerlebnis zu ermöglichen, das kommerziellen Flugreisen ähnelt (da Fahrzeuge autonomer und Fahrer zu Passagieren werden).
- Produktivitäts-Apps für die Büroarbeit, das Bezahlen von Rechnungen oder zum Bestellen von Lebensmitteln.
- KI-gestützte virtuelle Assistenten zur Koordination von Terminen, zur Reservierung von Restaurants oder zur Planung von Werkstattbesuchen.
- Anpassung der Leistung des Fahrzeugs an den persönlichen Geschmack oder die Bedürfnisse – vom sportlichen Handling über das Fahren bei schlechter Witterung bis hin zum Ziehen von Anhängern.
- Concierge-Services und Notfalldienste wie beispielsweise BMW ConnectedDrive.

Die patentierte serviceorientierte Architektur (SOA) von GuardKnox ermöglicht die Individualisierung des Fahrzeugs und sichert den Automobilherstellern eine leistungsstarke Datenspeicherung und -verarbeitung an Bord.

SOA ermöglicht eine einheitliche Kommunikation sowie Zugriffskontrolle und Service-Level-Partitionierung.

Die GuardKnox-Lösungen bilden die Grundlage für zusätzliche Konnektivität, Services und Personalisierung - und schaffen so ein verbessertes Endbenutzererlebnis und umsatzfördernde Möglichkeiten für Hersteller.

Sie fügen sich nahtlos in jedes Fahrzeug, die automobile Wertschöpfungskette und den Produktionsprozess ein.

www.guardknox.com | info@guardknox.com | 2 Hahazon St. PO Box 320, Ramla, Israel 7210202