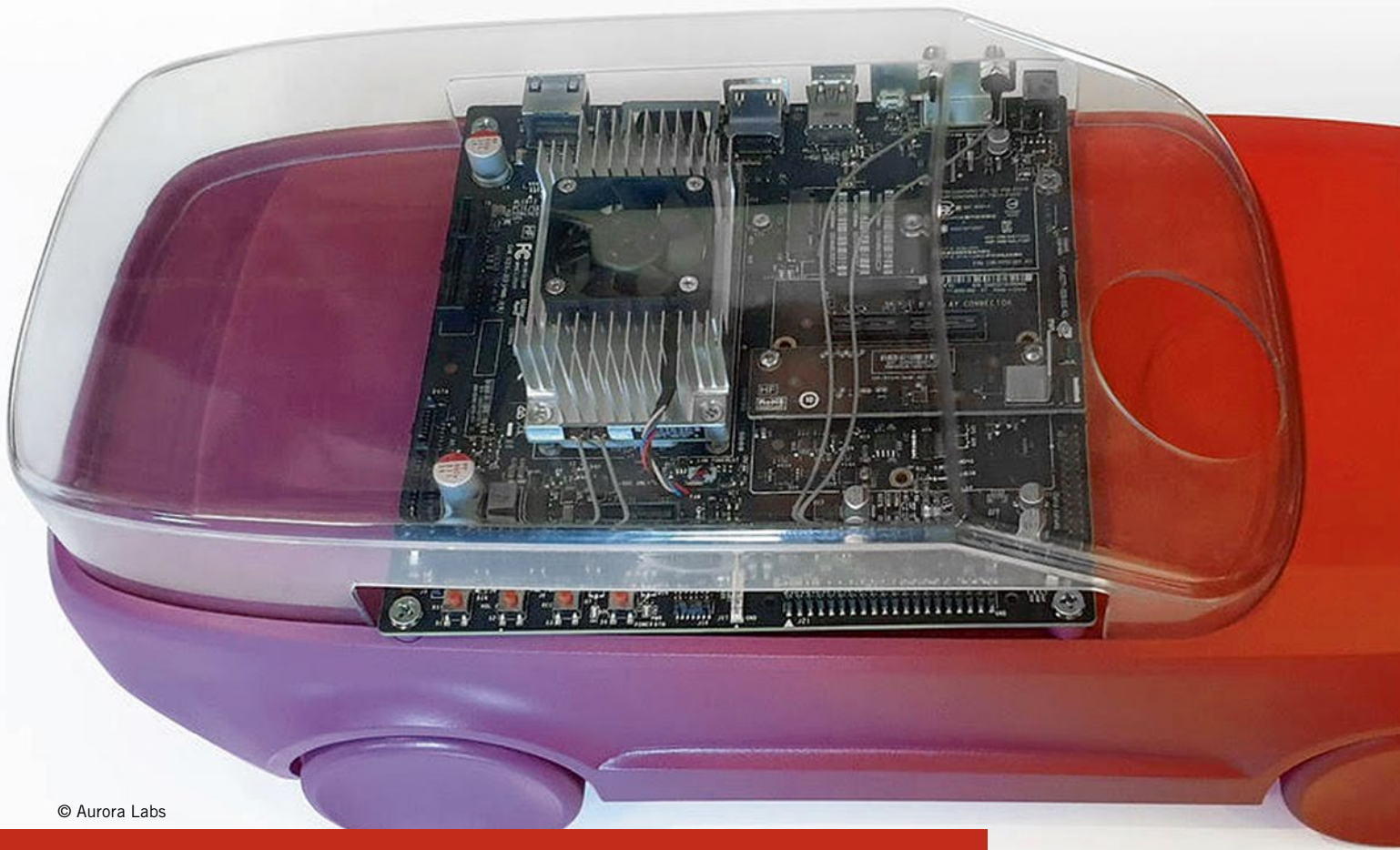

Beschleunigte Typgenehmigung durch Validierung von Softwareupdates

Erhalten Softwarefunktionen von Fahrzeugen Updates, erfordert dies in der Regel eine aktualisierte Typgenehmigung. Mit einer im Fahrzeug integrierten Softwaremanagementlösung ermöglicht es Aurora Labs Fahrzeugherstellern, die genauen Änderungen im Code nachzuweisen. Dadurch muss nicht mehr die gesamte Software, sondern nur noch der betroffene Teil für die neue Typgenehmigung getestet werden.

AUTOR

Rudolf von Stokar
ist General Manager Germany bei Aurora Labs in Unterschleißheim.

Weltweit müssen Fahrzeuge nach spezifischen Vorschriften zertifiziert werden, um für den Verkauf und die Straße zugelassen zu werden. Verfahren und Vorschriften rund um die Fahrzeugzulassung werden als Typgenehmigung bezeichnet. Typgenehmigungsverfahren unterscheiden sich zwar von Land zu Land, jedoch stützen sich alle auf eine Reihe von umfangreichen Regeln, die von der Wirtschaftskommission der Vereinten Nationen für Europa (Unece) herausgegeben werden.

Die Unece hat ein neues Regelwerk angekündigt, das voraussichtlich Mitte 2020 in Kraft treten wird. Diese neuen Regeln ermöglichen es, eine geänderte Komponente des Fahrzeugs mit einer neuen oder geänderten Typgenehmigung in Übereinstimmung zu bringen. Eine neue Typgenehmigung ist dann nur erforderlich, wenn die geänderte Komponente – zum Beispiel ein Softwareupdate – dem Fahrzeug neue Funk-

tionen verleiht. Handelt es sich hingegen nur um eine Behebung einer bestehenden und bereits genehmigten Komponente, etwa einem Bugfix oder einem Cyber-Security-Patch, ist keine neue Typgenehmigung erforderlich.

BEDEUTUNG DER SOFTWARE IM FAHRZEUG

Moderne Autos sind zunehmend vernetzt und enthalten bis zu 100 Computer und Millionen Zeilen von Softwarecode. In dieser großen Menge an Code können potenziell zahlreiche Fehler enthalten sein, die zu Softwareproblemen führen. Um die Sicherheit des Fahrzeugs und des Fahrers zu gewährleisten, müssen solche Fehler behoben werden, bevor sie zu einem Problem werden.

Software wird bis 2025 voraussichtlich 40 % des Fahrzeugwerts ausmachen. Einige Analysten prognostizieren mehr als 600 Millionen Zeilen an Codes in zukünftigen Autos. Darüber hinaus kosten Typgenehmigungen Automobilhersteller rund 36 Millionen Euro pro Jahr. Wiederum 40 % davon sind auf Software zurückzuführen. Es ist also offensichtlich, dass die Typprüfung ein komplexes, teures und zeitaufwendiges Problem ist.

TYPGENEHMIGUNG FÜR SOFTWAREUPDATES

Die voraussichtlich Mitte 2020 in Kraft tretenden Unece-Regelungen werden erwartungsgemäß weiterhin eine aktualisierte Typgenehmigung nach Softwareupdates fordern. „Die Hersteller sollen dazu verpflichtet werden, der Genehmigungsbehörde/den technischen Diensten relevante Dokumente von der Anforderungsanalysephase bis zur Umsetzungsphase vorzulegen“, heißt es in dem Positionspapier, das unter den Over-the-Air(OTA)-Stakeholdern verbreitet wird [1].

Es gibt jedoch verschiedene Arten von Softwareupdates, die von Korrekturen für bestehende Softwarefunktionen bis hin zu Sicherheitspatches und neuen Funktionen reichen und die während des gesamten Lebenszyklus des Fahrzeugs hinzugefügt werden. Daher unterschied die Unece die Notwendigkeit geänderter Typgenehmigungen insbesondere in folgendem Punkt: „Der Fahrzeughersteller wendet sich an die zuständige Typgenehmigungsbehörde, um eine Erweiterung oder Neuzertifizierung für die betroffenen Systeme für alle Aktualisierungen einzuholen. Eine Ausnahme besteht, wenn das Update die Konformität eines typgenehmigten Systems nicht beeinträchtigt (z. B. zur Behebung von Softwarefehlern). In diesem Fall kann der Fahrzeughersteller das Update durchführen, ohne die Typgenehmigungsbehörde zu kontaktieren, stellt aber sicher, dass der verwendete Aktualisierungsprozess sicher und geschützt ist“ [2].

Der Typgenehmigungsprozess und die laufenden Softwareupdates müssen Hand in Hand gehen, ohne den Fortschritt in der Automobilindustrie zu behindern. Dafür ist ein System erforderlich, das den Nachweis dafür liefert, dass zum einen ein Softwareupdate nur Fehler behebt oder einen Sicherheitspatch anwendet, aber keine neuen Funktionen hinzufügt. Dadurch entfällt die Notwendigkeit, eine aktualisierte Typgenehmigung zu beantragen. Zum anderen muss nachgewiesen werden, dass eine neue Softwarefunktion nur einen begrenzten und definierten Teilbereich der installierten Software im Fahrzeug betrifft. Dies schränkt die durchzuführenden Prüfungen ein, um die geänderte Typgenehmigung zu erhalten.

Das Einholen einer Typgenehmigung für erforderliche Updates ist ein langwieriger und kostspieliger Prozess. Automobilhersteller sind verpflichtet, die Genehmigungsbehörden darüber zu informieren, dass für eine zugelassene Komponente auch eine neue Version der Software verfügbar ist. Abhängig von der Art des Updates sind die Hersteller außerdem verpflichtet zu erklären, ob das Update zu Abweichungen von den bestehenden Typgenehmigungsbedingungen führt. Werden neue Funktionen hinzugefügt, muss der Hersteller das aktualisierte Bauteil und alle relevanten Unterlagen zur erneuten Prüfung an die Typengenehmigungsbehörde (Type

BILD 1 Die Line-of-Code Behavior Technologie analysiert Software und erstellt darauf basierend eine Übersicht, wie sich Softwarefunktionen gegenseitig beeinflussen (© Aurora Labs)

Approval Authority, TAA) senden. Obwohl eine geänderte Typgenehmigung für eine Behebung bestehender Funktionen nicht erforderlich ist, muss der Hersteller nachweisen, dass das Update keine neuen Funktionen hinzufügt.

Während eine Typgenehmigung zuvor einmal für jedes Fahrzeugmodell eingeholt wurde, wird in der Welt des softwaredefinierten Fahrzeugs erwartet, dass Änderungen an der Typgenehmigung regelmäßig auch für Updates von bereits verkauften Fahrzeugen erforderlich sein werden.

NACHWEIS VERÄNDERTER FUNKTIONALITÄT IM FAHRZEUG

Die auf maschinellem Lernen basierende Line-of-Code Behavior-Technologie von Aurora Labs analysiert neue Software bereits während sie entwickelt wird und erstellt darauf dieser Grundlage eine Übersicht der Beziehungen und des Verhaltens von Softwarefunktionen. Diese dynamische Karte ermöglicht transparente Einblicke in die ECU-Funktionalität in Echtzeit, **BILD 1**.

Die Software Functionality Relationship Map genannte Karte veranschaulicht die Beziehungen zwischen den Softwarefunktionen in verschiedenen Steuereinheiten und ermöglicht es so, Änderungen an der Softwarekonfiguration und im Softwareverhalten systemweit nachzuweisen. Im Gegensatz zu aktuellen Lösungen, die im Rahmen des Zertifizierungsprozesses den Hashwert für die gesamte Software berechnen, erzeugen die Line-Of-Code-Behavior-Algorithmen einen digitalen Fingerabdruck der Softwarefunktionen und ihrer Eigenschaften. Dieser liefert den Nachweis über Änderungen an der Softwarefunktionalität, sowohl bei neuen Softwareupdates als auch bei Änderungen, die nach der Zertifizierung und dem Verkauf des Fahrzeugs auftreten können, **BILD 2**.

Um beispielsweise einen Softwarefehler zu beheben, wird der Software ein neuer Code hinzugefügt. Ein bloßer Hashwert identifiziert lediglich eine Änderung in der Software, die eine geänderte Typgenehmigung erfordert. Aurora Labs analysiert hingegen das Funktionsverhalten der neuen Software anhand der Codezeilen und ermöglicht es dem Automobilhersteller, die tatsächlichen Auswirkungen der Softwareänderungen auf die Funktionen nachzuweisen, die bereits eine Typgenehmigung erhalten haben. Hat ein Softwareupdate keine Auswirkungen auf das Verhalten der Softwarefunktionen, so liefert Aurora Labs dem Fahrzeughersteller den nötigen Nachweis für die Zulassungsbehörden, dass keine neue Typgenehmigung erforderlich ist.

Stellt man eine Änderung des Funktionsverhaltens eines bestimmten Steuergeräts fest, können bei Verwendung dieser Technologie auch Abhängigkeiten der aktualisierten Steuergerätesoftware mit anderen Systemen erkannt werden. Ein solches Verfahren bestimmt, ob ein bestimmtes Softwareupdate andere Systeme oder Software betrifft. Beispielsweise kann die Bremssteuerung möglicherweise die Airbagsteuerung beeinflussen. Aurora Labs liefert den Nachweis und die Transparenz über die Softwarefunktionen, die nicht von der aktualisierten Software betroffen ist und daher für die aktualisierte Typgenehmigung nicht erneut getestet werden muss.

BILD 3 zeigt den Analyseprozess der Line-of-Code-Behavior-Technologie.

Dabei unterscheidet sich die Delta-Datei von Aurora Labs nicht von einer normalen Datei, die den bestehenden Software-Programmierprozess durchläuft. Bei Updates einer Delta-Datei wird nicht der komplette Softwarecode aktualisiert, sondern lediglich der Teil des Codes, an dem Änderungen vorgenommen wurden. Die entwickelte Lösung unterstützt dabei folgendes:

- S19-Dateiformat
- den bestehenden Kompressions- und Signaturprozess
- das bestehende zentrale Software-Repository
- das vorhandene Programming-Master-Tool mit relevanten Programmierparametern unter Verwendung des vorhandenen Bootloaders.

Die im folgenden erläuterten Anwendungen und Vorteile ergeben sich durch die Technologie.

EINHALTUNG DER TYPPRÜFUNG UND HAFTUNG

Automobilhersteller müssen eine Typgenehmigung beantragen, wenn sie ein neues Auto auf den Markt bringen wol-

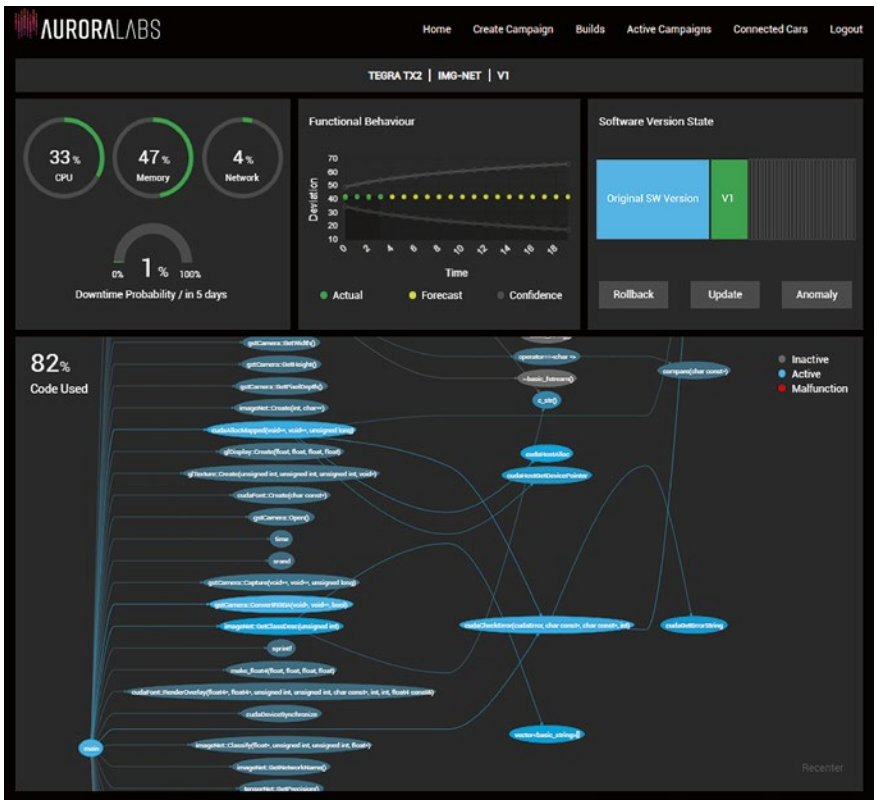

BILD 2 Die Lösung erkennt Anomalien in Softwarefunktionen und sagt Ausfallwahrscheinlichkeiten voraus (© Aurora Labs)

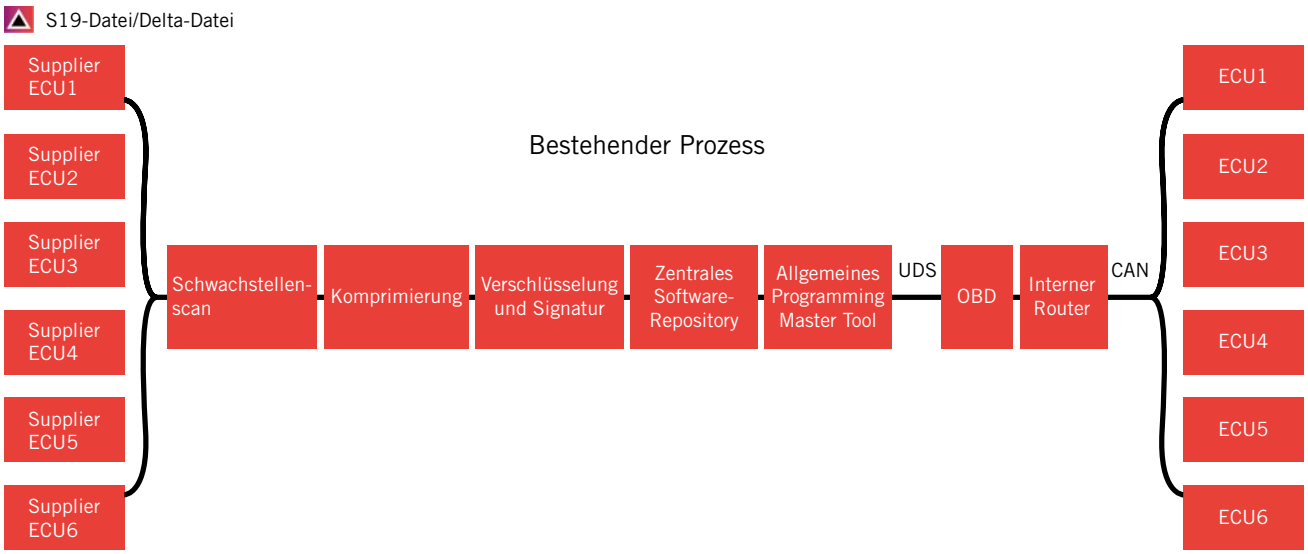

BILD 3 Der Analyseprozess der Line-of-Code-Behavior-Technologie (© Aurora Labs)

len. Der Hersteller ist verpflichtet, nachzuweisen, dass das Fahrzeug den einschlägigen Vorschriften entspricht. Es ist auch der Nachweis erforderlich, dass nach der Zertifizierung keine Änderungen an der Fahrzeugfunktionalität vorgenommen wurde, da neue Funktionen eine neue Typgenehmigung erfordern. Aurora Labs erstellt einen digitalen Fingerabdruck der tatsächlichen Software, die im Fahrzeug in jeder Phase des Lebenszyklus läuft. Dies gibt dem TAA die Möglichkeit, die digitalen Fingerabdrücke vor und nach einem Update zu vergleichen und so zu bestätigen, ob die im Fahrzeug laufende Softwarefunktion mit der Software identisch ist, die die Typgenehmigung erhalten hat.

KLARHEIT BEI GEWÄHRLEISTUNG

Dieselbe Funktion kann auch Klarheit bei Streitigkeiten bezüglich der Gewährleistung schaffen. Durch den Vergleich des digitalen Fingerabdrucks des Funktionalitätsverhaltens der Software des zu untersuchenden Fahrzeugs mit dem ursprünglichen digitalen Fingerabdruck des Fahrzeugs beim Verlassen der Produktionshalle kann der Hersteller feststellen, ob das Fahrzeug derart verändert und manipuliert wurde, dass eventuell Garantiebestimmung verletzt wurden.

VALIDIERUNG DER HARDWAREKONFIGURATION

Durch den Vergleich des digitalen Fingerabdrucks der Softwarefunktionalität im Fahrzeug mit dem digitalen Fingerabdruck der Software, die bei der Produktion freigegeben und von der TAA zertifiziert wurde, kann das Fahrzeug selbst identifizieren, ob ein neues Steuergerät zum Fahrzeug hinzugefügt wurde. Dadurch wird der Automobilhersteller gewarnt, dass nicht autorisierte Hardware im Fahrzeug installiert wurde und kann dann entweder die Garantie aufheben oder sogar das Anlassen des Fahrzeugs verhindern, um die Insassen nicht zu gefährden.

SICHERHEIT GEGEN HACKANGRIFFE

Bei Cyberangriffen wird häufig die Software während des Betriebs im Netzwerk abgefangen und geändert, bevor sie das Fahrzeug erreicht. Die Fähigkeit, den digitalen Fingerabdruck des Softwareverhaltens vor dem Einsatz, beispielsweise im Ruhezustand oder auf dem Server, zu analysieren und mit dem digitalen Fingerabdruck der Software zu vergleichen, die im Fahrzeug kurz vor der Installation steht, stellt sicher, dass die Software dazwischen nicht manipuliert wurde.

HILFE FÜR HERSTELLER, VERSPRECHEN EINZUHALTEN

Die oben beschriebene Lösung ist nur ein Teil der Line-of-Code-Behavior-Lösung. Sie verwendet maschinelles Lernen, um die vier Phasen Erkennung, Behebung, Update und Validierung eines Software Health Checks durchzuführen. Zunächst analysiert die Software mithilfe von maschinellem Lernen die Millionen von Zeilen Softwarecode im Fahrzeug, um Anomalien im Softwareverhalten zu erkennen und vorherzusagen, die zu Systemausfällen führen können. Nachdem eine Anomalie identifiziert wurde, kann die Lösung die Software nahtlos auf die neueste zertifizierte und sichere Version zurücksetzen. Sobald eine neue Softwareversion verfügbar ist, wird diese über ein OTA-Update ohne Ausfallzeiten installiert. Schließlich werden Struktur, Beziehungen und Abhängigkeiten der Software in Echtzeit überprüft, was den Genehmigungsprozess erheblich vereinfacht. Dieses ganzheitliche Softwaremanagement sichert die Zukunft softwarebasierter Fahrzeuge und rationalisiert den Typgenehmigungsprozess.

LITERATURHINWEISE

[1] Unece: Software updates-type approval and surveillance measures. Online: https://wiki.unece.org/download/attachments/42041676/TFCS-04-12e%20%28NL%29%20Type%20Approval%20of%20Software%20updates.pdf?api=v2, aufgerufen am 17.12.2019

[2] Unece: Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues. Online: https://undocs.org/ECE/TRANS/WP.29/GRVA/2019/3, aufgerufen am 17.12.2019