© Softing Automotive

>>> SICHERE REMOTE-DIAGNOSE

Diagnose und Security: Schöne neue Welt

Solange die Diagnose am Fahrzeug mittels einer Kabelverbindung zwischen dem Diagnosetester und dem Diagnose-Interface bzw. dem Fahrzeug erfolgt, kann man davon ausgehen, dass das Diagnosesystem bezüglich unerlaubten Zugriffs halbwegs sicher ist. Kommt aber eine Remote-Verbindung über das Internet als Datenverbindung zum Einsatz, entsteht ein vollkommen anderes Bild. Hackern wird Tür und Tor geöffnet.

Lieb gewonnene Wahrheiten sind so eine Sache – praktisch für eine rasche Beurteilung, aber halt nicht für immer wahr! Genau so einen Fall stellt die heutige Fahrzeugdiagnose dar. Bisher konnte man sich darauf verlassen, dass der Zugang zum Fahrzeug die genormte OBD-Buchse ist, über die mit ebenfalls standardisierten Protokollen kommuniziert wird. Protokolle übrigens, die *by design* keine nennenswerten Sicherheitsanforderungen erfüllen können. Moderne Fahrzeuge öffnen sich allerdings auf vielfältige Art nach außen. V2x (Vehicle to any environment) erfordert drahtlose Kommunikation mit externen Geräten und die heute in allen Fahrzeugen geforderte eCall-Funktionalität integriert verpflichtend eine SIM-Karte im Fahrzeug. Die Forderung nach einer Update-Fähigkeit von Fahrzeug-Software ohne Werkstattbesuch (SOTA – Software over the air) lässt auch im Diagnose-Umfeld drahtlose Verbindungen einziehen.

© Carl Hanser Verlag, München

© Carl Hanser Verlag, München. Vervielfältigungen, auch auszugsweise, sind ohne Lizenzierung durch den Verlag nicht gestattet.

Das Ganze ist allerdings nicht ohne Risiko. Ein unerlaubtes Eindringen in diese drahtlosen Kommunikationswege kann zu erheblichen Schäden führen:

- Personenschäden: Ein Hacker übernimmt die Kontrolle über das Fahrzeug, Personen werden verletzt oder sogar getötet.
- Gewährleistungsfälle: Tuner verstellen *„over the air"*-Fahrzeugdaten so, dass vorzeitig Verschleiß auftritt und der Austausch auf OEM-Kosten erfolgt.
- Datenschutz: Unerlaubte Dritte greifen auf personenbezogenen Daten zu, wobei nach aktueller Rechtsprechung die VIN (Vehicle Identification Number) als personenbezogen gilt.
  Die Strafandrohung liegt bei bis zu 50.000 € – pro Einzelfall.

Ein Beispiel für die möglichen Schadenshöhen ging kürzlich durch die Presse: British Airways hatte kundenbezogenen Daten nicht ausreichend gesichert. Als Strafe wurde von englischen Richtern 200 Mio. € festgesetzt *(Spiegel Online, 08.07.2019).*

Hard- und Software-Reparatur

Ohne Diagnose kommt man heute im Lebenszyklus des Fahrzeugs nicht mehr aus: Die Reparatur eines Netzwerks aus über 100 Steuergeräten, bei denen Funktionen auch noch verteilt sind, ist für den Mechatroniker in der Werkstatt nicht leistbar. In der Produktion gilt entsprechendes: Ob ein Fahrzeug im jeweiligen Bandabschnitt korrekt verbaut ist, kann der Mitarbeiter an der Linie nicht beurteilen. In der Entwicklung sind viele Größen in seriennahen Steuergeräten nicht mehr zugänglich. Für all diese Fälle gilt, dass ein Expertensystem Informationen beurteilen muss, die im Fahrzeug selbst generiert und zur Verfügung gestellt werden. Darüber hinaus werden die Kommunikationsmechanismen, die durch die Diagnose eingeführt sind, auch für das Update der Steuergeräte-Software verwendet. Dies gilt gleichsam in Entwicklung, wo neue Stände zum Testen eingespielt werden, wie in Produktion und im After-Sales-Service, wo dann mit dem aktuellsten Software-Stand quasi eine Reparatur der Software durchgeführt wird.

Für den Zugriff auf das Fahrzeug stehen drei grundsätzliche Klassen von Diensten zur Verfügung:

- *Lesende Dienste* werden verwendet, um Informationen aus dem Fahrzeug auszulesen. Dies können Messwerte, also physikalische Größen, sein, die im Steuergerät zur Kontrolle von Funktionen verwendet werden, oder Fehlerspeichereinträge. Letztere werden durch das Steuergerät eingetragen, sobald bei kontinuierlich laufenden Selbsttestroutinen Auffälligkeiten auftreten. »

© Carl Hanser Verlag, München. Vervielfältigungen, auch auszugsweise, sind ohne Lizenzierung durch den Verlag nicht gestattet.

- *Schreibende Dienste* verändern Inhalte in einer ECU. Dies erfolgt einerseits bei der Programmierung, andererseits bei der Varianten Codierung. Mit dieser wird eine einheitliche Steuergeräte-Software auf unterschiedliches Verhalten adaptiert, das sich beispielsweise aus Länderspezifika (Rechts-/Linkslenker) oder Ausstattungsvarianten ergibt (gleicher Motor mit unterschiedlichen Leistungsstufen).
- *Ausführende Dienste* ermöglichen das Starten von Routinen im Steuergerät. Dazu zählen neben Testfunktionen insbesondere die Ansteuerungen von Aktuatoren wie einem Wischermotor. Mithilfe der Diagnose ist dazu, etwa an Prüfständen, kein Schalter nötig.

Der Zugriff auf das Fahrzeug erfolgt heute in der Regel über zwei Bussysteme: Klassisch über CAN mit dem Protokoll UDS (Unified Diagnostic Services) oder über Ethernet mit Diagnostics over IP (DoIP).

Einfallstore ...

Solange die Diagnose am Fahrzeug lokal (Kabelverbindung) zwischen dem Diagnosetester und dem Diagnose-Interface bzw. dem Fahrzeug erfolgt, kann man davon ausgehen, dass das Diagnosesystem gegen unerlaubte Zugriffe halbwegs sicher ist. Kommt aber eine Remote-Verbindung über das Internet als Datenverbindung zum Einsatz, entsteht ein vollkommen anderes Bild:

Eine Remote-Diagnoseverbindung wird durch den Benutzer nach dem Start der Anwendung und Auswahl des Fahrzeugs mit diesem aufgebaut. Im Allgemeinen wird hierfür das Internet als Transportschicht verwendet. Über diese Verbindung werden dann die entsprechenden Service-Requests an das Fahrzeug gesendet, welches im Gutfall mit den zugehörigen Responses antwortet. Nach Erhalt der angeforderten Daten wertet die Tester-Applikation diese aus und legt sie bei Bedarf z. B. in einer Datenbank ab.

Auf den ersten Blick ein alltägliches Szenario in einem modernen Automotive-Umfeld. Bei genauerer Betrachtung erkennt man jedoch den ersten Angriffspunkt bereits auf der Seite der Tester-Applikation: Verfügt die Tester-Applikation über einen ausreichenden Schutz gegen unerlaubten Zugriff bzw. Hacking? Ein sorgloser Umgang mit Zugangsdaten, wie man es aus dem Büroumfeld kennt, stellt hier ein enormes Risiko dar. Aber auch die beste Absicherung der Diagnosesoftware hilft nichts, wenn die entsprechenden Rechte halbherzig vergeben wurden: Ist der jeweilige Benutzer überhaupt berechtigt, den jeweiligen Dienst auszuführen? Nicht jeder Benutzer sollte Steuergeräte programmieren oder codieren können. In vielen Fällen ist es sinnvoll, die Berechtigungen zunächst auf ausschließlich lesende Dienste einzuschränken und im Bedarfsfall zu klären, ob und wie lange eine Erweiterung der Rechte sinnvoll ist.

Ein weiterer wichtiger Punkt ist die Ablage der ermittelten Daten: Maximaler Schutz der Daten gegen unberechtigten Zugriff ist hier ein Muss! Im Zeitalter von Big-Data stellen diese Daten eines der wichtigsten Angriffsziele für Hacker dar. Bleibt noch die Datenverbindung via Internet zu erwähnen: Die Möglichkeiten eines Angriffs sind hier vielfältig: Beginnend beim Mithören der Kommunikation über die Manipulation der Daten bis hin zur Übernahme der Kommunikationsverbindung ist hier alles denkbar. Die Verhinderung solcher Man-in-the-Middle-Attacken stellt hohe Anforderungen an die Absicherung der Datenverbindung.

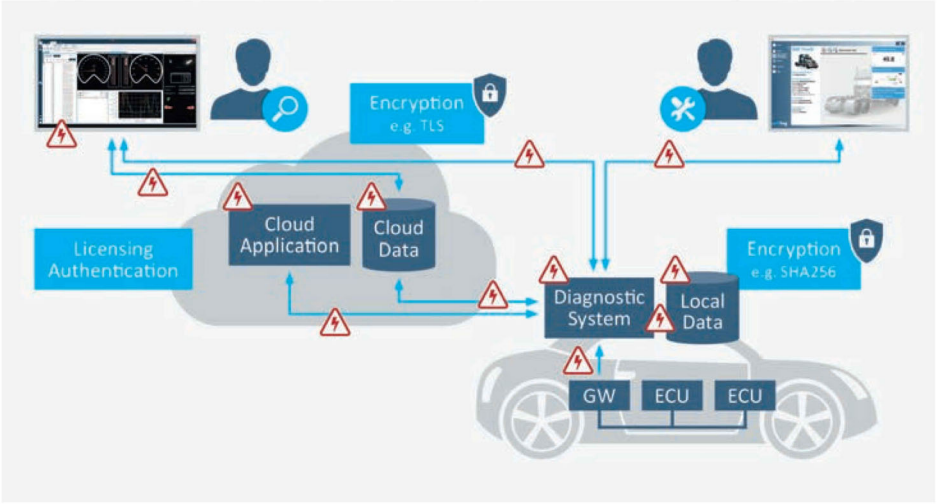

Bild 1: Das Diagnose Ökosystem (© Softing Automotive)

... und wie man sie schließt

Um ein Maximum an Sicherheit zu erreichen, ist eine End2End-Absicherung zwingend erforderlich, wobei diese seitens des Fahrzeuges an der ersten Schnittstelle endet. Ein Diagnosesystem hat keinen Einfluss auf die Kommunikation innerhalb des Fahrzeugs. Die Absicherung in diesem Bereich liegt in der Verantwortung des OEM.

Durch geeignete Zugriffsrechte, einer tragfähigen Lizenzierung sowie die Verwendung von modernen Verschlüsselungsmethoden kann seitens der Diagnose-Applikation sowie der abgelegten Daten ein hohes Maß an Sicherheit erreicht werden. Verschlüsselung ist auch das Keyword für ODX- und OTX-Daten, welche für die Diagnose notwendig sind. Darüber hinaus ist es erforderlich, dass geeignete Prozesse und Tools den Zugriff Unbefugter verhindern.

Für die Absicherung im Bereich der Datenverbindung kommen symmetrische sowie asymmetrische Verschlüsselungsverfahren in Frage. Da beide Verfahren ihre Vor- und Nachteile haben, muss im Einzelfall entschieden werden, welches zum Einsatz kommt. Eine Erhöhung des Sicherheitsniveaus kann durch eine zusätzliche Verschlüsselung auf Protokollebene erreicht werden. Im Falle von UDS, einem der verbreitetsten Diagnoseprotokolle im Automotive-Umfeld, ist dies aufgrund des definierten Standards nicht möglich, für den Newcomer unter den Diagnoseprotokollen ‚DoIP' ist eine TLS-Verschlüsselung als Standard bereits in Vorbereitung.

Bei all diesen Sicherheitsvorkehrungen dürfen jedoch wichtige Aspekte für die Diagnose, wie z. B. die Performance und die Handhabbarkeit, nicht auf der Strecke bleiben.

© Carl Hanser Verlag, München

© Carl Hanser Verlag, München. Vervielfältigungen, auch auszugsweise, sind ohne Lizenzierung durch den Verlag nicht gestattet.

Remotediagnose mit Softing SDE

Die Vielzahl notwendiger Tester-Applikationen verlangt zwangsläufig eine leistungsfähige Diagnose-Middleware, welche Diagnosemethoden einheitlich implementiert und einfach integriert werden kann. Ein Beispiel ist Softing SDE (Smart Diagnostic Engine). In ihr werden industrieerprobte Diagnosekomponenten zur Verarbeitung standardisierter Diagnosedaten (ODX und OTX – ISO 22901 und ISO 13209) mit einer einfach verständlichen API kombiniert. Diese stellt die wichtigsten Diagnosemethoden als Funktionen zur Verfügung, beispielsweise „FehlerspeicherLesen" oder „EcuProgrammieren". Der damit verfolgte Service-orientierte Ansatz ist, im Gegensatz zu den zugrunde liegenden Standards, voll remotefähig und die Kommunikationsstrecken sind über gängige Mechanismen verhältnismäßig einfach abzusichern. Dies nutzen Kunden, um die gleiche Diagnosefunktionalität im Entwicklungstester und an Prüfständen verwenden zu können, die heute in der Regel an anderen Standorten betrieben werden. Die Vorteile der weltweit verteilten Entwicklung werden um ein Effizienzkriterium erweitert.

Fazit

Diagnose und Kommunikation im und um das Fahrzeug werden auch in Zukunft eine immer wichtigere Rolle im Automotive-Umfeld spielen – egal ob in der Entwicklung, der Produktion, während des Betriebes oder im After-Sales-Bereich. Hinzu kommen stetig wachsende Anforderungen an die Sicherheit. Es kommt nun darauf an, beide Bereiche unter einen Hut zu bekommen, sodass auch in Zukunft ein gefahrloser Betrieb und die Diagnose eines Fahrzeuges sichergestellt sind. Denkt man z. B. an das Thema Autonomes Fahren, so wird dies offensichtlich. Umso wichtiger ist es, dass in Zukunft Lösungen zur Verfügung stehen, die auf der einen Seite Aspekte der Sicherheit auf Basis des aktuellen Technologiestandes berücksichtigen und auf der anderen Seite die eigentliche Funktionalität auf komfortable Art zur Verfügung stellen. Security muss ein integraler Bestandteil der Lösung sein, kein AddOn. ■ (oe)

» www.automotive.softing.com

Markus Steffelbauer leitet das Produktmanagement und Marketing bei Softing Automotive und engagiert sich in Standardisierungsgremien.

Günter Fahböck ist Projektmanager bei Softing Automotive und beschäftigt sich mit dem Thema Cybersecurity im Diagnoseumfeld.

© Carl Hanser Verlag, München. Vervielfältigungen, auch auszugsweise, sind ohne Lizenzierung durch den Verlag nicht gestattet.