Engineering Partner

Software-Updates „over-the-air“ – und ihre Folgen

Von Dr. Roman Cunis, Senior Consultant/Senior Systemingenieur, ServiceXpert GmbH Hamburg

Schöne neue Welt? Heute ist es ein Leichtes und eine Selbstverständlichkeit, dass App-Anbieter neue und erweiterte Softwareversionen auf Kundengeräte – Computer und Smartphones – „over-the-air“ verteilen können und so permanent in der Lage sind, ihren Kunden verbesserte und umfassendere Dienstleistungen zur Verfügung zu stellen – und zu verkaufen.

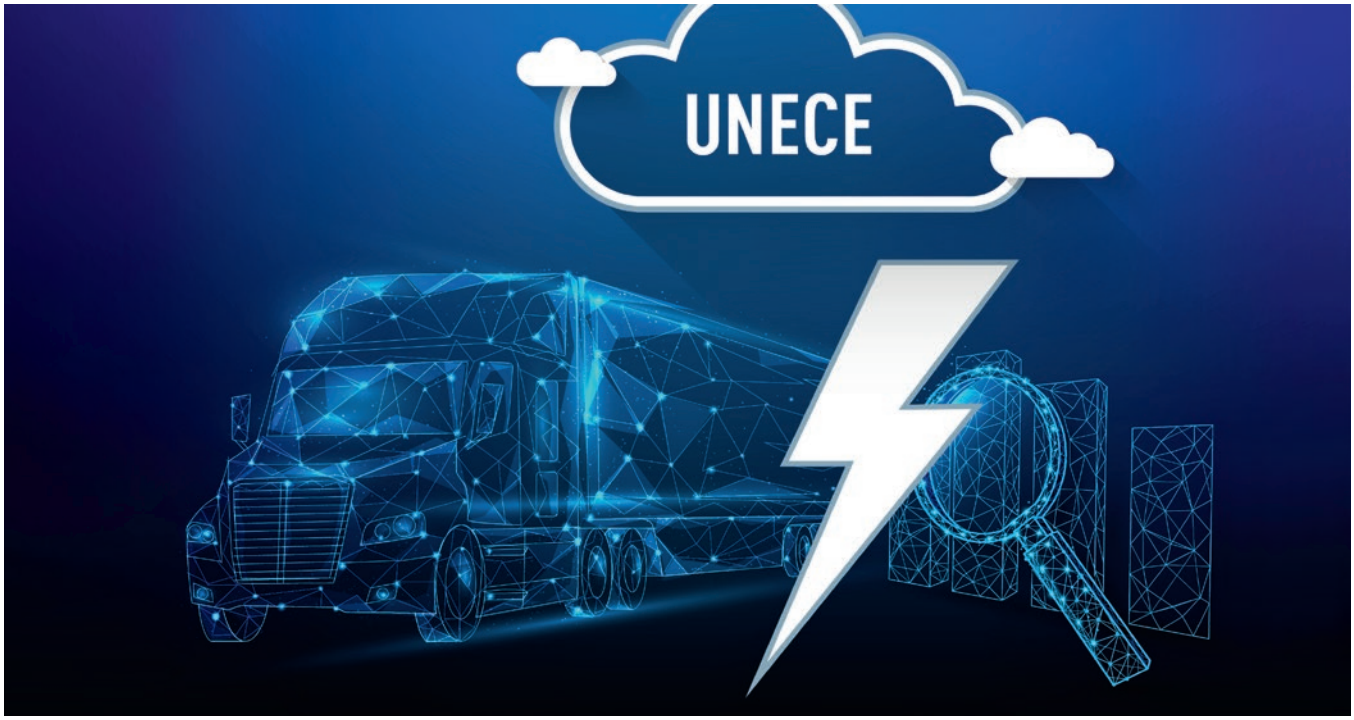

Bild: © ServiceXpert

Im Zeitalter zunehmend und dauerhaft vernetzter Fahrzeuge mit hohem Softwareanteil wollen auch Fahrzeughersteller und Anbieter von Software- und Datendienstleistungen rund um das Auto von diesen Möglichkeiten profitieren – in jeder Hinsicht des Wortes. Auch die Kunden freuen sich – glaubt man den Versprechungen der Werbung – auf den Tag, an dem sie an einem steilen Hang die Antriebsleistung ihres LKW oder an einem heißen Tag die Leistungsfähigkeit ihrer Klimaanlage „boostern“ können – „mal eben schnell“ und ohne Werkstattbesuch.

Was für die einen ein Traum von Komfort und für die nächsten ein Traum von Profit sein soll, erweist sich jedoch für wiederum andere zunehmend als Albtraum. Die Zulassungsbehörden fürchten, dass ein als steuersparend und energiearm zugelassenes Fahrzeug per Softwareupdate in ein energiefressendes „Monster“ verwandelt werden könnte. Die Hersteller befürchten, dass das unkontrollierte Einbringen von Softwareänderungen von außen, d. h. von anderen Anbietern als ihnen selbst, ein Fahrzeug auf eine Art verändern könnte, die schwerwiegende Schäden verursacht, für die der Hersteller zur Haftung verpflichtet werden könnte. Bereits mehrfach wurde in den vergangenen Jahren in Experimenten bewiesen, dass es möglich ist über offene und „over-the-air“ erreichbare Kommunikationsschnittstellen steuernd in das Verhalten von Fahrzeugen einzugreifen. Schon 2015 machte die erfolgreiche Kontrollübernahme eines Jeeps vom Computer aus Schlagzeilen in aller Welt.

Die UNECE-Regulierungen Nr. 155 und Nr. 156

Die UNECE – in ihrer Eigenschaft als europaweit tätige Regulierungsbehörde für Fahrzeuge und Fahrzeugteile – hat mit ihren Regelungen Nr. 155 und Nr. 156 einen Regulierungskorpus geschaffen, der diesen Risiken und Bedenken Rechnung tragen soll.

Regelung Nr. 155 über Anforderungen zur Cyber-Security in Fahrzeugen hat zur Folge, dass jegliche Kommunikation mit einem Fahrzeug, sei es „over-the-air“ oder herkömmlich per Kabel und Diagnosestecker gegen Manipulation abgesichert werden muss. Die Kommunikation erfolgt nur noch verschlüsselt, der Zugang setzt das Vorhandensein gültiger Zertifikate, die vom Fahrzeughersteller ausgestellt und im Fahrzeug selbst geprüft werden, voraus.

Regelung Nr. 156 über Anforderungen an ein Software-Update-Management seitens des Herstellers legt fest, dass nur freigegebene Software in einem Fahrzeug verwendet werden darf. Der Terminus „Software“ umfasst in diesem Kontext auch jegliche steuerungsrelevanten Parametersätze. Die Behörde hat erkannt, dass eine Fahrzeugtypzulassung (Homologation) nicht mehr nur von den physischen Eigenschaften eines Fahrzeugs abhängig sein kann, sondern auch von dem im Fahrzeug verwendeten Softwarestand. Jede Software bzw. jeder Softwarestand,

der eine regulierungsrelevante Fahrzeugfunktion betrifft, muss selbst homologiert werden. Er erhält eine sogenannte RxSWIN, eine eindeutige Software-Identifikationsnummer, die sich auf die regulierte Fahrzeugfunktion bezieht (die Regulierung R13 z. B. bezieht sich auf Bremsen, die RxSWIN einer zugehörigen Software beginnt daher ebenfalls mit „R13“).

Anforderungen an den Fahrzeughersteller

Der Fahrzeughersteller muss nun jede regulierungsrelevante Software separat homologieren. Zudem muss er bei jeder Softwareänderung prüfen, ob die Änderung „harmlos“ ist oder ob sie im Sinne der betroffenen Regulierung einen neu zu homologierenden Softwarestand darstellt. Weiterhin muss er für jedes Fahrzeug buchführen, welche Softwarestände in dem Fahrzeug enthalten sind – beginnend im Produktionsprozess und fortlaufend während des Fahrzeuglebenszyklus, d. h. also bei jeder Softwareaktualisierung oder -änderung in einer Werkstatt oder vermittels eines „over-the-air“-Updates. Er muss sicherstellen, dass bei einer behördlichen Prüfung eines Fahrzeugs, sei es beim TÜV oder bei einer Polizeikontrolle, der Softwarestand des Fahrzeugs festgestellt und geprüft werden kann. Mit der zusätzlichen Einführung einer IVD (Integrity Verification Data) für jede Software und jeden steuerungsrelevanten Parametersatz im Fahrzeug soll zudem sichergestellt werden, dass jederzeit festgestellt werden kann, ob Software oder Daten manipuliert worden sind bzw. von den Herstellervorgaben abweichen.

Man kann sich leicht vorstellen, dass diese Vorgaben einen immensen Aufwand bei der Umgestaltung von Entwicklungs-, Produktions- und Werkstattprozessen nach sich ziehen, und dass auch beteiligte Softwareanwendungen (für die Erstellung von Steuergerätesoftware, für die Bandendeprüfung in der Produktion und für die Werkstattdiagnose, um nur einige zu nennen) angepasst und erweitert werden müssen.

Schließlich und endlich muss jeder Fahrzeughersteller im Zuge eines behördlichen Audits nachweisen können, dass und wie er seine Prozesse und Softwareanwendungen ertüchtigt hat, den neuen Anforderungen zum Software-Update-Management zu genügen.

Auswirkungen auf den freien Markt im Fahrzeugumfeld

Was für viele Fahrzeugbesitzer und Fahrzeughalter wie eine längst überfällige Absicherung gegen Softwaremanipulation am Fahrzeug erscheinen mag, hat in der Konsequenz aber auch eklatante Auswirkungen auf die Fahrzeugbetreuung in freien Werkstätten. Erst vor wenigen Jahren wurden mit den Regelungen zur Bereitstellung von Reparatur- und Wartungsinformationen (RMI

Bild: © Adobe Stock/vegefox.com

= Repair and Maintenance Information) an freie Werkstätten und andere unabhängige Marktteilnehmer die Hersteller aufgefordert, den freien Markt nicht gegenüber herstellereigenen Werkstätten zu benachteiligen. Die Regelungen, die im Rahmen der Euro-5-Norm für PKWs und der Euro-VI für LKWs in den Jahren 2009 bis 2015 in Kraft traten, sollten den freien Wettbewerb in Europa fördern, und sie drohten den Herstellern bei Zuwiderhandlung Strafen bis hin zur Aberkennung von Fahrzeugtypzulassungen an.

Technisch bedeutete die Bereitstellung von RMI die Offenlegung von Bedeutung und Strukturen derjenigen Fahrzeugdaten, die über die ohnehin offene Diagnoseschnittstelle (OBD-II-Stecker) von jeder Werkstatt ungehindert gelesen und bis zu einem gewissen Grad auch verändert werden konnten. Diese Veränderungsmöglichkeit betraf zum einen das Ändern von Parametern, mit denen das Fahrverhalten eines Fahrzeugs gesteuert werden kann, zum anderen das Einspielen von Softwareupdates.

Mit den UNECE-Regelungen Nr. 155 und Nr. 156 wird der Fahrzeughersteller nun gezwungen (nach anderer Lesart: „... wird es ihm wieder erlaubt“), den freien Zugang einzuschränken. Der verschlüsselte Zugriff über die offene Diagnoseschnittstelle erzwingt den Erwerb von Zugangszertifikaten. Mit den Forderungen zum Software-Update-Management stellt sich die grundsätzliche Frage, ob die Pflicht zum Nachhalten des aktuellen Softwarestandes eines Fahrzeugs beim Hersteller die Veränderung des Fahrzeugs durch jemand anderen als den Hersteller nicht grundsätzlich ausschließt. Die Folgen betreffen nicht nur freie Werkstätten, sondern auch Anbieter von Mehrmarken-Diagnosetools und Zulieferer von Fahrzeugsteuergeräten, denen der Zugriff auf ihre eigenen Komponenten verwehrt wird.

Neue Diagnosetechnologien wie das Passthrough-Verfahren, bei dem ein unabhängiger Marktteilnehmer Diagnosesoftware und Fahrzeugdaten von einem Herstellerportal herunterladen kann und diese als geschlossenes „Paket“ auf das Fahrzeug anwenden kann, versprechen hier möglicherweise Abhilfe. Auch die aktuell in der Entwicklung befindlichen Diagnosemöglichkeiten über die sogenannte Extended-Vehicle-Schnittstelle (ISO 20077/78), bei der der Diagnosezugriff auf ein Fahrzeug durch einen Server des Herstellers geleitet wird und nur der Hersteller selbst den direkten Kommunikationszugriff auf das Fahrzeug hat, können hier – je nach Ausführung – helfend oder behindernd wirken. Die Interessenvertreter der unabhängigen Marktteilnehmer sind aktuell in intensiven Verhandlungen mit den Herstellern, wie unter den neuen Gegebenheiten der freie Wettbewerb im Fahrzeugumfeld erhalten werden kann.

Es wird wohl noch eine Zeit lang dauern, bis die erträumte schöne neue Welt für Fahrzeugnutzer, -hersteller und alle weiteren Beteiligten Wirklichkeit werden wird. Aus ihren jeweiligen Perspektiven arbeiten alle intensiv daran, das Ihre dazu beizutragen. Die ServiceXpert unterstützt ihre Kunden unter den Fahrzeugherstellern und Fahrzeugzulieferern in der Anpassung und Entwicklung von Prozessen und Tools dahingehend, dass mit diesen die neuen UNECE-Regularien bestmöglich unterstützt und eingehalten werden können.

Dr. Roman Cunis
Senior Consultant/
Senior Systemingenieur,
ServiceXpert Hamburg

ServiceXpert GmbH
https://servicexpert.de