www.dspace.com

Absicherung von TLS-geschützter Ethernet-Kommunikation

Ralf Grosse Börger, Björn Müller, Tobias Schaeffer
dSPACE GmbH

Heinfried Cznottka, Dr. Michael Jahnich
achelos GmbH

achelos

YOUR PARTNER IN SIMULATION AND VALIDATION

dSPACE

Seit Mitte 2022 müssen Fahrzeughersteller die Cybersicherheit bei der Zulassung eines neuen Fahrzeugtyps gemäß UNECE 155 nachweisen. Wenig Zeit also, um die Integrität und Authentizität der Kommunikation zwischen Steuergeräten und zwischen Fahrzeug und Back-end-Systemen effektiv abzusichern.

Da bei Ethernet in der Regel TLS (Transport Layer Security) zur Protokollsicherheit zum Einsatz kommt, müssen Testsysteme für die TLS-Implementierung entwickelt werden, die nicht nur funktionale Aspekte absichern, sondern auch auf Schwachstellen in der Cybersicherheit prüfen. Das vorliegende Whitepaper beschreibt eine solche technische Lösung, die in Kooperation von dSPACE und achelos realisiert wurde und die umfassend zur Qualitätssicherung einer TLS geschützten Ethernet-Kommunikation im Fahrzeug eingesetzt werden kann.

Cybersicherheit und die UNECE 155

Seit Jahren gehören fortgeschrittene Fahrerassistenzsysteme (ADAS) und autonomes Fahren (AD) zu den wichtigsten Treibern der Automobilindustrie. Sie sind Meilensteine auf dem Weg zu unfallfreiem Verkehr und autonomen Fahrzeugen und Bestandteil einer umfassenden EU-Strategie, die den Weg zu einer kooperativen, vernetzten und automatisierten Mobilität namens CCAM ebnen soll. Die direkte Kommunikation von Fahrzeug zu Fahrzeug (V2V) oder von Fahrzeug zu Infrastruktur (V2I) – allgemein auch V2X – ist ein entscheidender Baustein und wird das Fahrzeug weiter in ein mobiles IT-Datenzentrum mit vielen eingebetteten Steuergeräten (ECU), Sensoren, Überwachungssystemen, Infotainmentsystemen und drahtlosen Kommunikationsmodulen verwandeln. Die dazu notwendigen Kommunikationsschnittstellen vergrößern aber auch die Angriffsfläche für potenzielle Hacker oder Cyberkriminelle erheblich. Cyberangriffe auf die Konnektivität werden skalierbar und können zu großen negativen Auswirkungen für Automobilhersteller und ihre Zulieferer führen. Die UNECE-Arbeitsgruppe 29 hat daher eine Verordnung zur Cybersicherheit – Regulierung 155 – und zum Software-Update-Management – Regulierung 156 – vorgeschlagen, die Anfang 2021 in Kraft getreten sind und damit einen Paradigmenwechsel in der Automobilindustrie in allen teilnehmenden Mitgliedsstaaten bewirkt. Diese EU-Verordnung verpflichtet die Fahrzeughersteller, für jeden neuen Fahrzeugtyp ein Cybersicherheitsmanagementsystem (CSMS) einzurichten. Darüber hinaus schreibt sie vor, dass identifizierte Risiken gemindert und umfangreiche Tests durchgeführt werden müssen.

Die Richtlinie 155 der UNECE-Arbeitsgruppe 29 ist ab Juli 2022 für alle neuen Fahrtypzulassungen und ab Juli 2024 für alle neuen Fahrzeugzulassungen verpflichtend. Es bleibt also festzustellen, dass neben der funktionalen Sicherheit auch die Cybersicherheit sicherzustellen ist. Während das Vorgehensmodell für die funktionale Sicherheit in der ISO 26262 definiert wurde, ist das Vorgehensmodell für die Cybersicherheit in der neuen ISO 21434 beschrieben; ein Baustein dieser Norm ist die Validierung der Sicherheitsanforderungen.

Ein großer Schwerpunkt der UNECE 155 liegt auf der Prüfung der Cybersicherheit. Die Regelung besagt, dass „die Genehmigungsbehörde oder der Technische Dienst die Typgenehmigung verweigern muss, wenn der Fahrzeughersteller vor der Genehmigung keine angemessenen und ausreichenden Tests durchgeführt hat, um die Wirksamkeit der eingeführten Sicherheitsmaßnahmen zu überprüfen". Ohne angemessene und ausreichende Tests wird ein Fahrzeughersteller keine Typgenehmigung in Bezug auf die Cybersicherheit erhalten. Daher schreibt die Verordnung vor, dass „Verfahren zur Prüfung der Cybersicherheit eines Fahrzeugtyps" festgelegt und Cybersicherheitstests mit einer angemessenen Testabdeckung durchgeführt werden müssen. Da die Cybersicherheitstests darauf abzielen, die Widerstandsfähigkeit gegen böswillige Angriffe zu modellieren und nachzuweisen, stehen auch die Tests und Qualitätskontrollen vor neuen Herausforderungen.
Die UNECE 155 führt weiter aus, welche Schwachstellen und Bedrohungen mindestens bei der Einführung von CSMS berücksichtigt werden müssen, siehe Annex 5. So müssen OEMs die Bedrohungen mindern mit Maßnahmen, die ebenso, wenn auch nur

sehr allgemein, in der UNECE 155 beschrieben sind.
Als Beispiel diene Annex 5: Tabelle A1 Schwachstelle/Bedrohung.
Unter 4.3.2 listet Richtlinie 155 Bedrohungen für Fahrzeuge bezüglich ihrer Kommunikationskanäle auf. So können vom Fahrzeug empfangene Nachrichten, zum Beispiel X2V- oder Diagnosenachrichten, oder innerhalb des Fahrzeugs übertragene Nachrichten schädliche Inhalte enthalten. Dies können zum Beispiel CAN-Nachrichten sein, welche die Fahrzeugsicherheit beeinträchtigen können. Kommunikationskanäle können damit für die unerlaubte Manipulation, Löschung oder sonstige Änderung von Fahrzeugdaten genutzt werden. Auch ermöglichen Kommunikationskanäle die Einspeisung von Daten oder Code in das Fahrzeug.
Basierend auf diesen potenziellen Schwachstellen definiert die Richtlinie 155 abstrakte Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit diesen Fahrzeugkommunikationskanälen, siehe Tabelle B1. So muss das Fahrzeug die Authentizität und Integrität der empfangenen Nachrichten überprüfen. Vertrauliche Daten, die an das Fahrzeug oder vom Fahrzeug übermittelt werden, müssen vor dem Ausspähen geschützt werden.

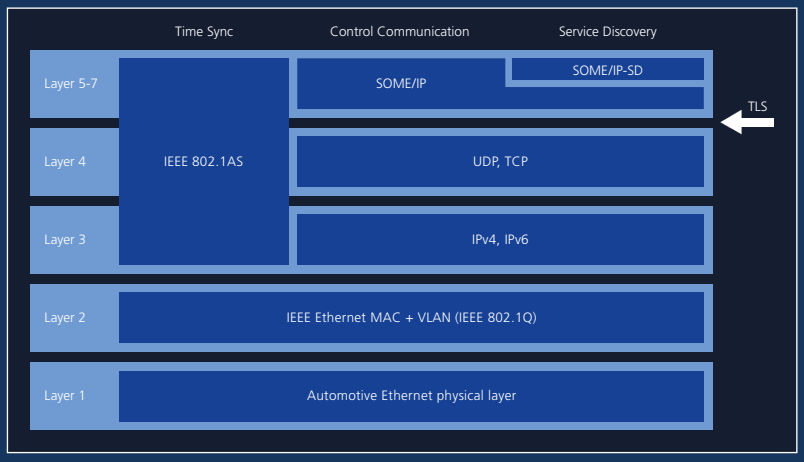
IP-basierte Kommunikation

Seit der ersten Einführung von Ethernet im Fahrzeug für eine dedizierte Funktion sind inzwischen mehr als 10 Jahre vergangen. Seitdem hat sich Ethernet als zentrale Steuergeräte-Vernetzungstechnologie weltweit durchgesetzt. Die Nutzung erstreckt sich dabei über alle Domänen und Anwendungen und geht von Infotainment und Konnektivität über den Antriebsstrang bis zu ADAS- und AD-Anwendungen. Eine aktuelle Steuergerätearchitektur ohne Ethernet als Fahrzeug-Backbone ist dabei gar nicht mehr möglich. Allen Anwendungen gemein ist, dass es sich dabei um

Was ist TLS?

TLS ist die Abkürzung für Transport Layer Security. Es handelt sich dabei um einen Standard bestehend aus mehreren Protokollen, mit dem sich Daten verschlüsselt übertragen lassen. Ziel von TLS ist es, die Authentizität der Kommunikationspartner sowie Integrität und Vertraulichkeit des Datenverkehrs sicherzustellen.
Als Nachfolger des bekannten SSL (Secure Sockets Layer)-Standards wird TLS vielfach in der Internet-Kommunikation per HTTPS (Hypertext Transfer Protocol Secure) zwischen einem Browser und einem Webserver genutzt. Im ISO/OSI-Schichtenmodell wird TLS im Session Layer angesiedelt. Es befindet sich als Zwischenschicht zwischen den Transportprotokollen UDP/TCP und der Anwendungsschicht. Im Fall einer automotiven Nutzung ist die Nutzung somit für das in der Anwendungsschicht darüber befindliche SOME/IP-Protokoll transparent. Obwohl bereits seit einiger Zeit eine Version 1.3 in der RFC 8446 beschrieben ist, findet die Version 1.2 aktuell noch am häufigsten Anwendung in der Automobil- und Internet-Kommunikation.

Mit der AUTOSAR-Version 4.4 wurde im November 2018 auch TLS für die Classic und Adaptive Platform eingeführt. Hier wurde festgelegt, dass TLS ≥ 1.2-Versionen eingesetzt werden sollen. Für Adaptive AUTOSAR ist inzwischen auch eine dTLS-Unterstützung standardisiert worden.



hochbandbreitige Datenübertragungen handelt. Sicherheitskritisch sind jedoch insbesondere die Daten zu ADAS/AD-Anwendungen der Fahrzeuglängs- oder -querdynamik. Da es sich dabei um Applikationen mit bis zu SIL Level 4 handelt, muss die funktionale Sicherheit gemäß ISO 26262 sichergestellt werden. Typische Tests umfassen dabei unter anderem die Veränderung der Eingangsdaten einer Applikation, zum Beispiel mit Hilfe von Restbussimulationen im Rahmen von HIL-Simulationen. Neben Tests mit korrekten Daten (bzgl. des Inhalts sowie des Versendezeitpunkts) werden dabei auch invalide Daten versendet. Typische Fehler, die dabei simuliert werden, sind Maskierungsfehler oder Wiederholungsfehler, die mit Hilfe von zusätzlichen Daten gemäß in AUTOSAR standardisierten End-to-End-Protection-Profilen erkannt werden sollen. Diese Tests dienen also der Sicherstellung der Datenintegrität. Neben der ungewollten verfälschten Übertragung von Eingangsdaten existiert jedoch auch die Möglichkeit, die Daten bewusst zu verändern oder zu manipulieren. In diesem Fall sind Cybersicherheitsmaßnahmen erforderlich, um die Authentizität und Integrität der Daten sicherzustellen. Unter Authentizität wird der vertrauenswürdige Datenaustausch zwischen Sender und Empfänger verstanden. Mit Integrität ist dabei die Prüfung gemeint, ob die übertragenen Daten vollständig und unverändert sind. Zur Sicherstellung der Datenintegrität in automotiven Anwendungen kommen dabei unterschiedlichste Verfahren und Methoden zum Einsatz.

Die bekanntesten Verfahren sind die Folgenden:

- Secure Onboard Communication (SecOC)
- Transport Layer Security (TLS)
- Internet Protocol Security (IPsec)
- Media Access Control Security (MACsec)

Von den oben genannten Verfahren ist SecOC das in der Steuergerätekommunikation etablierteste, da es bereits im Jahre 2015 mit der AUTOSAR-Version 4.2.1 standardisiert wurde. Die Absicherung von SecOC befindet sich dabei gemäß ISO/OSI-Schichtenmodell in der Anwendungsschicht. Hierbei werden zusätzliche verschlüsselte Authentifizierungsinformationen zu den unverschlüsselten Nutzdaten übertragen. Am tiefsten im Schichtenmodell (Layer 2) ist das MACsec-Verfahren gemäß IEEE-Norm 802.1AE angesiedelt. Hierbei findet eine Verschlüsselung zwischen zwei miteinander verbundenen Netzwerkkomponenten statt. Technisch realisiert wird dieses in der Regel über die Transceiver, die miteinander verbunden sind. IPsec und TLS befinden sich zwischen der hardwarenahen MACsec- und der anwendungsnahen SecOC-Absicherung. Während IPsec sich auf Layer 3 abspielt, befindet sich TLS als Zwischenschicht zwischen den

Was ist IKE/IPsec?

IPsec steht für IP Security und bezeichnet eine Familie von Protokollen zur kryptographischen Absicherung der Kommunikation über potenziell unsichere IP-Netze wie das Internet. Ziel von IPsec ist es, die Kommunikationspartner zu authentisieren sowie Integrität und Vertraulichkeit der IP-Pakete, die Payload, sicherzustellen. Die Absicherung der IP-Pakete erfolgt über die Encapsulating Security Payload (ESP), die in RFC 4303 definiert ist. IPsec bedient sich des Internet-Key-Exchange-Protokolls IKE (IKEv2 nach RFC 7296), um die im Protokoll verwendeten kryptographischen Schlüssel automatsch zu vereinbaren und zu verwalten. Im Internet wird IPsec von VPN-Gateways verwendet, um sichere Tunnel zu zentralen Servern zu ermöglichen.

Im ISO/OSI-Schichtenmodell wird IPsec im IP-Layer 3 angesiedelt (Siehe Bild zum ISO/OSI-Schichtenmodell). AUTOSAR-Version 4.5 definiert im Jahr 2019 IPsec sowohl für die Classic und als auch für die Adaptive Platform. Automotive IPsec erfüllt die Anforderungen gemäß AUTOSAR FO R19-11 „Requirements on IPsec Protocol", die sich wiederum an den gängigen IETF-Standards RFC 4301 bis 4303 und RFC 7296 orientieren.

IPsec wird für die Fahrzeugtechnik in AUTOSAR FO R20-11 definiert: Use of IPsec protocol.

Transportprotokollen UDP/TCP und der Anwendungsschicht. Da neben der reinen Kommunikation zwischen Steuergeräten auch die Kommunikation mit dem Back-End immer stärker wird, sind Protokolle und Mechanismen gefragt, die durchgängig genutzt werden können. Hier bietet sich das TLS-Verfahren an, da es bereits seit Jahren erfolgreich für sicherheitskritische Internetanwendungen genutzt wird. Diese Sicherheitsprotokolle implementieren die Echtheit, Integrität und Vertraulichkeit für IP-basierte Kommunikation, wie es seitens der UNECE 155 gefordert wird, und können als „State-of-the-Art" betrachtet werden.

Testen der TLS-Schnittstelle

Wenn Server- und Clientsysteme miteinander kommunizieren, ist die Absicherung dieser Verbindungen heute unabdingbar. Der Nachweis, wer mit wem verbunden war oder ist, die Verschlüsselung der übertragenen Daten, damit Dritte diese nicht mitlesen oder verändern können, muss jederzeit erbracht werden können. Diese Netzwerkverbindungen nutzen kryptographische Technologien. Dabei sind die Implementierung sowie der korrekte Einsatz bestehender Bibliotheken eine große Herausforderung. achelos bietet ein leistungsfähiges Instrument, um diese Lücken und Fehler zu finden und dadurch sichere Netzverbindungen aufzubauen.

Beim Testen der TLS-Implementierung müssen folgende Aspekte berücksichtigt werden:

- **Konformität zum Standard:** Die Übereinstimmung des funktionalen Verhaltens sowohl mit den RFC-Standards als auch mit den funktionalen Anforderungen der Automotiv-Anwendung, zum Beispiel gemäß AUTOSAR, muss gewährleistet sein, damit Fahrzeugkomponenten interoperabel miteinander kommunizieren können.
- **Konfiguration:** Die verfügbare Vielfalt an Konfigurationsoptionen ist derart umfangreich, dass sowohl bei der Integration als auch bei der späteren Konfiguration der Fahrzeugkomponente Schlupflöcher für Angreifer entstehen können. Die Überprüfung der Konfiguration sollte sicherstellen, dass die implementiere Konfiguration sicher im Sinne der Anforderungen ist, zum Beispiel AUTOSAR oder BSI-Checklisten (Bundesamt für Sicherheit in der Informationstechnik). Dazu gehören die Protokollversion (kein SSL 3.0, kein TLS 1.0 ...), die eingesetzte Cipher-Suite (keine EXPORT-Cipher-Suites, keine schwachen Verschlüsselungsalgorithmen ...), die kryptographischen Parameter (RSA-Schlüssellänge ≥ 2048 Bit ...) und Protokollerweiterungen (TLS-Komprimierung, Heartbeat ...).
- **Bekannte Schwachstellen:** Die zu testende Fahrzeugkomponente sollte auf bekannte Schwachstellen untersucht werden. Hierzu gehören unter anderem die Angriffe BEAST, Bleichenbacher, CCS, CRIME, DROWN, FREAK, POODLE, ROBOT. Diese Liste ist dynamisch und wird kontinuierlich erweitert, da Angriffe sowohl Gegenstand der Forschung als auch der Hacker-Community sind.
- **Tests auf korrekte Implementierung:** Überprüft werden sollte auch eine robuste Protokollimplementierung, zum Beispiel bei einer Manipulation der Nachrichtenreihenfolge. Die Implementierung muss das eingesetzte Padding auf Korrektheit prüfen, zum Beispiel das Einfügen ungültiger Padding-Werte. Auch sollte getestet werden, dass die zu testende Implementierung eine Constant-Time-Implementierung ist, um zum Beispiel die Lucky-Thirteen-Attacke abwehren zu können.

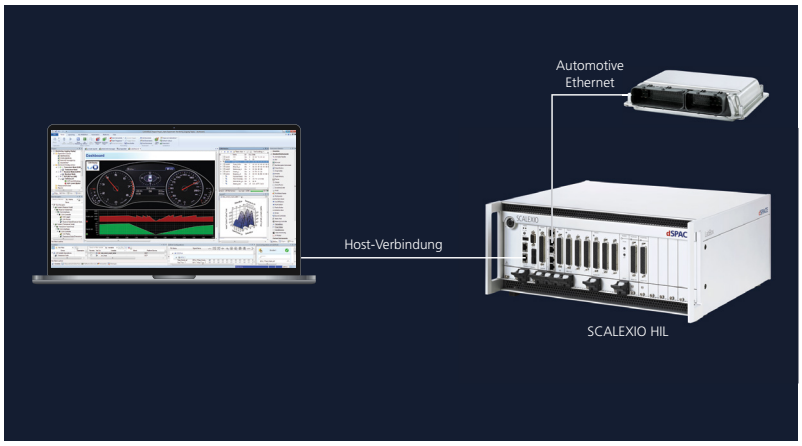
Gegenstand der Prüfung ist der Aufbau der TLS-Verbindung bis zur gegenseitigen Authentisierung, die Reaktion auf fehlerhaftes Verhalten und der Abbau der Verbindung. In diesen Testabläufen werden folgende Szenarien berücksichtigt:

- fehlende oder falsche Kommunikationsteile
- fehlende oder falsche Konfigurationseinstellungen
- fehlerhaftes Schlüsselmaterial
- fehlerhafte Zertifikate
- ungeeignete Cipher-Suiten
- fehlerhafte Reaktion auf Manipulationen
- untypische Fehlermeldungen
- unerwartete Protokolländerungen

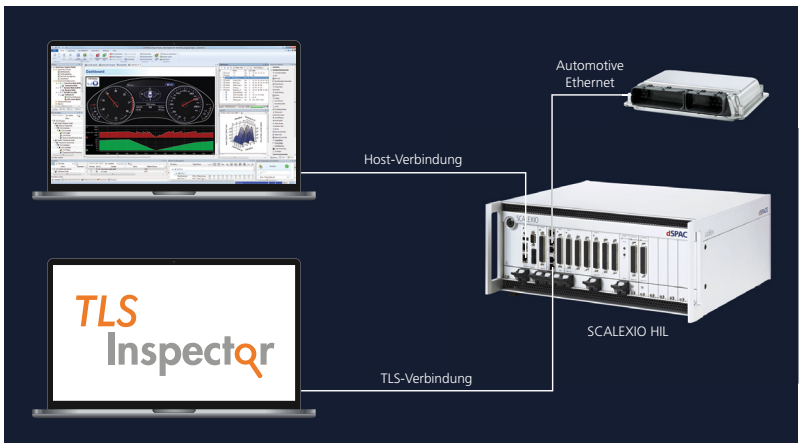
Angriffsszenarien, die bei bestehenden TLS-Verbindungen angreifen, und Seitenkanalangriffe werden aktuell nicht betrachtet. Perspektivisch sind aber auch die Prüfung von Seitenkanälen, die sich zum Beispiel durch Timing-Unterschiede, Fehlermeldung und TCP-Status ergeben, möglich.

Technische Realisierung

Bei einem Hardware-in-the-Loop (HIL)-System ist das reale Steuergerät (Device unter Test, DUT) immer möglichst direkt mit einem SCALEXIO-HIL-Simulator verbunden.
Wenn man neben dem HIL-System noch ein weiteres Testsystem für TLS-Tests an das reale Steuergerät anschließen möchte, ist dies am einfachsten über eine weitere Ethernet-Schnittstelle des SCALEXIO-Simulators möglich. Dazu wird das Steuergerät wie gewohnt an einen Automotive-Ethernet-Port des SCALEXIO-Systems angeschlossen, zum Beispiel 1000BASE-T1.



Standard dSPACE HIL-Aufbau ohne TLS Inspector



Integration des TLS Inspectors

Vollständige TCP-Durchleitung

Das Testsystem **TLS Inspector** von achelos wird dann an einen zweiten Ethernet-Port angeschlossen (Standard Gigabit Ethernet), wobei die Durchleitung des Datenverkehrs wie folgt abläuft:

- Eine Software-Komponente auf dem HIL leitet nur TCP-Verbindungen auf vorher festgelegten TCP-Ports zwischen den beiden Ethernet-Schnittstellen durch.
- Damit sind ein TCP- bzw. TLS-Verbindungsaufbau und eine Datenkommunikation zwischen dem Steuergerät und dem TLS Inspector möglich.
- Für die Durchleitung wird jeweils die exakt gleiche IP- und MAC-Adresse verwendet. Für den TLS Inspector und das Steuergerät erscheint die Verbindung wie eine Direktverbindung.
- Dieser Mechanismus kann so erweitert werden, dass die Restbussimulation des SCALEXIO-Systems zuerst die für den weiteren Ablauf benötigten Voraussetzungen herstellt (Bekanntmachung eines TCP-basierenden Dienstes per SOME-IP Service Discovery) und dann durch das Testsystem von achelos die TLS-spezifischen Testabläufe gestartet werden.

Hiermit können dann diverse Testszenarien für den Auf- und Abbau der TLS-Verbindung geprüft werden. Diese entsprechen den Aspekten, die im Kapitel „Testen der TLS-Schnittstelle“ beschrieben wurden. Die für solche TLS-Szenarien notwendigen Parameter (IP-Adresse, TCP-Port, TLS-Version, Cipher-Suites etc.) können aus der Restbussimulation des SCALEXIO-Systems kommen. Zertifikate werden zumeist nicht fest in das Echtzeitmodell einkompiliert, liegen aber zumindest als separate Dateien auf dem Echtzeitsystem vor.

Da die zur TLS-Kommunikation notwendigen Parameter auf dem Echtzeitsystem vorliegen, könnten sie zur (halb-)automatischen Konfiguration des TLS Inspectors genutzt werden. Damit reduziert sich der Konfigurationsaufwand für den Anwender.

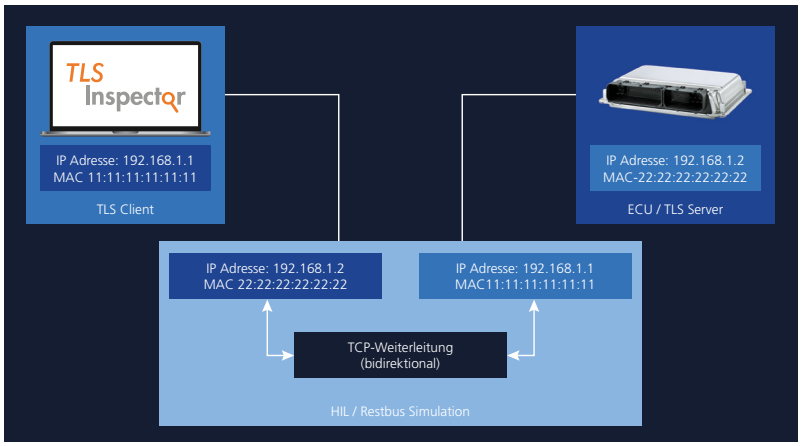
In einer weiteren Ausbaustufe können die vorliegenden Parameter genutzt werden, um eine vollständige Konfiguration des TLS Inspector vorzunehmen. Diese Vorkonfiguration ist insbesondere dann sinnvoll, wenn IP-Adressen und Port-Nummern dynamisch (zur Laufzeit der Simulation) bestimmt werden. Dies kann etwa im Rahmen des SOME-/IP-Service-Discovery-Protokolls vorkommen. In der Praxis stellt sich häufig das Problem, dass der TLS-Client „motiviert“ werden muss, eine TLS-Verbindung zum Server aufzubauen. Die Restbussimulation kann flexibel und automatisiert die notwendigen Vorbedingungen herstellen und den Verbindungsaufbau durch das Steuergerät auslösen.

Da der TLS Inspector weder echtzeitfähig ist noch die Möglichkeit einer Restbussimulation bietet, können jedoch bei der vollständigen TCP-Durchleitung keine realistischen Nutzdaten über die gerade aufgebaute TLS-Verbindung gesendet oder empfangen werden.

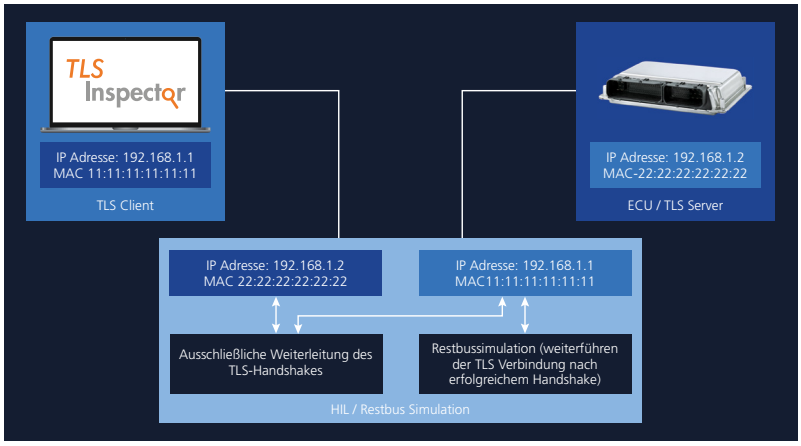
Durchleitung des TLS-Handshakes

Um auch TLS-Verbindungen mit Nutzdaten aus der Restbussimulation zu unterstützten, planen wir als nächsten Schritt die Möglichkeit, den TLS-Verbindungsaufbau (TLS-Handshake) vom TLS Inspector auszuführen, die Verbindung an den dSPACE HIL-Simulator weiterzuleiten und dort mit den Nutzdaten aus der Restbussimulation fortzusetzen.

Dabei wird in der Phase des Verbindungsaufbaus genauso verfahren wie bei der vollständigen TCP-Weiterleitung. Sobald der TLS-Handshake abgeschlossen ist, werden allerdings die Parameter der TLS-Verbindung (ausgehandelte TLS-Version, Cipher-Type, Key etc.) an das HIL-System übergeben. Der HIL-Simulator kann damit die TLS-Verbindung transparent weiterführen, so dass über die aufgebaute TLS-Verbindung die normalen Applikationsdaten gesendet und empfangen werden können. Eine engere Verzahnung zwischen dem SCALEXIO-System und dem TLS Inspector erlaubt es, die Parameter aus der Kommunikationsmatrix (IP-Adressen/Portnummern, TLS-Parameter wie die erlaubten Cipher-Suites) dynamisch an den TLS Inspector zu übergeben. Hiermit sind auch neue Testszenarien denkbar, bei denen in den TLS-Handshake Fehler injiziert werden und deren Auswirkungen auf die weitere Echtzeitkommunikation geprüft werden.



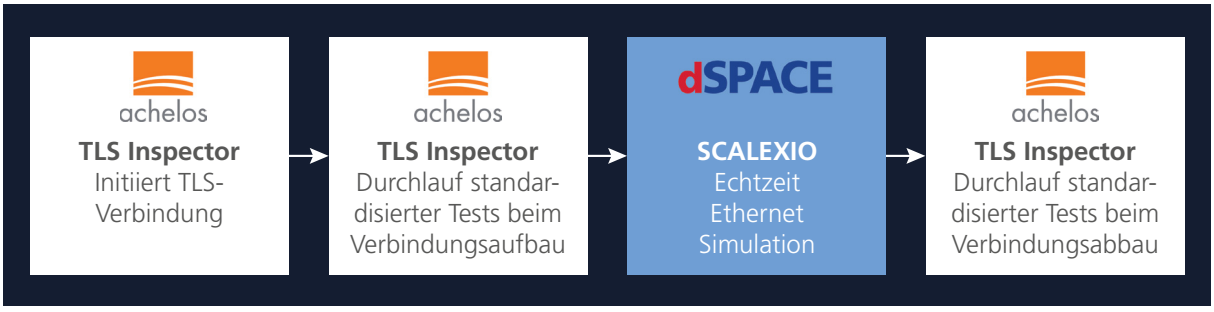
Netzwerktopologie mit IP/MAC-Adressen, Weiterleitung des gesamten TCP-Verkehrs



Netzwerktopologie mit IP/MAC-Adressen, Weiterleitung nur von TLS-Handshake

Zusammenfassung

Mit dem Automotive Ethernet befindet sich die IP-basierte Kommunikation bereits als hochbandbreitige Möglichkeit zur Datenübertragung zwischen zentralen Steuereinheiten im Fahrzeug im Einsatz, insbesondere im ADAS/AD-Anwendungsumfeld. Aufgrund der Forderung nach einer kryptographischen Absicherung solcher Kommunikationskanäle durch die UNECE 155 kommen Sicherheitsprotokolle



Ablauf eines Tests: Nicht echtzeitkritische Anteile (weiß); echtzeitkritische Anteile (blau)

wie TLS als Stand der Technik in Fahrzeugen neuerer Bauart zum Einsatz. Diese cybersicherheitstechnischen Maßnahmen sind letztendlich Bestandteil einer Prüfung zur Fahrzeugtypzulassung. Doch wie prüft man, ob die eingerichteten TLS-Verbindungen sicher implementiert und konfiguriert sind, so dass sie ausreichenden Schutz vor Hacker-Angriffen bieten? In diesem Whitepaper zeigen dSPACE und achelos, wie Steuergeräte mit TLS-basierten Ethernet-Schnittstellen durch den Einsatz des Testwerkzeugs TLS Inspector in Verbindung mit der dSPACE Restbussimulation auf bekannte Schwachstellen, kryptographisch schwache Konfigurationen und Normenkonformität geprüft werden können. In einer Kooperation haben beide Unternehmen ein einsatzfähiges Testsystem prototypisch aufgebaut, das die Experten beider Firmen Kunden und Interessierten gerne näher vorstellen.

Wir freuen uns darauf, die spezifischen Anforderungen des Testens von Cybersicherheit mit Ihnen zu diskutieren und Ihre speziellen Anforderungen kennenzulernen.

Heinfried Cznottka
achelos GmbH
heinfried.cznottka@achelos.de

Dr. Michael Jahnich
achelos GmbH
michael.jahnich@achelos.de

Ralf Grosse Börger
dSPACE GmbH
RGrosseBoerger@dspace.de

Björn Müller
dSPACE GmbH
BjMueller@dspace.de

Tobias Schaeffer
dSPACE GmbH
TSchaeffer@dspace.de

Über achelos

Die achelos GmbH ist ein herstellerunabhängiges Softwareentwicklungs- und Beratungshaus mit Sitz in Paderborn. Der 2008 gegründete Technologieexperte bietet branchenübergreifende Lösungen für sicherheitskritische Anwendungsfelder mit Kernkompetenzen in Embedded Development und Subscription Management. Das Unternehmen entwickelt und betreibt hochspezialisierte Produkte, Lösungen und Dienste für den internationalen Markt. achelos bietet eine umfassende Expertise in Entwicklung, Testing as a Service (TaaS) und Zertifizierung. Neben der ISO-9001- und -27001-Zertifizierung ist der achelos-Entwicklungsstandort in Paderborn nach Common Criteria zertifiziert. Seit Juni 2022 gibt es mit achelos Hungary Kft. einen zusätzlichen Entwicklungsstandort in Budapest (Ungarn).

Weitere Informationen unter *www.achelos.de*.

Über dSPACE

dSPACE ist einer der weltweit führenden Anbieter von Simulations- und Validierungslösungen, die bei der Entwicklung von vernetzten, selbstfahrenden und elektrisch angetriebenen Fahrzeugen eingesetzt werden. Mit dem durchgängigen Lösungsangebot des Unternehmens entwickeln und testen vor allem Automobilhersteller und ihre Zulieferer Software- und Hardware-Komponenten ihrer neuen Fahrzeuge, lange bevor ein neues Modell auf die Straße kommt. Aber nicht nur in der Fahrzeugentwicklung ist dSPACE ein gefragter Partner; auch bei Unternehmen der Luft- und Raumfahrt oder der Industrieautomation verlassen sich Ingenieure auf das Know-how von dSPACE. Das Angebot reicht von durchgängigen Lösungen für die Simulation und Validierung über Engineering- und Consulting-Leistungen bis zu Training und Support. Mit mehr als 2.000 Mitarbeitern weltweit ist dSPACE am Stammsitz in Paderborn, mit drei Projektzentren in Deutschland sowie durch Landesgesellschaften in den USA, Großbritannien, Frankreich, Japan, China, Kroatien und Korea vertreten.

Weitere Informationen unter *www.dspace.com*.

Deutschland
dSPACE GmbH
Rathenaustraße 26
33102 Paderborn
Tel.: +49 5251 1638-0
Fax: +49 5251 16198-0
info@dspace.de

Großbritannien
dSPACE Ltd.
Unit B7 · Beech House
Melbourn Science Park
Melbourn
Hertfordshire · SG8 6HB
Tel.: +44 1763 269 020
Fax: +44 1763 269 021
info@dspace.co.uk

Frankreich
dSPACE SARL
7 Parc Burospace
Route de Gisy
91573 Bièvres Cedex
Tel.: +33 169 355 060
Fax: +33 169 355 061
info@dspace.fr

Kroatien
dSPACE Engineering d.o.o.
Ulica grada Vukovara 284
10000 Zagreb
Tel.: +385 1 4400 700
Fax: +385 1 4400 701
info@dspace.hr

China
dSPACE Mechatronic Control Technology (Shanghai) Co., Ltd.
Unit 01-02,06-09, 19F/L
Middle Xizang Rd. 168
The Headquarters Building
200001 Shanghai
Tel.: +86 21 6391 7666
Fax: +86 21 6391 7445
infochina@dspace.com

Japan
dSPACE Japan K.K.
10F Gotenyama Trust Tower
4-7-35 Kitashinagawa
Shinagawa-ku
Tokyo 140-0001
Tel.: +81 3 5798 5460
Fax: +81 3 5798 5464
info@dspace.jp

USA und Kanada
dSPACE Inc.
50131 Pontiac Trail
Wixom · MI 48393-2020
Tel.: +1 248 295 4700
Fax: +1 248 295 2950
info@dspaceinc.com

Korea
dSPACE Korea Co. Ltd.
16th floor, Dongwon Building
60 Mabang-ro
Seocho-gu
06775 Seoul, Republic of Korea
Tel.: +82 2 570 9100
info@dspace.kr

07/2022