© Softing Automotive

Security-Herausforderungen bei der Diagnose 4.0

Remote- und Cloud-Diagnoseverfahren werden bei künftigen Fahrzeugreparaturen einen immer höheren Stellenwert haben. Von zentraler Bedeutung bei der Konfiguration entsprechender Konzepte ist die Security, die alle Bereiche des Zugangs und der Kommunikation der Fahrzeugelektronik mit externen Systemen umfassen muss. Softing zeigt im Folgenden, welche Herausforderungen es bei der praktischen Umsetzung gibt und welche Systeme bereits heute verfügbar sind.

AUTOR

Markus Steffelbauer
leitet das Produktmanagement und Marketing bei der Softing Automotive Electronics GmbH in Haar bei München.

DIAGNOSE – EINE EINFACHE UND SCHWIERIGE AUFGABE ZUGLEICH

Die Hauptaufgabe von Diagnosefunktionen ist eine ganz einfache: ein Fahrzeug, das nicht mehr fährt, zum Laufen zu bringen. Dazu muss in der Regel zunächst der Fehler lokalisiert, anschließend die Reparatur durchgeführt und schließlich die erfolgreiche Fehlerabstellung verifiziert werden. Das kann grundsätzlich zwei Klassen von Fehlern betreffen: Hardwarefehler, bei denen beispielsweise Teile ausgetauscht oder Steckverbindungen in Ordnung gebracht werden müssen, oder Softwarefehler, bei denen ein Update der Steuergerätesoftware durchgeführt wird.

Im Detail sind die Herausforderungen durchaus unterschiedlich. Der Halter eines Pkws wird meist bei auftretenden Problemen einen Termin mit seiner Werkstatt vereinbaren, wo diese analysiert und behoben werden. Bei Lkw sieht das

schon anders aus: Die Ladung muss zum vorgegebenen Zeitpunkt abgeladen sein, der Lkw insgesamt so lange wie möglich unterwegs sein. Die Werkstattzeiten orientieren sich also an den vorhandenen Leerzeiten, denn erst dann wird die nächste Werkstatt angefahren, die oft eine spezialisierte ist, etwa vom Getriebehersteller. Bei fahrenden Arbeitsmaschinen ist die Situation ähnlich, allerdings sind diese oft aufwendig zu bewegen, die Werkstatt muss also zur Maschine kommen.

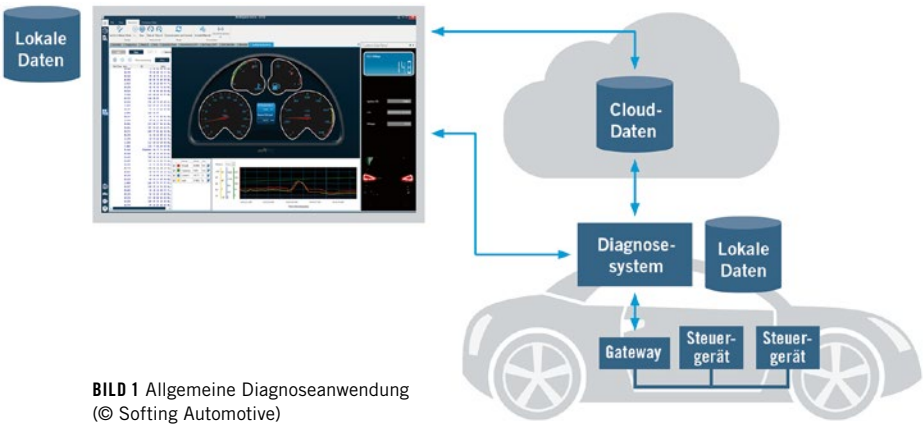

BILD 1 Allgemeine Diagnoseanwendung (© Softing Automotive)

REMOTE, CLOUD UND SECURITY

Diese Herausforderungen führen in Kombination mit den immer komplexeren E/E-Architekturen dazu, dass die Reparaturprozesse sowie die Erstellung der zugehörigen Diagnose- und Testwerkzeuge immer schwerer zu beherrschen sind. Ein Lösungsansatz ist die Ferndiagnose:

- Die neue Steuergerätesoftware wird über eine Internetverbindung auf das Fahrzeug gebracht und zum passenden Zeitpunkt programmiert (Software-Updates „over the air“).
- Über ein Cloud-basiertes Diagnosesystem wird regelmäßig der Fahrzeugstatus überprüft und bei vorhersehbaren Problemen rechtzeitig ein Werkstatttermin vorgeschlagen (Predictive Maintenance).
- Wenn eine Maschine von einem technischen Center überprüft wird, kann der Werkstattmitarbeiter mit dem passenden Teil ausrücken und kurzfristig einen Fehler beheben (Remote Diagnostics).

Dies sind nur einige offensichtliche Möglichkeiten, wie über einen Fernzugriff die Diagnose effektiver und effizienter werden kann. Darüber hinaus gibt es zahlreiche weitere Anwendungsfälle im Entwicklungsumfeld [1]. Die Gesamtheit aus aktuellen Diagnosemethoden wird allgemein unter dem Begriff Diagnose 4.0 zusammengefasst: Remote- und Cloud-Diagnose (Remote) sowie Diagnose am Fahrzeug (Proximity). In der Praxis kommt noch ein weiterer Anwendungsfall dazu. Nachdem für Ferndiagnosen aufgrund der heutigen Netzwerkverbindungen die Anforderungen an Latenz, Bandbreite und Verfügbarkeit nicht hinreichend abgesichert sind, wird ein Teil eines modernen Diagnosesystems ohnehin auf das Fahrzeug verlegt.

Für einige Anwendungsfälle – insbesondere solche, bei denen eine Anwenderinteraktion nur eingeschränkt notwendig ist – kann dann auch der gesamte Tester dort implementiert werden (der sogenannte In-Vehicle-Ansatz).

HERAUSFORDERUNG SECURITY

Unabhängig von der Methode, mithilfe der Diagnose kann am Fahrzeug fast alles gemacht werden: Es können Parameter oder die gesamte Software geändert, Fahrzeugfunktionen ausgelöst oder Informationen aus den Steuergeräten ausgelesen werden. Dies führt schon bei heutigen Diagnoseanwendungen zu einem nicht unerheblichen Gefahrenpotenzial; gerade bei Remoteanwendungen ist es allerdings ungleich höher. Daher muss eine adäquate Absicherung im Hinblick auf Vertraulichkeit (Confidentiality), Unversehrtheit (Integrity) und Echtheit (Authenticity) erfolgen:

- Es dürfen von Dritten keine Informationen aus dem Fahrzeug ausgelesen werden, insbesondere keine personenbezogenen Daten. Dies unterliegt der Datenschutzgrundverordnung mit den bekannten Strafandrohungen.
- Es dürfen weder gespeicherte noch Kommunikationsdaten von Dritten verändert werden. Dies betrifft beispielsweise Fahrzeugkonfigurationen, deren Änderung zu erhöhten Gewährleistungskosten führen kann.
- Es darf kein Missbrauch von Fähigkeiten des Fahrzeugs durch Dritte erfolgen. Im schlimmsten Fall führt ein Eingriff in das Fahrzeug während der Fahrt zu Personenschäden.

In einem allgemeinen Diagnosesystem, **BILD 1**, muss der Schutz an zahlreichen Stellen greifen. Zunächst werden die Anwendungen (Tester und Diagnosesystem) gegen missbräuchliche Nutzung geschützt. Dazu müssen sich Anwender authentifizieren. Danach werden alle lokalen und Cloud-Daten verschlüsselt, damit sie von außen nicht mehr lesbar sind. Die Anwendungen selbst erlauben den Zugriff nach dem ersten Schritt nur noch autorisierten Anwendern. Schließlich sind alle Kommunikationsverbin-

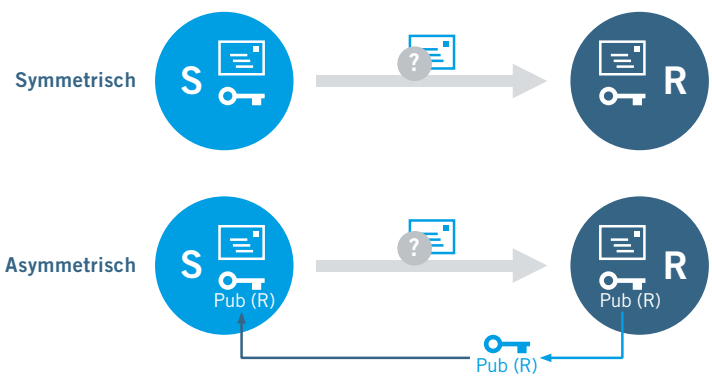

BILD 2 Symmetrische und asymmetrische Verschlüsselung (© Softing Automotive)

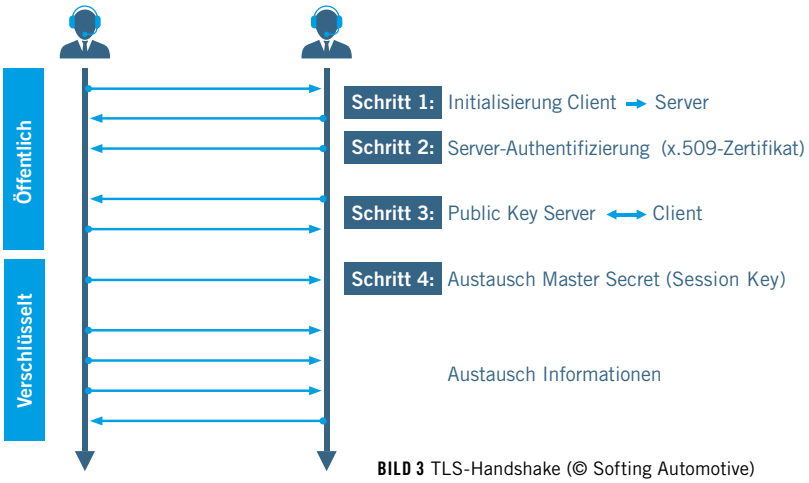

BILD 3 TLS-Handshake (© Softing Automotive)

dungen gegen Mithören abzusichern; auch hier ist wieder eine Verschlüsselung notwendig. Das Ziel aller Maßnahmen muss eine Ende-zu-Ende-Absicherung der Gesamtfunktion „Diagnose“ sein, wobei der Anwender das eine Ende darstellt, das andere Ende typischerweise das Fahrzeug-Gateway. Innerhalb des Fahrzeugs sind andere Schutzmechanismen notwendig.

Bei der Verschlüsselung unterscheidet man zwischen zwei grundsätzlichen Verfahren, der symmetrischen und der asymmetrischen Verschlüsselung, **BILD 2**. Bei der symmetrischen Verschlüsselung kennen beide Beteiligte den geheimen Schlüssel, mit dem verschlüsselt und entschlüsselt wird. Das Verfahren ist mit eher kurzen Schlüsseln von 256 Bit Länge schon sehr sicher und kann auch effizient berechnet werden. Allerdings muss der Dechiffrierschlüssel sicher und ohne dass ein Dritter ihn korrumpieren kann zu den Beteiligten gelangen, etwa durch persönlichen Kontakt.

Die asymmetrische Verschlüsselung arbeitet mit je einem Schlüsselpaar bei beiden Beteiligten. Der öffentliche Schlüssel (Public Key) wird dem jeweiligen Partner zur Verfügung gestellt und dient diesem zur Verschlüsselung. Der private Schlüssel (Private Key) wird sicher verwahrt und dient zur Entschlüsselung der mit dem Public Key verschlüsselten Nachricht. Auf diese Weise kann die Schwierigkeit der Schlüsselübertragung beim symmetrischen Verfahren umgangen werden, allerdings werden hier größere Schlüssellängen benötigt, die auch zu langen Rechenzeiten führen. Zudem muss man die öffentlichen Schlüssel von einer vertrauenswürdigen Stelle beziehen.

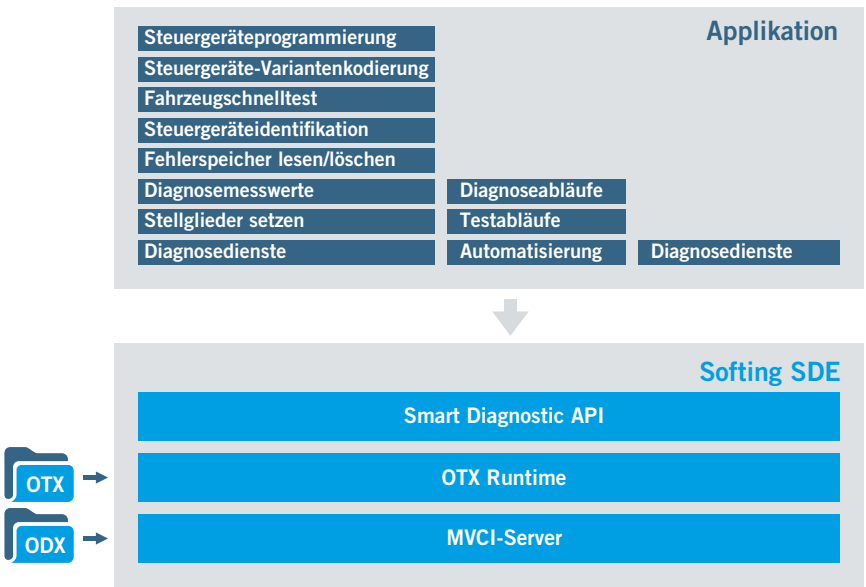

BILD 4 Das Diagnoselaufzeitsystem Softing SDE (© Softing Automotive)

PASSENDE LÖSUNGSANSÄTZE

Für eine sichere Ende-zu-Ende-Absicherung muss zunächst die Anwendung geschützt werden. Sie darf weder durch Kopieren der gesamten Anwendung noch durch Patchen einzelner Dateien kompromittierbar sein. Dies erfolgt typischerweise durch Lizensierungsverfahren und durch „Verpacken“ der relevanten Anwendungsteile (Enveloping). Kommerzielle Werkzeuge sind dafür verfügbar. Zusätzlich muss sich der Anwender authentifizieren. Dies ist wichtig, weil nicht jeder, der zufällig einen Tester in die Hand bekommt, auf das Fahrzeug zugreifen darf – aber auch nicht jeder grundsätzlich Berechtigte unbedingt Steuergeräte programmieren sollte. Dazu können Rollenmodelle in der Anwendung hinterlegt werden und durch Anmeldeverfahren – im einfachsten Fall ein Passwort – abgesichert werden.

Der Schutz der Daten, unabhängig davon, ob anwendungslokal, fahrzeuglokal oder in der Cloud, erfolgt in der Regel über symmetrische Verschlüsselungsverfahren. Der zugehörige Schlüssel muss entsprechend sicher in das Programm kompiliert und zur Laufzeit im Speicher gehalten werden, damit sehr gute Sicherungsgrade erreicht werden. Beispiele für solche Verschlüsselungsverfahren sind Blowfish oder Advanced Encryption Standard (AES), die beide Blockchiffren darstellen und somit die Datengröße nicht negativ beeinflussen. Außerdem sind beide nicht patentiert und können frei genutzt werden.

Kommunikationsverbindungen werden meist über Protokolle abgesichert, die einen Hybriden aus symmetrischer und asymmetrischer Verschlüsselung implementieren. Dabei werden zunächst in einer Initialisierungsphase über eine asymmetrische Kommunikation ein Code oder die zur Berechnung benötigten Bestandteile ausgetauscht. Mit dieser Information kann dann anschließend über eine symmetrische Verschlüsselung sehr effizient die eigentliche Kommunikation durchgeführt werden. Der Schlüs-

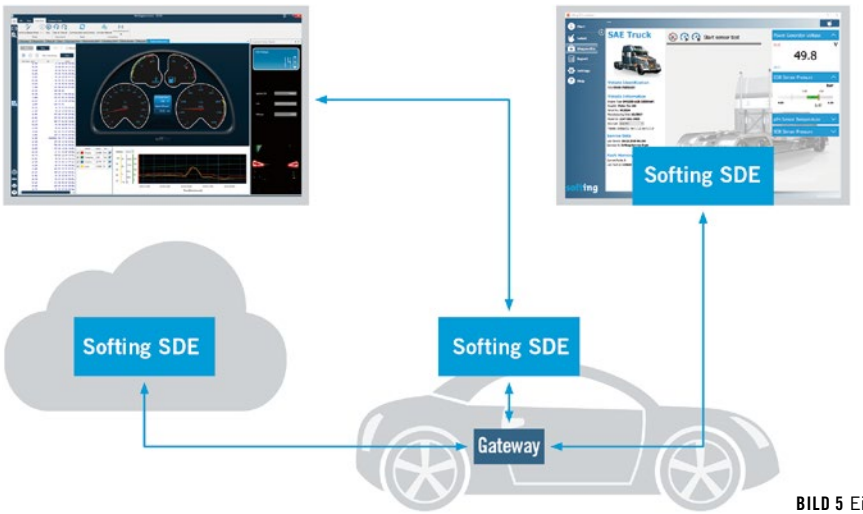

BILD 5 Einsatzszenarien für Softing SDE (© Softing Automotive)

sel ist für sichere Verfahren nur während einer Kommunikationssitzung gültig und wird dann verworfen.

Ein Beispiel für ein solches Verfahren ist Transport Layer Security (TLS), das regelmäßig in Internetprotokollen eingesetzt wird, beispielsweise bei https, in VPN-Implementierungen und im Internet der Dinge (Internet of Things, IoT) im Protokoll MQTT, **BILD 3**. TLS implementiert einen Handshake zur Initialisierung, bei dem über verschiedene Verfahren (RSA- oder Diffie-Hellman-Merkle-Schlüsselaustausch) zunächst der Schlüssel gebildet wird. Die Authentifizierung des Kommunikationspartners erfolgt dabei ebenfalls über ein standardisiertes Verfahren mit vertrauenswürdigen Zertifikaten (X.509-Zertifikat). Anschließend wird über das in der Initialisierung ausgehandelte Verfahren symmetrisch verschlüsselt. In der Regel ist dies wieder, wie bei der Verschlüsselung von Daten, AES.

UMSETZUNG IN DER PRAXIS

Will man sichere Remote-Diagnosesysteme implementieren, muss man neben der Security eine zweite Herausforderung meistern, denn heutige Diagnosesysteme sind meist diagnosedienstbasiert, sie müssen also für jede Teilaufgabe einen Diagnosedienst auslösen. Diagnoseaufgaben benötigen aber regelmäßig mehrere Teilschritte und umfassen verschiedene Steuergeräte. Über eine Fernverbindung wird dies in gleichem Maße langsam und instabil, sodass eine andere Systemarchitektur benötigt wird. Die Praxis zeigt, dass die Kombination von Diagnosediensten zu in sich geschlossenen Diagnoseaufgaben sehr gut abstrahierbar ist. Als Beispiel kann die Funktion „FehlerspeicherLesen“ dienen: Es muss vom Steuergerät zunächst eine Fehlerliste abgefragt werden und anschließend pro Fehler für weitere Informationen ein zusätzlicher Diagnosedienst ausgeführt werden. Wenn man diesen Ablauf als ganze Sequenz im Fahrzeug ablaufen lässt, muss ein Remotetester den Ablauf nur noch anstoßen und nach Beendigung Ergebnisse abholen.

Im Diagnoselaufzeitsystem Softing SDE, **BILD 4**, ist dieses Prinzip bereits umgesetzt. Für die wichtigsten Diagnoseaufgaben, beispielsweise „IdentifikationLesen“, „FehlerspeicherLesen“, „VariantenCodieren“ oder „ECUProgrammieren“, stehen Funktionen am API (Application Programming Interface) zur Verfügung. Die Kommunikation ist über den Standard ODX (Open Diagnostic Data eXchange) beschrieben, Abläufe werden entweder fest programmiert oder im Standard OTX (Open Test sequence eXchange) definiert. Das gesamte Diagnosesystem ist plattformunabhängig umgesetzt, kann also unter verschiedenen Betriebssystemen eingesetzt werden. Dadurch wird immer der gleiche Datensatz verwendet, und das Laufzeitverhalten ist ebenfalls identisch. Egal ob im Entwicklungstester unter Windows und ohne Remoteanbindung, in der Produktion mit einem im VCI (Vehicle Communication Interface) integrierten Diagnoselaufzeitsystem oder direkt im Fahrzeug integriert – Softing SDE ermöglicht eine merkliche Qualitäts- und Effizienzsteigerung, **BILD 5**.

FAZIT

Zusätzlich zur heutigen Diagnose direkt am Fahrzeug hält die Remote- und Cloud-Diagnose – Diagnose 4.0 – Einzug in die Reparaturlandschaft. Die erweiterten Möglichkeiten, die sich aus den Anwendungsfällen im Fahrzeug, am Fahrzeug und aus der Ferne ergeben, erfordern aber ein Umdenken in Bezug auf die Architektur des Diagnosesystems und der Security. Ein Teil der Diagnosefunktionen muss ins Fahrzeug verlegt werden, um von der Netzwerkinfrastruktur unabhängig zu werden und die Diagnose auch unabhängig vom Tester autark im Fahrzeug abwickeln zu können. Security für eine Fernverbindung muss ganzheitlich gedacht werden, von der Anwenderauthentifizierung über die Anwendung und die Verbindungsstrecken bis ins Fahrzeug-Gateway. Dann kann mit den existierenden Technologien eine sichere Ende-zu-Ende-Diagnose aufgebaut werden. Softing SDE zeigt bereits heute, wie eine solche Diagnose im Fahrzeug funktioniert, sowohl im VCI als auch in klassischen Diagnosesystemen.

LITERATURHINWEIS

[1] Steffelbauer, M.: Größtmögliche Entwicklungseffizienz durch Remote Engineering. In: ATZelektronik 14 (2019), Nr. 10, S. 40-45

READ THE ENGLISH E-MAGAZINE
Test now for 30 days free of charge:
www.ATZelectronics-worldwide.com