Digital Twin für maximale Cyber Security

Mit digitalem Fahrzeug-Zwilling neue UNECE-Cyber-Security-Vorgaben einfacher erfüllen

Jens Krüger, München

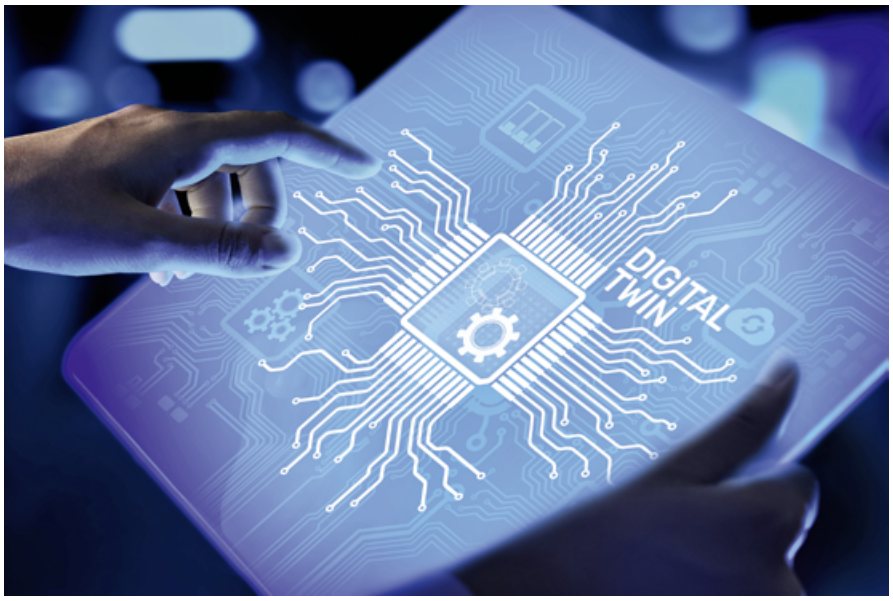
Die Digitalisierung in der Automobilindustrie macht Cyber Security bei Fahrzeug-Software-Updates zum Fokusthema – internationale Regulierungsgremien arbeiten dazu gerade Sicherheitsrichtlinien aus. Für Fahrzeughersteller bedeutet das, dass sie schnellstmöglich Prozesse und Systeme gemäß den neuen Cyber-Security-Vorgaben etablieren müssen. „Digital Twin Computing“ kann hier wesentlich unterstützen. Die neue Initiative aus Japan ist mehr als das, was gemeinhin unter einem Digitalen Zwilling verstanden wird.

Moderne Fahrzeuge sind „Rechenzentren auf Rädern“: Sie enthalten über 100 Steuergeräte für Funktionen wie Motorsteuerung, Antiblockiersystem, Airbag oder Navigation. Jedes Steuergerät ist ein Computer mit entsprechender (Embedded-) Software. In Summe sind derzeit ungefähr 100 Millionen Zeilen Code in einem Premium-Fahrzeug verbaut. Durch Innovationen wie automatisiertes Fahren sowie die zunehmende Vernetzung der Fahrzeuge wird sich das Software-Volumen in den nächsten zehn Jahren mindestens verdoppeln. Diese Software muss über den gesamten Lebenszyklus gewartet werden, um Sicherheit und Kundenzufriedenheit zu erreichen. Dabei kann Software-Wartung einerseits in der Korrektur von Fehlern bestehen. Andererseits kann sie aber auch neue Funktionen ermöglichen. In beiden Fällen müssen die Software Updates auf jedes einzelne Fahrzeug aufgebracht werden. Dazu war bisher meistens ein Werkstattbesuch erforderlich. In Zukunft wird dieser Prozess immer häufiger „Over-the-Air“, kurz „OTA“, ablaufen.

Safety ist nicht gleich Security

In den historisch gewachsenen Fahrzeugarchitekturen stand funktionale Sicherheit (Safety) im Vordergrund, sie wurde in der ISO 26262 bereits 2011 definiert. Informationssicherheit (Security) ist dagegen in diesem Umfeld eine neuere Disziplin. Diese Art von Sicherheit hat aufgrund der steigenden Zahl potenzieller Angriffspunkte in intelligenten, vernetzten Fahrzeugen (Bild 1) schnell große Bedeutung erlangt.

OTA ist dabei nur eines von vielen Informationssicherheitsrisiken, die mit entsprechenden Maßnahmen so klein wie möglich gehalten werden müssen. Dies gilt umso mehr, da Cyber Security und OTA Gegenstand internationaler Standardisierung sind und somit Voraussetzung für die Typzulassung (Homologation) der Fahrzeuge in den einzelnen Märkten werden.



Neue Cyber-Security-Vorschriften verändern Typzulassung

Fahrzeuge werden global verkauft und genutzt. Dabei müssen sie länderspezifische Zulassungsvorschriften erfüllen. In Deutschland erfolgen zum Beispiel Typgenehmigungen durch das Kraftfahrt-Bundesamt auf Basis der Straßenverkehrs-Zulassungs-Ordnung. Um den Prozess der Homologation zu vereinfachen, gibt es bei der „United Nations Economic Commission for Europe“, kurz „UNECE“, das „WP.29“, also das „World Forum for Harmonization of Vehicle Regulations“. Dort werden die Regelwerke abgestimmt und anschließend in nationales Recht überführt. Insbesondere sind in der Task Force „Cyber Security and Software Updates OTA“ zwei Regelungen in Arbeit,

die in den kommenden Jahren massiven Einfluss auf die Typzulassung haben werden und Fahrzeughersteller vor große Herausforderungen stellen. Der Digitale Zwilling des Fahrzeugs ist dabei ein wesentlicher Lösungsbaustein.

SUMS – enormer Aufwand für Automobilhersteller

Der aktuelle Entwurfsstand der Regelungen von Anfang 2019 sieht vor, dass der Fahrzeughersteller Prozesse und Systeme etabliert, um Informationssicherheit während der Entwicklung, Produktion und Nutzung sicherzustellen. Unter anderem soll ein Software Update Management System (SUMS) geschaffen und alle drei Jahre auditiert werden. Die Anforderungen an das SUMS umfassen die Identifikation aller Software-Versionen und ihrer Abhängigkeiten zur eingesetzten Hardware- und Software-Umgebung (Kompatibilität), die Identifikation von Ziel-Fahrzeugen für ein Software Update, die Auswirkungsanalyse auf bestehende Typzulassungen, die Information der Fahrzeugnutzer und die sichere Durchführung von Software Updates – alles verbunden mit umfangreicher Dokumentation.

Eine weitere Anforderung im Zusammenhang mit SUMS ist die „RX Software Identification Number“ (RXSWIN), die regelungsspezifische Informationen über homologationsrelevante Software enthält. Jedes Fahrzeug muss über Standardschnittstellen (On-Board-Diagnose – OBD) Auskunft geben können, welche Softwarestände für typzulassungsrelevante Funktionen auf dem Fahrzeug installiert sind.

Erfüllen neuer Regularien: Digital Twin reduziert Aufwand

Um Cyber-Security-Vorschriften wie SUMS & Co. zu erfüllen, ist der Digitale Zwilling des Fahrzeugs ein wesentlicher Lösungsbaustein. Denn Automobilhersteller können Digital Twins nutzen, um das reale Fahrzeug zu überwachen und zu analysieren. So bietet ein digitaler Fahrzeug-Zwilling genau das, was die neuen UNECE-Regularien an Transparenz für eine höchstmögliche Cyber Security erfordern: Die Integrität und Authentizität der im Fahrzeug vorhandenen Software lässt sich jederzeit nachvollziehen, Software Updates sind frühzeitig zu verifizieren und zu validieren, zum Beispiel durch Simulation von Cyber-Angriffen.

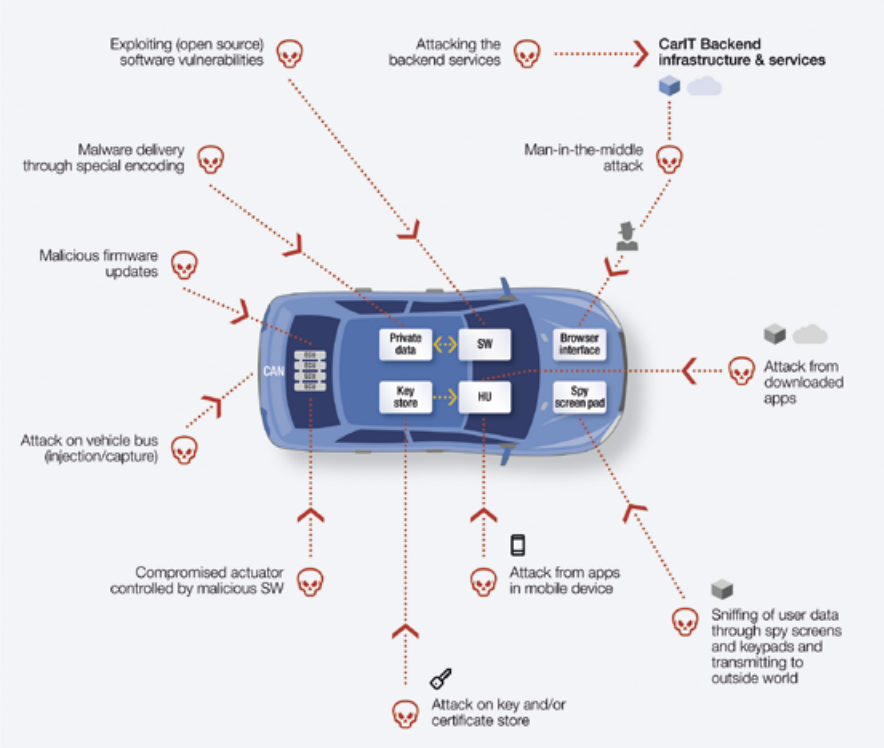


Bild 1. Übersicht der Angriffspunkte eines vernetzten Fahrzeuges (Quelle: NTT)

Digital Twin für Fahrzeuge

Für ein effizientes Software Update Management System ist somit ein Digitaler Zwilling des Fahrzeugs fast schon ein Muss. Sämtliche Informationen zur Software- und Steuergeräte-Konfiguration des Fahrzeugs sind zwar zum Auslieferungszeitpunkt beim Hersteller vorhanden, können sich aber zum Beispiel durch Werkstattaufenthalte oder Unfälle ändern. Daher muss die aktuelle Konfiguration jedes individuellen Fahrzeugs vor der Installation eines Updates geprüft werden, um Voraussetzungen wie Speicherplatz, Bibliotheken, Steuergeräte-Versionen und Kompatibilität sicher zu erfüllen. Mit Konzepten wie App Stores für Fahrzeuge kann zudem im Entertainment-Bereich eine hohe Anzahl komplexer Konfigurationen über den Produktlebenszyklus entstehen.

Die Kombination des Fahrzeug-Zwillings mit dem Fahrprofil des Eigentümers erlaubt weitere Optimierungen im Prozess. So lässt sich zum Beispiel ein Zeitpunkt ermitteln, an dem das Fahrzeug wahrscheinlich nicht benutzt wird, um dann das Update durchzuführen.

Umsetzung über den Produktlebenszyklus

Der Digitale Zwilling für die Software muss sowohl beim Automobilhersteller als auch auf dem einzelnen Fahrzeug verfügbar sein. Der Hersteller baut den Digital Twin in der Produktentwicklung auf und sichert ihn mit virtuellen und physi-

Neue Herausforderungen für OEMs und Zulieferer

Die Automobilhersteller (OEMs) stehen unter großem zeitlichen Druck, das SUMS & CSMS (Software Update Management System & Cyber Security Management System) sowie die zugehörigen Prozesse und Dokumentation zu etablieren und auditieren zu lassen, sobald die UNECE-Regularien finalisiert wurden.

Die Einführung der Software-Identifikations-Nummer (RXSWIN), die über die gesamte Wertschöpfungskette und den kompletten Produktlebenszyklus Bestand haben muss, erfordert eine umfassende Überprüfung und gegebenenfalls Neudefinition von Prozessen – angesichts der vielen involvierten Partner und Zulieferer eine komplexe Anforderung.

kalischen Tests ab. Dabei sind auch die Abhängigkeiten zwischen Steuergeräten und Softwaremodulen sowie deren Lieferanten zu managen. In der Produktion müssen dann je nach Fahrzeugausstattung die passenden Software-Stände und Daten auf die Steuergeräte gebracht werden. Im Aftersales gilt es schließlich, die Händler und Werkstätten mit den aktuellen Versionen zu versorgen.

Basis für diese Prozesse sind IT-Anwendungen zum Software-Konfigurationsmanagement inklusive Kompatibilitätsmanagement. Neben dem Quellcode ist es erforderlich, die ausführbaren Binärdateien sowie weitere Daten zur Parametrierung zu verwalten. Diese Software-Konfiguration ist mit der Produktstruktur in der Entwicklung und Produktion verknüpft. Den Auslieferungsstand der Softwarekonfiguration eines Fahrzeugs kann man als den initialen Stand des Digitalen Zwillings betrachten. Dieser Stand muss nicht nur zentral in Datenbanken des Fahrzeugherstellers verwaltet, sondern auch auf dem Fahrzeug gespeichert werden und abfragbar sein.

Erfolgreiches Automotive OTA

Vom Smartphone kennen wir den Update-Prozess für Software, der üblicherweise vom Benutzer initiiert wird. Neben diesem Pull-Mechanismus ist im Automotive-Bereich auch ein Push-Mechanismus zum Beispiel für Rückrufe und sicherheitskritische Updates nötig. Einige Erfahrungen aus diesem Umfeld sollten auch für Automotive OTA beachtet werden:

- Code signieren: die sichere Herkunft vor der Installation prüfen,
- Updates nur über sichere Kommunikationskanäle übertragen: den Weg von der Cloud zum Gateway/Edge und von dort zum Fahrzeug verschlüsseln,
- Delta-Updates der betroffenen Code-Module: Bandbreiten-Bedarf und Update-Dauer optimieren,
- Automatische Recovery inklusive Rollback: einen funktionsfähigen Stand nach Verbindungsproblemen herstellen.

Ausblick: Digital Twin Computing

Die japanische NTT hat Ende 2019 mit der Digital Twin Computing (DTC)-Initiative erste Forschungsergebnisse vorgestellt, um die Anwendungsgebiete von Digital Twins durch moderne IT deutlich zu erweitern.

Der Unterschied zwischen Digital Twin und DTC ist: Herkömmliche Digitale Zwillinge werden für bestimmte Zwecke erstellt und verwendet. Es ist schwierig, verschiedene Digitale Zwillinge zu kombinieren und in Interaktion zu bringen. Die DTC-Vision erweitert dieses Konzept durch Verschmelzen mehrerer Digitaler Zwillinge in verschiedenen Branchen und durch das Erweitern bestehender Digitaler Zwillinge. So könnten beispielsweise ganze Lieferketten inklusive Fabrikplanung und Logistik abgebildet werden.

Dafür wäre eine enorme Menge an IT-Ressourcen erforderlich. Daher ist eine Infrastruktur, die auf einem „Innovative Optical and Wireless Network (IOWN)“, wie es NTT bietet, ein wichtiger Baustein für die Aktivierung von DTC. Ein solches IOWN verwendet die Zukunftstechnologie Photonik für eine ultraschnelle Datenübertragung.

Die technischen Lösungsbausteine für DTC bilden eine Architektur mit folgenden vier Schichten:

- Cyber/Physical Interaction Layer für die Interaktion zwischen der realen Welt des Menschen und der Dinge mit dem Cyberspace,
- Digital Twin Layer zur Erzeugung und Pflege von Digital Twins,
- Digital World Presentation Layer, in dem Digitale Zwillinge kombiniert werden können,
- Application Layer für die Ausführung von Anwendungen.

Bibliography
DOI **10.3139/104.112335**
ZWF 115 (2020) Special; page 29–31

ISSN 0947–0085

Fazit

„DTC ist eine breite Vision. Wir glauben, dass wir mit vielen Partnern aus vielen verschiedenen Disziplinen zusammenarbeiten müssen, zum Beispiel aus den Sozial- und Naturwissenschaften sowie den Geistes- und angewandten Wissenschaften, um dieses Konzept zu verwirklichen und die Gesellschaft voranzubringen“, so Koya Mori, Senior Research Engineer vom NTT Software Innovation Center in Tokio.

Der Autor dieses Beitrags

Jens Krüger, geb. 1966, ist Diplom-Wirtschaftsinformatiker (FH). Nach dem Studium an der FH Wedel hat er zunächst zehn Jahre in der Engineering IT eines globalen Automobilzulieferers gearbeitet. Seit 1998 ist er beim japanischen IT-Dienstleister NTT DATA in München als Consultant im Bereich Product Lifecycle Management tätig und leitet das globale Engineering Center of Excellence.

Summary

Digital Twin for maximum Cyber Security. Compliance with new UNECE cyber security regulations by using a digital twin of the car Digitization in the automotive industry makes cyber security a focus topic for vehicle software updates – international regulatory bodies are currently working on security guidelines. For vehicle manufacturers, this means that they have to establish processes and systems in accordance with the new cyber security requirements as quickly as possible. Digital Twin Computing can provide significant support in this area. The new Digital Twin Computing initiative from Japan is going beyond the traditional understanding of Digital Twin.

Kontakt

NTT DATA Deutschland GmbH
Hans-Doellgast-Straße 26
80807 München
Tel.: +49 89 9936–1133
Fax: +49 89 9936–1844
Mobil: +49 174 1714336
E-Mail: Jens.Krueger@nttdata.com
www.nttdata.com/de