Fraunhofer IPMS

Whitepaper

CANsec – Security für die dritte Generation des CAN-Bus

Inhalt

1. Zonale E/E-Architektur und Auswirkungen auf die Cybersecurity im Automobil

Die Elektrische/Elektronische Architektur (E/E-Architektur) des Fahrzeugs durchläuft derzeit eine Veränderung von einer domänenbasierten zu einer zonalen Architektur und durchbricht so die klare Trennung in Funktionsbereiche, wie Infotainment, Chassis Control oder Powertrain. Im zonalen Ansatz werden die Endgeräte nicht gemäß ihrer Funktion, sondern nach ihrer optimalen Verortung innerhalb des Fahrzeugs verteilt und miteinander vernetzt, was die Länge und das Gewicht des Kabelbaums signifikant verringern soll. Dieser Wandel führt zu einer deutlich höheren Flexibilität, denn bisherige Konzepte erforderten für jede Fahrzeugfunktion ein eigenes elektronisches Steuergerät. Funktionen können so in weniger Steuergeräten zusammengefasst werden, weswegen auch die Interoperabilität und Performanz der einzelnen Geräte im Auto steigen wird. Die Nutzung einer Middleware, die als ein software-basiertes Overlay über die Steuergeräte hinweg dient, soll die funktionsübergreifende Kommunikation erleichtern, ein Konzept, das auch als das software-definierte Fahrzeug bezeichnet wird. Domänenspezifische Datenpfade werden durch eine Infrastruktur ersetzt, in der Datenpakete an jeden anderen Punkt des Netzes weitergeleitet werden können. Die Architektur bietet viele Vorteile hinsichtlich Kosten und Gewichtseinsparungen, birgt aber auch Potential für neue Sicherheitslücken, wie bspw. in den etablierten signalbasierten Kommunikationsprotokollen wie dem CAN-Bus.

Der CAN-Bus ist seit mehr als 20 Jahren ein zentrales Element in der E/E-Architektur des Fahrzeugs und ermöglicht die serielle Übertragung von Daten zwischen Steuergeräten und Sensoren in Echtzeit. Obwohl er in vielen Fahrzeugen vertreten ist, ist er anfällig für Sicherheitsbedrohungen. Entwickelt wurde das Protokoll erstmalig in den 80ern, zu dieser Zeit wurden keine Cyber-Bedrohungen berücksichtigt, denn Vernetzung und Konnektivität waren noch keine relevanten Themen.
Später als der Bedarf an sicheren Lösungen sichtbar wurde, etablierte die Automotive Open System Architecture (AUTOSAR) eine Lösung für die signalbasierte Kommunikation im Fahrzeug. Das Secure-Onboard-Communication (SecOC) Modul arbeitet allerdings auf den höheren Schichten des OSI-Modells und bringt so bei den einzelnen Aufgaben viel Software-Overhead mit sich, der zu einer hohen CPU-Auslastung führen kann. Security-Protokolle, die auf den unteren Schichten arbeiten und Absicherung in Echtzeit garantieren, bieten daher eine sinnvolle Ergänzung im Security-Konzept des Fahrzeugs. Eine Lösung für die Absicherung der CAN-Kommunikation ist CANsec. CANsec ist Teil der dritten CAN-Bus Generation CAN XL und lässt die Authentifizierung, Verschlüsselung und die Integritätsprüfung von CAN-Rahmentelegrammen (engl. CAN Frame) zu.

2. Die dritte Generation des CAN-Bus – CAN XL

CAN XL basiert auf den in der ISO 11898-1:2015 - Straßenfahrzeuge – Controller Area Network (CAN) spezifizierten Konzepten. Die Merkmale des CAN XL Protokolls werden seit 2018 von der CAN in Automation Special Interest Group (CiA SIG) definiert und sind noch nicht vollständig abgeschlossen. Eine der wichtigsten Motivationen für die Entwicklung ist es die Bitratenlücke zwischen CAN/CAN FD und Ethernet 100Base-T1 in zukünftigen Bordnetzarchitekturen von Fahrzeugen zu schließen.
Seit Dezember 2018 spezifiziert die CiA SIG (Special Interest Group) die Eigenschaften des CAN XL-Protokolls in den folgenden Dokumenten:

- CiA 610: CAN XL - Protocol
- CiA 611: CAN XL - Higher-layer services
- CiA 612: CAN XL - Guidelines and application notes
- CiA 613: CAN XL - Add-on services

Die Hauptmerkmale, im Vergleich zu den vorangegangen Standards Classic CAN und CAN FD, sind die hohe mögliche Bitrate bis 20 Mbit/s, als auch die Nutzdatenlänge von 1 bis 2048 Bytes. Die größere Nutzdatenlänge ermöglicht das Tunneln von Ethernet Frames, womit sowohl signalbasierte Echtzeitkommunikation als auch serviceorientierte Kommunikation über dasselbe Netzwerk möglich sind.

Dafür bietet CAN XL die neuen 8-Bit-Felder SDU-Type und VCID (Virtual CAN Network ID), die es dem CAN-Bus ermöglichen als Backbone-Netzwerk in der zonalen Architektur des Fahrzeugs zu fungieren. SDU-Type gibt das verwendete Protokoll der nächsten OSI-Schicht an, was die Implementierung von Multiprotokoll-Stacks ermöglicht, eine Notwendigkeit, wenn unterschiedliche Anwendungen auf einem Kabel laufen sollen. Das VCID-Field erlaubt die Vergabe von virtuellen CAN IDs. Innerhalb eines einzigen CAN XL Netzwerk Segments sind so bis zu 256 virtuelle Netzwerke definierbar. Damit lassen sich zur Arbeitserleichterung logische Strukturen aufbauen.

Neu ist außerdem die Aufteilung der Funktionen Prioritätszuteilung und Adressierung. CAN XL besitzt nun einen 11-Bit-Identifier und ein 32-Bit-Akzeptanzfeld, das eine Knotenadresse oder einen Inhaltsanzeiger enthalten kann. In Classical CAN bzw. CAN FD ist das alles im Identifier enthalten.

Das Buszugriffsverfahren hat sich nicht verändert, es kommt nach wie vor das Carrier Sense Multiple Access / Collision Resolution) (CSMA/CR-Verfahren) zum Einsatz, das ein eindeutiges Prioritätskonzept zur Verfügung stellt. Bei der physikalischen Übertragung zwischen Controller und Transceiver kann der Anwender die übliche Non-Return-to-Zero-Kodierung (NRZ) oder die neue Pulse-Width Modulation (PWM)-Codierung verwenden. Mit der PWM-Codierung sind die höheren Bitraten bis 20 Mbit/s in der Datenphase erreichbar.

Die CiA spezifiziert zudem einige neue Funktionen. Das Fragmentieren des Daten-Frames lässt eine stückweise Übertragung des Frames zu, womit sich die Netzwerk-Latenzzeit optimieren lässt. Eine weitere Funktion ist das Security-Protokoll CANsec, zur Vermeidung von unberechtigten Zugriffen auf die Datensicherungsschicht.

CAN XL im Überblick

- Skalierbarer Datendurchsatz mit einer Bitrate bis 20 Mbps
- Skalierbare Nutzdatenlänge bis 2048 Bytes
- Mapping und Tunneling von Ethernet-Frames möglich
- Kompatibel zu CAN FD
- Getrennte Prioritätsfunktionen und Adressierung
- Unterstützung virtueller CAN-Netzwerke und Service Data Unit Type (SDT)
- Bereitstellung des Sicherheitsprotokolls CANsec
- Fragmentierung von CAN XL-Frames für verbesserte Latenzen

3. CAN-Bus Sicherheit

Angriffe wie Spoofing, Sniffing und Replay, Repudiation, Ressource Exhaustion auf das CAN-Netzwerk eines Fahrzeugs sind einfach, insofern keine Maßnahmen dagegen ergriffen werden. Daher gibt es bereits seit einigen Jahren eine Lösung von AUTOSAR für die sichere signalbasierte Kommunikation im Fahrzeug. Das SecOC Modul wird in heutigen E/E-Architekturen bereits umgesetzt. Allerdings agiert SecOC ab Layer 4 und wird in heutigen Netzwerken üblicherweise in Software umgesetzt. SecOC verleiht der CAN-Kommunikation im Auto Integrität, Authentizität und wendet Replay-Attacken ab, allerdings sind die Anforderungen an die Host-CPU-Leistung hoch, da mehrere Softwareschichten erforderlich sind, um das Freshness-Management und die Authentifizierung auszuführen.

Eine ressourcenschonendere Lösung ist das Layer-2 Security-Protokoll CANsec. Die in Vorbereitung befindlichen Standards CiA 613-1 und -2 der CAN in Automation (CiA) erweitern das CAN XL-Protokoll um Sicherheitsfunktionen, wie die Integrität, Authentizität und die Vertraulichkeit von Daten. Die möglichen Angriffe auf ein solches Netzwerk sowie deren Gegenmaßnahmen durch CANsec sind detailliert in Tabelle 1 beschrieben.

Das CANsec Konzept definiert Secure Zones (SZ), in denen teilnehmende Knoten sicher miteinander kommunizieren können. Die Teilnehmer der SZ verfügen über gemeinsame

Threat	Beschreibung	Gegenmaßnahmen (CANsec)
Spoofing	Angreifer sendet einen CAN XL Frame und gibt sich als ein bestimmter Knoten im Netzwerk aus.	Alle veränderbaren Felder im CAN XL Frame werden mit einem gemeinsamen geheimen Schlüssel authentifiziert.
Sniffing	Angreifer fängt den Datenverkehr ab, um Informationen über die Architektur zu erhalten.	Verschlüsselung der Nutzdatenfelder im CAN XL Frame.
Replay	Angreifer gibt vorher abgefangene Frames wieder, um die Steuergeräte zu einer Aktion wie bspw. das Türöffnen zu veranlassen.	Alternierender Freshness-Wert innerhalb der Frame-Authentifizierung bei jeder Übertragung.
Repudiation	Angreifer fälscht einen Frame. Empfänger hat keine Möglichkeit den Sender zu erkennen.	Der Schlüssel ist nur den berechtigten Kommunikationspartnern bekannt. Wenn ein Frame mit einem gültigen Authentifizierungs-Tag geschützt wird, ist davon auszugehen, dass einer der Schlüsseleigentümer der Sender des Frames war.
Ressource Exhaustion	Angreifer sendet viele aufeinanderfolgende ungültig authentifizierte Frames, um die CPU des Empfängers mit Authentifizierungsaufgaben zu überlasten.	Verlagerung der Authentifizierungsvorgangs zur CAN XL Hardware, um Vorgang in-line im Empfangsfluss durchführen zu können. CPU kann entscheiden, ob ein Frame empfangen oder abgelehnt werden soll.
Denial of Service	Angreifer sendet kontinuierlich 0-ID Nachrichten, und vermeidet so, dass die Arbitration von anderen Teilnehmern gewonnen werden kann, was zur Beeinträchtigung von Funktionen führen kann.	-

Tabelle 1: Threat Model CAN XL Bus

Informationen, um Frames untereinander authentifiziert und bei Bedarf verschlüsselt zu übertragen. Knoten außerhalb der SZ haben diese Information nicht und können damit keine Frames einschleusen oder verschlüsselte Frames lesen. Durch die Strukturierung wird auch das Key-Management des Netzwerks erleichtert.

Teilnehmer in einer SZ können in sogenannten Secure Channels (SC) miteinander kommunizieren, wie in Abbildung 1 dargestellt. Knoten A, B und C können sicher miteinander kommunizieren, während Knoten D außen vor ist, und keine verschlüsselten Frames lesen kann. Jeder der SC hat einen einzigartigen Identifier (Secure Channel Identifier, kurz: SCI), der Teil des CANsec Headers ist.

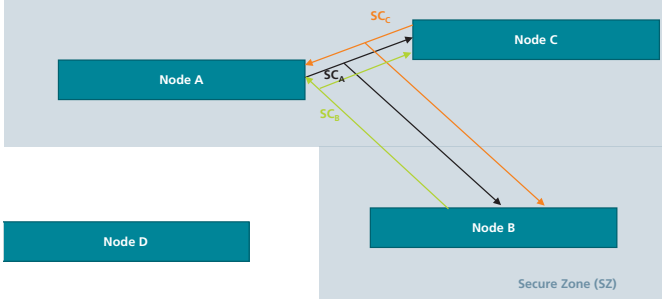

Abbildung 1: CANsec Secure Zone (SZ) Konzept

Wie in Abbildung 2 dargestellt, ist CANsec im OSI-Modell in der Sicherungsschicht (Layer2) und angesiedelt. Aus der Anwendungsschicht sind initiale Daten wie der Schlüssel, Cipher Mode (CM) und ein initialer Freshness Value (FV) notwendig. Das CANsec Modul nutzt als Input den CAN XL LLC Frame, die obere Subschicht des Datenlink-Layers.

Durch das Setzen des Simple/Extended Content Bit (SEC) im CAN XL Header wird angezeigt, dass sich eine Erweiterung im Datenbereich des CAN XL Frames befindet, wodurch der Datenbereich des CAN XL Frames entsprechend erweitert wird. Der eingefügte CANsec Header beginnt mit einem Identifier der zeigt um welches Add-on es sich handelt. Der Identifier steht in diesem Falle für die ID CANsec, es könnte aber auch ein anderes höhergelegenes Schichtprotokolle enthalten sein. Weitere CAN XL Erweiterungen, die im Standard als „Add-on Functions“ beschrieben werden, können außerdem kaskadiert ausgeführt werden. Im Falle eines CANsec Frames wird die ursprüngliche Nutzlast des Nutzers um den CANsec-Header am Anfang und den Integrity Check Value (ICV) am Ende der Nutzlast erweitert. Der ICV wird auf Basis eines Nachrichtenauthentifizierungsalgorithmus generiert, der auf Werte des CAN XL Header, auf alle Werte des CANsec Headers und der Nutzdaten zurückgreift, also auf Werte über den gesamten LLC Frame hinweg. Der CANsec Header besteht aus der Cipher Control Information (CCI), dass die Versionsnummer (VN) des CANsec Protokolls und den Cipher Mode (CM) enthält.

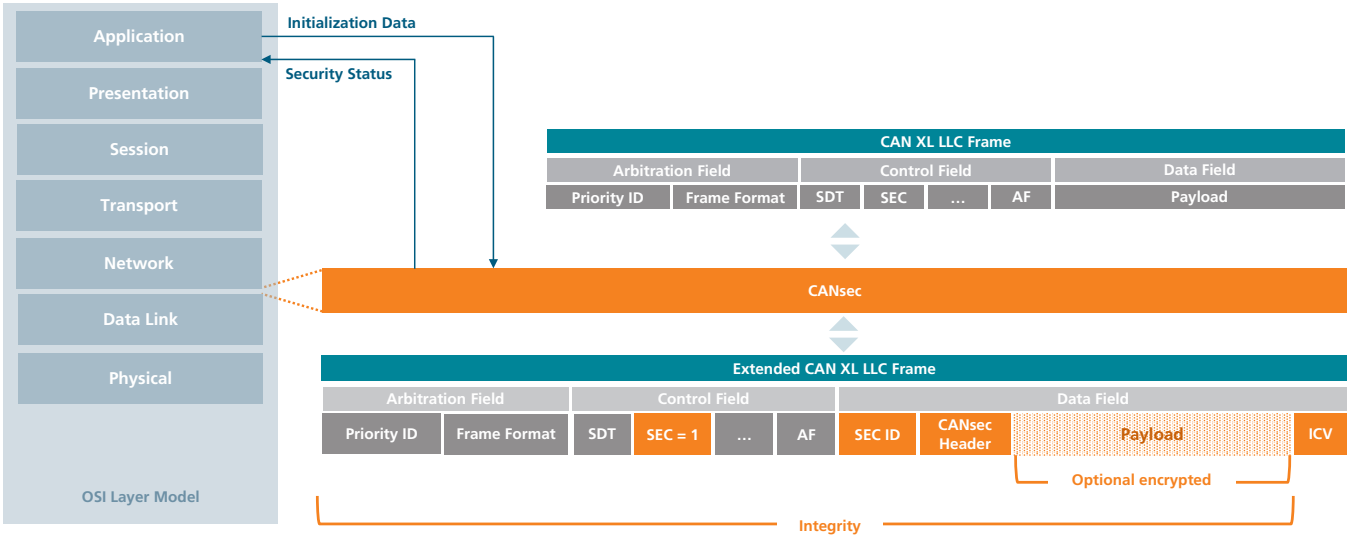

Abbildung 2: CANsec Frame Format und Einordnung im OSI Layer Modell

Der CM zeigt an, ob der Frame lediglich authentifiziert, oder authentifiziert und verschlüsselt ist. Darauf folgt der Secure Channel Identifier (SCI), der gemeinsam mit der Assoziation Number (AN) den zu verwendenden Schlüsselsatz aufzeigt. CANsec nutzt außerdem einen Freshness Value (FV), um Replay Attacken zu vermeiden. Ein weiterer Zweck des FV ist es dem Verschlüsselungsalgorithmus einen initialen Wert für die weitere Verarbeitung zu liefern. Das FV selbst ist nicht geheim, jedoch darf aus kryptographischen Gründen jeder Initialisierungswert nur einmal mit einem Schlüssel verwendet werden. Daher ist nach 2^{32} FV der Schlüssel zu tauschen.

Proof of Concept – CANsec-Performanztest

Um die Performanz hinsichtlich der Übertragungsdauer einer CANsec Implementierung zu untersuchen hat das Fraunhofer IPMS ein Proof of Concept (PoC) durchgeführt. Für das PoC wurde der eigene IP-Core CAN-CTRL verwendet, der neben den CAN-Varianten CAN 2.0 und CAN FD auch eine Lösung für CAN XL bietet. Als CANsec Controller kommt der IPMS CAN-SEC IP-Core zum Einsatz. Beide IP-Cores werden, wie in Abbildung 3 dargestellt, als ein memory-mapped device an den Bus eines Hostsystems, beispielsweise an einen Mikrocontroller, angeschlossen. Das Hostsystem legt Frames in den Pufferspeicher des CAN-CTRL ab, der die Daten anschließend CAN-konform überträgt und sie abschließend für das Hostsystem abholbereit in den Pufferspeicher legt. Über Parameter können mehrere Pufferspeicher zum Senden und Empfangen bereitgestellt werden, so dass das Hostsystem kontinuierlich neue Daten bereitstellen und auswerten kann. So kann ein kontinuierlicher Datenstrom bereitgestellt werden. Der CAN-SEC IP-Core fügt die zusätzlichen Informationen in den Pufferspeicher ein, und authentifiziert und verschlüsselt die Daten. Auf Empfängerseite wird der Frame ebenfalls in einem Pufferspeicher verifiziert und wieder in die ursprüngliche Form konvertiert, wobei seitens des CAN-CTRL

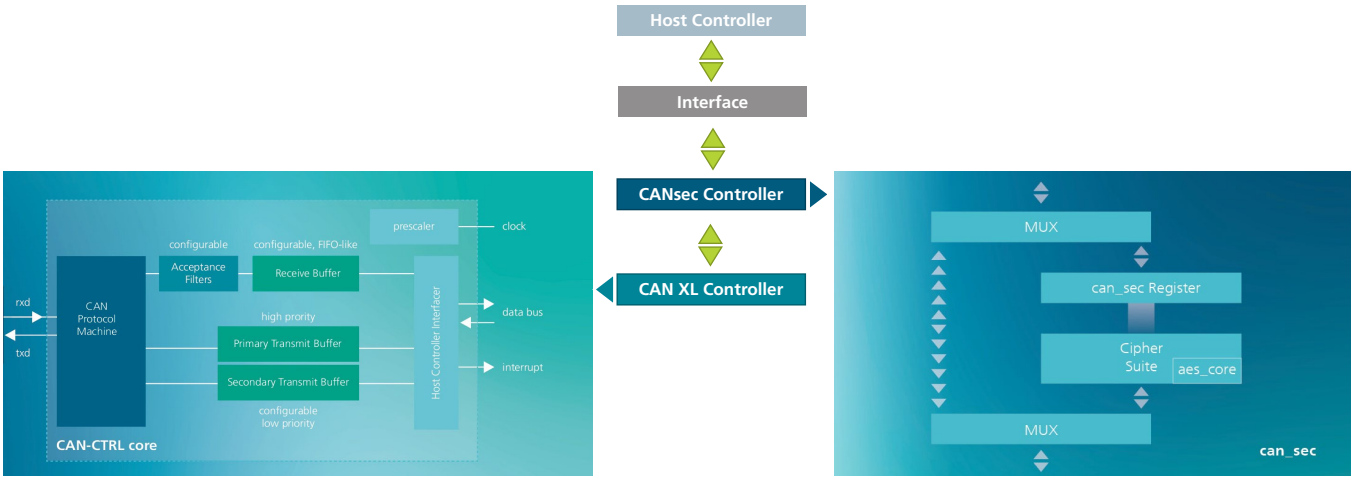

Abbildung 3: Proof of Concept mit Fraunhofer CAN-SEC und CAN-CTRL IP Core

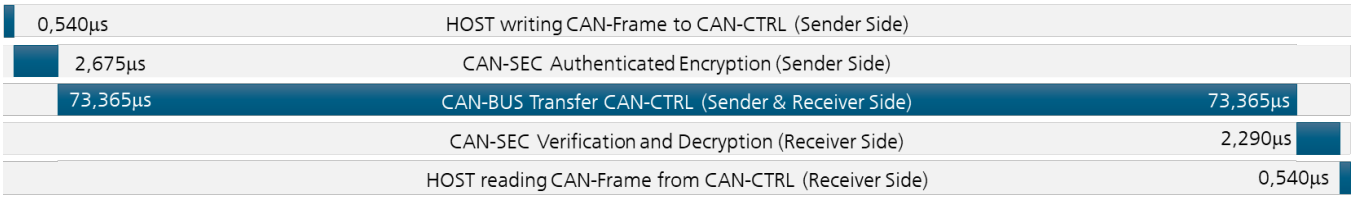

Abbildung 4: Ablauf CANsec-Übertragung

IP Cores und CAN-SEC IP Cores jeweils derselbe Pufferspeicher verwendet werden kann, so dass keine zusätzlichen Datentransferoperationen notwendig sind. Der CAN-SEC kann auch mit einem einfachen Pufferspeicher arbeiten und CANsec Frames von anderen Geräten verarbeiten oder die Authentifizierung und Verschlüsselung mehrere CAN-Knoten im Hostsystem übernehmen. Zur Authentifizierung und wahlweise zur Verschlüsselung des CANsec Frames stellt der CAN-SEC IP-Core den Galois/Counter Mode (GCM) zur Verfügung. Dieser nutzt den Advanced Encryption Standard (AES) als Basis, der im Core mit einer Schlüsselbreite von 128, 192 oder 256 Bit verwendet werden kann.

Beide Cores sind in einer Hardware-Beschreibungssprache verfügbar, die die Implementierung und Verifikation des Moduls im Zieldesign ermöglicht. Durch Synthese kann dieser dann einfach in FPGAs und ASICs implementiert werden.

Im PoC wurden die höchstmögliche Datenrate von 20 MBit und eine Schlüsselbreite von 256 Bit gewählt, was dem Worst-Case-Szenario entspricht. Für das Hostsystem wurde eine Taktfrequenz von 200 MHz gewählt. Da neben Nutzdaten-Bytes auch Header-Bytes übertragen werden, ist die Nutzdatenrate geringer als die Übertragungsrate auf den Busleitungen, im gewählten Beispiel entspricht die Nutzdatenrate 14,5 Mbit/s. Zwischen Anzahl der Nutzdaten-Bytes und Datenübertragungszeit besteht eine große Abhängigkeit. Das gilt in anderer Größenordnung auch für die Verarbeitungszeit des CAN-SEC IP Cores.

In Abbildung 4 ist der Ablauf und die zeitliche Dauer der einzelnen Schritte einer CAN-XL-Übertragung unter Verwendung des CAN-CTRL und des CAN-SEC dargestellt. Für die Speicherung der zu übertragenden Daten im Speicher durch das Hostsystem auf Senderseite vergehen ca. 0,5 µs. Anschließend wird der Frame vom CAN-SEC IP Core authentifiziert und verschlüsselt, wofür weitere 2,7 µs in Anspruch genommen werden. Für Senden und Empfangen des Frames werden weitere 73 µs benötigt. Weitere 2,3 µs kostet das Verifizieren und Entschlüsseln auf der Empfängerseite, und weitere 0,5 µs sind für das Abholen des Frames notwendig.

In Abbildung 5 wird die Dauer der Authentifizierung und Verschlüsselung, als auch die Übertragungsdauer des CAN XL Frames in Abhängigkeit von der Nutzdatenlänge dargestellt und miteinander verglichen. Da die Dauer der Authentifizierung und Verschlüsselung kürzer ist als die eigentliche CAN-XL Frame-Verarbeitungszeit kann im Beispiel die maximale Datenrate des CAN-Bus gewährleistet werden. Wenn mehrere Pufferspeicher eingesetzt werden, kann die Übertragung von Host und CAN-SEC bereits vorbereitet werden, während der CAN-CTRL noch den vorhergehenden Frame überträgt, wodurch keine zusätzlichen Wartezeiten (Latenzen) entstehen.

In Abbildung 6 ist ein Beispiel mit zwei aufeinanderfolgenden gleich großen Frames dargestellt, in dem eine kontinuierliche Übertragung gewährleistet ist und keine zusätzliche Latenz durch die Authentifizierung und Verschlüsselung entsteht.

In speziellen Ausnahmefällen kann es zu zusätzlichen Latenzen kommen. Abbildung 7 zeigt zwei aufeinanderfolgende Frames, wovon der erste besonders kurz und der darauffolgende sehr lang ist. In diesem Beispiel tritt zusätzliche Latenz auf, da die Dauer der Authentifizierung größer ist als die Übertragungsdauer des ersten CAN XL Frames. Das beschriebene Verhalten gilt im umgekehrten Fall auch für die Empfängerseite, wenn ein sehr kurzer Frame auf einen sehr langen folgt. Dieser Effekt kann allerdings nur bei Übertragungsgeschwindigkeiten von mehr als 10 Mbit/s auftreten, da nur in diesen Fällen die Übertragung des kürzesten Frames länger dauern kann als die Verschlüsselung des längeren Frames. Für reale Anwendungsszenarien dürfte dieser Fall eher selten auftreten, da der überwiegende Anteil aller Knoten derzeit mit Geschwindigkeiten bis 10 Mbit/s kommuniziert.

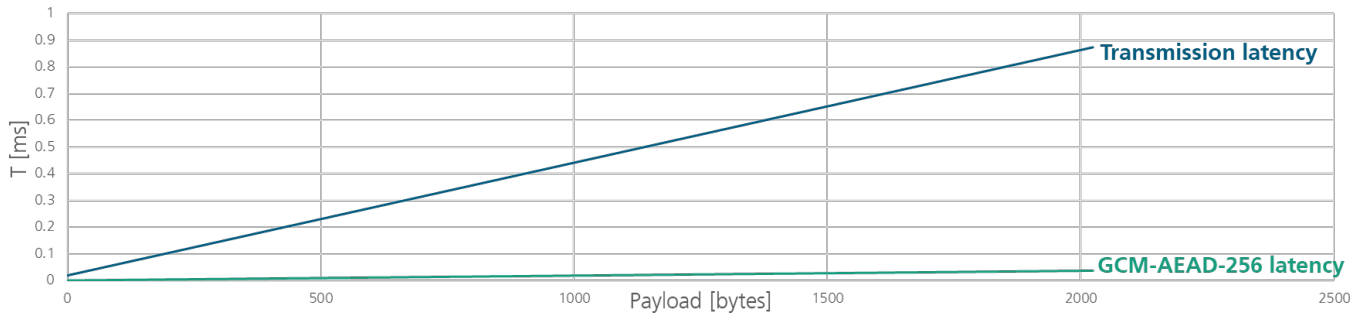

Abbildung 5: Gegenüberstellung Verschlüsselungs- und Übertragungsdauer des CAN XL Frames in Abhängigkeit zur Nutzdatenlänge

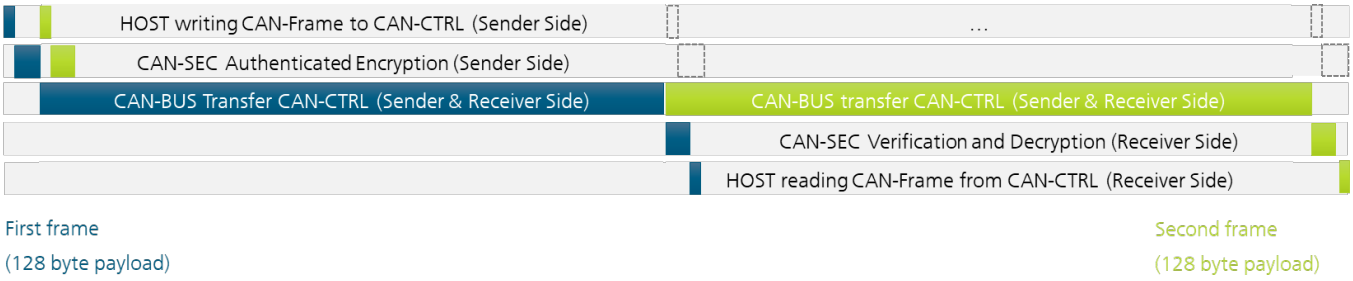

Abbildung 6: Abfolge zweier CANsec-Frames mit gleicher Nutzdatenlänge

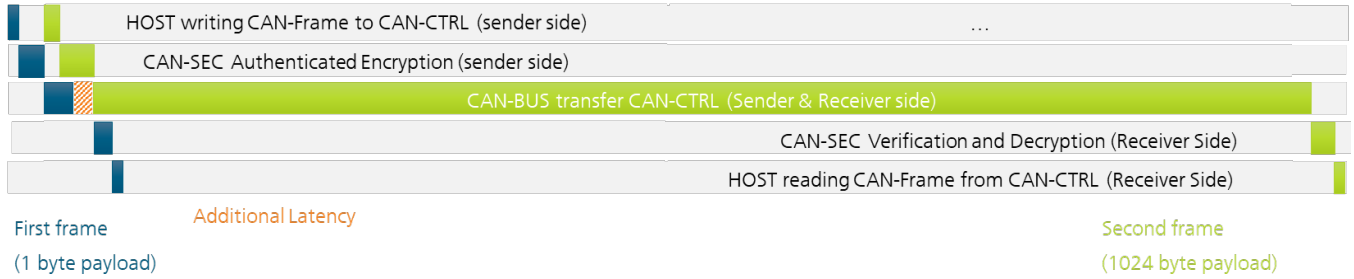

Abbildung 7: Abfolge zweier CANsec-Frames mit sehr unterschiedlicher Nutzdatenlänge

5. Fazit

Zonale E/E-Architekturen liefern dem Software-definierten Fahrzeug der nahen Zukunft die nötige Flexibilität und Performanz, bergen allerdings im Hinblick auf die Cyber-sicherheit neue Herausforderungen. Mit AUTOSAR SecOC existiert bereits eine Lösung, die signalbasierte Kommunikation vor Angriffen schützen kann, allerdings kann diese Lösung mit hoher CPU-Auslastung einhergehen, was insbesondere in zonalen Architekturen zu Schwierigkeiten führen kann.

CANsec arbeitet auf den unteren Schichten und ist eine vergleichsweise ressourcenschonende Lösung zur Absicherung des CAN-Busses gegen die häufigsten Bedrohungen, denen ein CAN-Netzwerk ausgesetzt sein kann. Im einem Proof of Concept konnte gezeigt werden, dass die Verschlüsselung und Authentifizierung von CAN XL Frames ohne Latenzen und bis auf wenige Ausnahmefälle eine Übertragung ohne Verlust an Bandbreite möglich ist.

Über das Fraunhofer IPMS

Die Fraunhofer-Gesellschaft mit Sitz in Deutschland ist die weltweit führende Organisation für anwendungsorientierte Forschung. Mit ihrer Fokussierung auf zukunftsrelevante Schlüsseltechnologien sowie auf die Verwertung der Ergebnisse in Wirtschaft und Industrie spielt sie eine zentrale Rolle im Innovationsprozess. Als eins von 76 Instituten arbeitet das Fraunhofer IPMS an elektronischen, mechanischen und optischen Komponenten und ihrer Integration in miniaturisierte Bauelemente und Systeme. Unser Leistungsangebot reicht von der Konzeption über die Produktentwicklung bis zur Pilotfertigung in eigenen Labor- und Reinräumen.

Das Geschäftsfeld DCC entwickelt und lizensiert IP-Cores wie CAN, LIN, TSN und RISC-V an Unternehmen aus verschiedenen Branchen weltweit und hat dabei einen besonderen Fokus auf die funktionale Sicherheit im Automotive-Bereich nach ISO-26262. Neben der Lizensierung von IP-Cores bietet das Fraunhofer IPMS Integrationssupport, kundenspezifische Anpassungen und Erweiterungen, als auch Analog und Mixed-Signal-Design für spezifische Lösungen an.

Kontakt

Stephan Kube
0351 88 23 - 1211
stephan.kube@ipms.fraunhofer.de

Fraunhofer IPMS
Maria-Reiche-Str. 2
01109 Dresden
www.ipms.fraunhofer.de