Key Legal Issues: Automotive Over-The-Air Updates

Date:	5 October 2017
Author:	Timo Littke, Chief Analyst
Publisher:	ATS Advanced Telematic Systems GmbH Germany
Contact:	www.advancedtelematic.com

Takeaways

- Legislation increasingly calls for mandatory over-the-air (OTA) software updates for cars.
- Following U.S. efforts in 2016 to regulate automated and autonomous vehicles, Germany published their own regulations in June 2017. Both parties propose that permanent up-to-date algorithms, localization data and traffic regulations be installed.
- In addition, several nations have published cyber security policies for connected cars addressing the full lifetime of a vehicle which require continuous remote updates.
- On the other hand, OTA updates must adhere to other regulations, especially type approval
- Apart from national legislators, a major international initiative from the UN Task Force on Cyber Security and OTA issues plans to release guidance by the end of 2017, affecting numerous nations.

1 Introduction

Automotive software and firmware updates distributed over the air (OTA) become increasingly important with the rise of the software-defined car, especially to address new cyber security threats as an essential part of lifecycle management.

The automotive industry faces new challenges for cyber security, safety, privacy, liability/customer experience and regulations. Regulators and standardization bodies are under high pressure to provide adequate control and guidance due to the fast pace of innovation. As of today, specific regulations for OTA updates are uncertain. Instead the situation is confusing as OTA updates are affected by diverse – national and international – regulations depending on various criteria.

However, various initiatives are currently underway across the world to enact regulations for automotive over-the-air updates in the near future.

This report gives an overview of current and upcoming regulatory and standardization activities to support parties involved in automotive over-the-air updates. It covers regulatory initiatives from the United Nations, the European Union, Germany, the United Kingdom, the United States of America, and China.

Within this report “automotive industry” mainly refers to passenger light vehicles; regulations and business conditions for commercial and heavy vehicles may differ to some extent.

2 Background

In the future, software and firmware updates for cars will increasingly be provided through wireless connectivity, installed automatically at the end customer and without expert control or supervision. Chiefly, these will affect, or even add, safety-relevant functions for the car's driving behavior.

At a glance: History of automotive software updates

Software has been running in cars for decades. Already in 1968, the Volkswagen1600 got introduced with a computer to control the electronic fuel injection system.[1]

Wider adoption increased the prevalence of electronic control units (ECU) in cars through the 1980s, when re-programming or 'flashing' of ECUs became possible – conducted in a garage by a mechanic, through a cable-connected external testing device.

Eventually, in 2012 Tesla installed the first ever over-the-air update of an operating system in a car[2], followed by numerous other OTA updates like the so called "Autopilot" feature in 2015, which caused controversial discussions about safety and type approval after critical incidents.[3]

Nowadays, due to the development of autonomous cars and the increase of software-related recalls, virtually all car manufacturers prepare for the introduction of OTA updates in series production.[4]

Enabling and requiring over-the-air software and firmware updates comes at the same time as four major game-changers seek to disrupt the automotive industry:

Connected, Autonomous, Shared, Electrified (CASE / ACES)

- **Connectivity of vehicles** for the first time facilitates new features and use cases to update or upgrade the vehicle remotely. But vulnerabilities could also turn into a threat of cyber-attacks which should be fixed immediately with patches installed over the air.
- **Autonomous or automated vehicles** intend to significantly reduce road fatalities. But functional safety always requires the best available driving algorithms and real-time high-definition maps updated continuously.
- **Shared mobility** is based on embedded connectivity within the vehicles. Service operators also demand remote vehicle diagnosis and maintenance capabilities through over-the-air updates to reduce downtime.
- **Electric vehicles** get built on new platforms utilizing new on-board networks and E/E architectures. Without any legacy hindrance, these EVs benefit from being developed from the ground up with remote updatability as a core consideration.

As today's vehicles become more reliant on software, an increasing number of recalls come in the form of software-related problems, such as bugs and cyber security vulnerabilities.[5]

Those disruptions in technology raise their own host of legal issues challenging regulators in collaboration with the automotive industry and other stakeholders to pave the way for secure over-the-air updates.

[1] The New York Times, Aug 27, 1998; www.nytimes.com/learning/teachers/featured_articles/19980827thursday.html / Der Spiegel 38/1967; www.spiegel.de/spiegel/print/d-46462479.html
[2] www.wired.com/2012/09/tesla-over-the-air/
[3] National Transportation Safety Board (NTSB), Report on fatal Tesla crash, Sept. 12, 2017; www.ntsb.gov/news/press-releases/Pages/PR20170912.aspx
[4] IHS Markit; www.ihssupplierinsight.com/shop/product/5002774/over-the-air-updates-real-market-emergence
[5] Strategy Analytics; www.strategyanalytics.com/strategy-analytics/blogs/automotive/infotainment-telematics/infotainment-telematics/2017/08/25/software-is-eating-the-auto-industry

3 Realm of regulations for Automotive OTA Updates

Automotive OTA updates can be sent to and installed in a connected vehicle during all phases of its lifecycle. Which regulations have to be considered in the context of an update depends on the phase. De jure, the phases are defined by particular contractual events which usually follow a chronology:

1. Type Approval (TA)
2. Certificate of Conformity (CoC)
3. Sale of vehicle by OEM
4. Vehicle registration

The legal consequences, on the other hand, depend on the reason and impact of the update. This also includes the distinction between whether an update is mandatory, e.g. in case of a software-related recall, or if it is voluntary, e.g. installation of a function on demand (FOD) on customer request.

Furthermore, various legal entities and therefore several sorts of regulations are affected:

The vehicle itself

Vehicles have to comply with relevant safety and environmental standards to be approved for usage on public roads. The primary goal of regulations for road vehicles and traffic is to ensure safety and protect human life.[6] Furthermore they provide legal certainty for liabilities and should consider social welfare, economic wealth and technological progress.

The vehicle owner or user

Besides functional safety, connectivity and access to consumer devices (vehicles) also invokes consumer protection and data privacy. Those fields of law are often controlled by different bodies from traffic and vehicles.

Society and third parties

All the above-named parties acknowledge that cyber security is crucial to protect consumers and vehicles against hacks and malfunctions, especially as those might harm third parties as well. Therefore many working groups address automotive cyber security in conjunction with over-the-air updates.

In addition, OTA software updates might have an impact on type approval values (engine power, CO2 emissions, pollutant emission level, etc.) used for purposes such as taxation or the implementation of transport policies such as low emission zones, etc. This might also affect the vehicle registration and oblige the owner to take action to update the registration. In this case several regulations will be involved and the OEM as well as the owner will have to act accordingly.

Vehicle regulations are requirements that automobiles must satisfy in order to be sold in a particular country. They are usually mandated by legislation, and administered by a government body, for example the United Nations Economic Commission for Europe (UNECE) at an international level, or the US National Highway Traffic Safety Administration (NHTSA) at a national level.

[6] cf. United Nations Convention on Road Traffic, 1968: „ Contracting Parties, desiring to facilitate international road traffic and to increase road safety through the adoption of uniform traffic rules, […]"; www.unece.org/index.php?id=26749

4 United Nations

The United Nations (UN) with its units and working parties (WP) play a vital rule for the global regulations of road traffic and road vehicles. Notably two WPs shape the regulatory framework:

- The Working Party on Road Traffic Safety (WP.1) is the only permanent body in the United Nations system that focuses on improving road safety.
- The World Forum for harmonization of vehicle regulations (WP.29) is a unique worldwide regulatory forum to establish regulatory instruments concerning motor vehicles.

Global importance of UNECE WP.29

The **United Nations Economic Commission for Europe (UNECE)** was established in 1947.[7] It initially included all participants in the reconstruction of post-war Europe and later increased **globally to 56 member States**.[8]

In 1952 it set up the **World Forum for Harmonization of Vehicle Regulations (WP.29)** as a subsidiary body of the Inland Transport Committee (ITC), which is the highest policy-making body of the UNECE in the field of transport.[9] WP.29 is tasked with the worldwide harmonization and development of technical regulations for vehicles to facilitate international trade.

WP.29 in 1958 released the "Agreement Concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of **Approval for Motor Vehicle Equipment and Parts**" ("**1958 Agreement**"). If a vehicle or component received **type approval** by any of the contracting parties to the 1958 Agreement, all other contracting parties will recognize this approval.[10]

Currently the **1958 Agreement has 54 contracting parties**, e.g.:[11]

Australia, Austria, Belgium, Czech Republic, Denmark, Egypt, European Union, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Russian Federation, South Africa, Spain, Sweden, Switzerland, Thailand, Tunisia, Turkey, Ukraine, United Kingdom

(Notable non-signatories: Brazil, Canada, China, India, United States of America)

Eventually, WP.29 with the subsequent **1998 Agreement** introduced **Global Technical Regulations (UN GTR)** without requiring type approval and mutual recognition of type approvals. This attracted new contracting parties, notably Canada, China, India, and the USA.[12]

The **Transatlantic Trade and Investment Partnership (TTIP)** is a trade agreement between the European Union and the United States under negotiations. It intends to create a transatlantic market for cars and trucks with harmonized regulations and safety standards.[13] Currently the negotiations are paused since the election of the new US government.

[7] www.unece.org/mission.html
[8] as of 26 September 2017; www.unece.org/oes/nutshell/member_States_representatives.html
[9] www.unece.org/trans/welcome.html
[10] http://www.unece.org/trans/main/wp29/faq.html
[11] ECE/TRANS/WP.29/343/Rev.25; www.unece.org/trans/main/wp29/wp29wgs/wp29gen/wp29fdocstts.html
[12] as of 26 September 2017; www.unece.org/trans/maps/un-transport-agreements-and-conventions-20.html
[13] http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_153012.4.9 Vehicles.pdf

4.1 UN Task Force on Cyber security and OTA issues

In early 2016, the United Nations Economic Commission for Europe (UNECE)[14] formed the UN Task Force on Cyber security and OTA issues (UN TF-CS/OTA).[15]

The UN TF-CS/OTA was established under the Intelligent Transport Systems and Automated Driving (ITS/AD)[16], an Informal Working Groups (IWGs) of the World Forum for Harmonization of Vehicle Regulations (WP.29).[17]

The scope of the UN TF CS/OTA is the development of guidance providing recommendations on automotive cyber security and software updates by the end of 2017; possibly not until March 2018. This might turn into an amendment or annex of a resolution of the UNECE in the future.

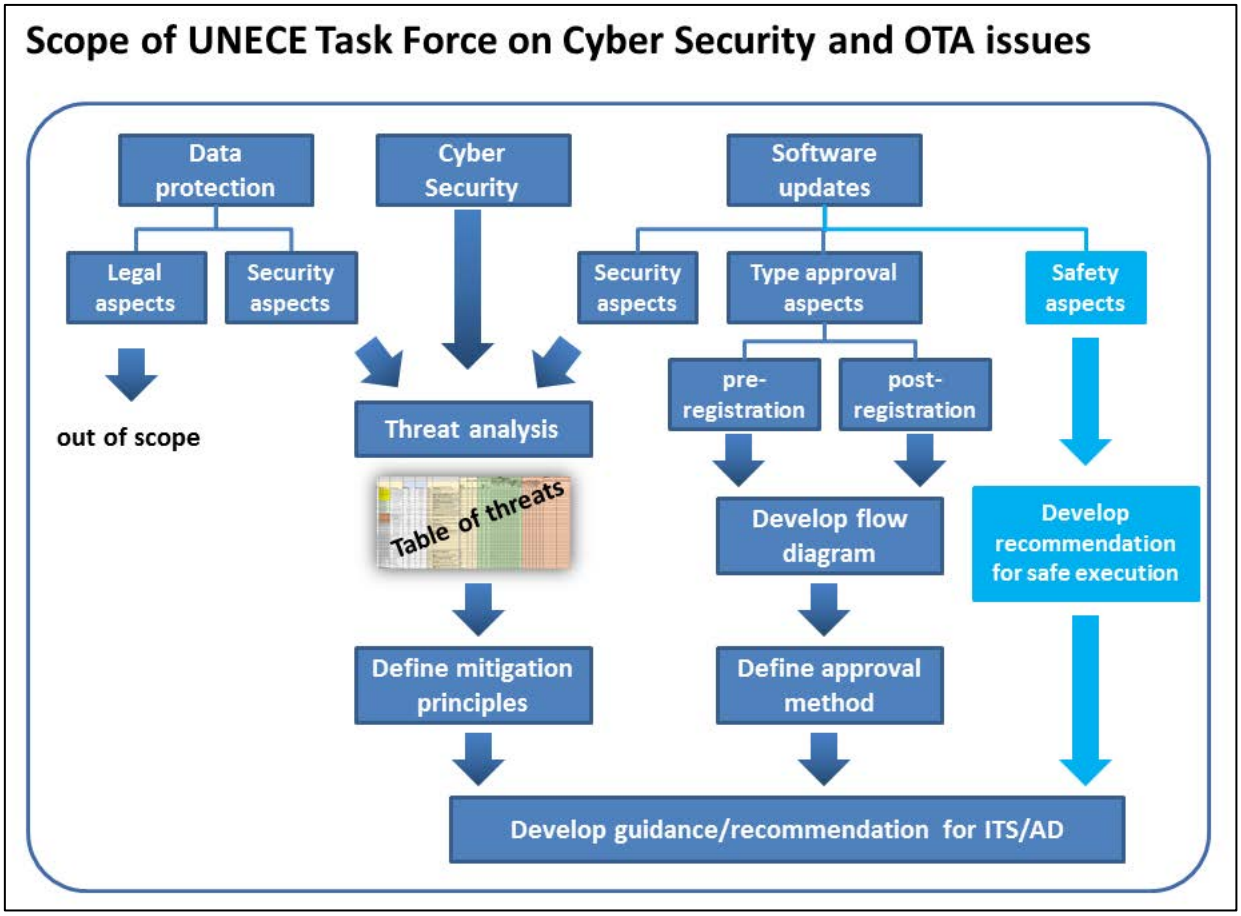


Figure 1: Scope of UNECE Task Force on Cyber Security and OTA issues[18]

The UN TF CS/OTA sees broad international engagement. Various stakeholders participate, e.g. national Type Approval Authorities (TAA), the automotive industry (OICA) and consumer lobby groups (e.g. FIA). From the TAA perspective, especially Germany, Japan, Netherlands, and the UK drive the process. From OICA standpoint, mainly European and Japanese car makers engage. The task force further has the support of the US and China.

Remarkably, the U.S. Department of Homeland Security presented its "UPTANE Secure Over-the-Air (SOTA) project" on how to perform software updates securely, including suppliers and OEMs, within the automotive industry.[19] It is the sole security framework discussed in the TF so far.

[14] www.unece.org
[15] https://wiki.unece.org/pages/viewpage.action?pageId=40829521
[16] https://wiki.unece.org/pages/viewpage.action?pageId=2523344
[17] https://wiki.unece.org/pages/viewpage.action?pageId=2523340
[18] Status report of TF-CS/OTA for IWG ITS/AD; https://wiki.unece.org/pages/viewpage.action?pageId=44269826
[19] (USA) UPTANE project overview ; https://wiki.unece.org/download/attachments/44269826/TFCS-06-15-Rev1%20%28USA%29%20UPTANE%20overview.pdf

Cyber Security

The TF in a working paper collected a list of 86 examples of vulnerability or attack methodologies with appropriate mitigations for connected cars. This includes a section for the misuse of updates, like the compromise of over-the-air software update procedures.[20]

The TF prepares a paper consolidating the analysis of cyber securities with the aim to create guidance for mitigations based on international security standards.

The Consolidated Resolution (R.E. 3), already incorporating the ITS/AD guideline on Cyber Security for Connected and Automated, was identified as a document to make the results publicly available.

Software Updates

The UN TF CS/OTA considers for OTA updates both security requirements and consequences for type approval. It is currently under discussion how the manufacturer must protect the software against manipulation and how to verify the integrity of the software.

The TF notes that OTA updates would fall into the realm of post-registration updates and that it has considered any software update to a type approved system. However, details and classifications have to be defined if and when an OTA update after type approval and registration will be an extension to an existing type approval or a "retrofit" approval for the vehicle already in use. As modifications to registered vehicles are covered solely by national legislation, the TF may provide recommendations for TAA only.

The TF will introduce a Regulation-linked Software Identification Number (RxSWIN). Merely the implementation is still discussed controversially. The Dutch TAA proposed for a new standalone Software Regulation.[21] In contrast the OICA/CLEPA prefers to introduce the RxSWIN in each relevant Regulation.[22]

The TF will evaluate for further proceedings the options guideline vs. regulation.

Impact for automotive OTA updates

> The UN TF CS/OTA has strong influence due to its structure and participants. Even if it will publish a non-binding guidance initially, it is foreseeable that it will turn into some form of national or international regulation at a later date addressing cyber security and type approval for OTA updates.

Type Approval for vehicle parts or whole vehicles

So far, the 1958 Agreement aims at type approval of vehicle parts solely. Therefore, under WP.29 an Informal Working Group (IWG) was established for **International Whole Vehicle Type Approval (IWVTA)** to develop UN R0 for type approval of full vehicles. UN R0 might be enacted in 2019[23]

The EU already has the **European Community Whole Vehicle Type Approval (ECWVTA)** in place but only applicable for its member states (Directive 2007/46/EC).[24]

[20] TFCS-08-03 (Sec) Mitigations table - cleaned.xlsx ; https://wiki.unece.org/download/attachments/46792870/TFCS-08-03%20%28Sec%29%20Mitigations%20table%20-%20cleaned.xlsx
[21] TFCS-07-05 (NL) Draft software regulation.docx; https://wiki.unece.org/download/attachments/46792867/TFCS-07-05%20%28NL%29%20Draft%20software%20regulation.docx
[22] TFCS-ahSU2-02-Rev1 (OICA-CLEPA) Draft position on NL proposal for a UN Software Regulation.pptx; https://wiki.unece.org/download/attachments/51973131/TFCS-ahSU2-02-Rev1%20%28OICA-CLEPA%29%20Draft%20position%20on%20NL%20proposal%20for%20a%20UN%20Software%20Regulation.pptx
[23] https://wiki.unece.org/pages/viewpage.action?pageId=2523342
[24] http://ec.europa.eu/growth/sectors/automotive/technical-harmonisation/eu_de

5 European Union

The European Union (EU) aims, among other things, to ease trade across its member states and to harmonize consumer protection. Thus, the EU on the one hand enacts its own regulations and on the other hand is signatory to several agreements and regulations of the UNECE which affect its members.

Impact of UN Regulations (UN-Rx)

Technical definitions for type approvals are regulated in 142 **UN Regulations (UN-Rx)** appended to the 1958 Agreement.[25] UN Regulations are not applicable on a mandatory basis, but if a Contracting Party decides to apply a UN Regulation, the adoption becomes a binding act.

The European Union can apply to UN Regulations in the way they become binding for each EU member state without further adoption into national law.

One prominent example is the **UN-R79 (Steering equipment)**. Until now, UN-R79 has been the primary regulatory hurdle for the type approval of automated vehicles. It only allows automated steering up to a speed of 12 km/h.[26] Currently this limitation is under discussion, to allow for e.g. highway autopilot or Audi's A8 Traffic Jam Pilot.

5.1 ''Cybersecurity Act''

In September 2017, the European Commission issued a proposal for a regulation on an "EU Cybersecurity Agency", building on the European Agency for Network and Information Security (ENISA).[27] This agency will put in place and implement an EU cybersecurity certification framework (''Cybersecurity Act'') that will ensure the trustworthiness of IoT devices, namely connected cars. "Cybersecurity certificates will be recognized across Member States, thereby cutting down on the administrative burden and costs for companies."[28]

Impact for automotive OTA updates:

> If the proposal gets adopted, the regulations will be directly applicable in all EU countries. For now, the use of the certification will be voluntary. Future EU legislation may prescribe an EU certificate as a mandatory requirement.

5.2 Protection of privacy

As of May 2018, the General Data Protection Directive (GDPR) will apply directly in all European member states.[29]

The data collected by connected vehicles (location data, sensor data, etc.) are regularly deemed as "personal data" according to the GDPR. This follows from the fact that most data collected by cars is linked to the vehicle identification number ("VIN"), which in turn is linked to the owner.

A car maker could most likely receive user consent under a contract for preemptive maintenance or other over-the-air updates. However, the OEM should consider technical measures like anonymization or pseudonymization.

[25] www.unece.org/trans/main/wp29/wp29regs.html
[26] www.unece.org/fileadmin/DAM/trans/main/wp29/wp29regs/R079r2e.pdf
[27] https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en
[28] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework
[29] Regulation (EU) 2016/679; http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Vehicle Registration & the Vehicle Identification Number (VIN)

Vehicle registration with a government authority is required before using the vehicle on the road. Prerequisite for the registration is the type approval of the vehicle. Hence registration ensures that the vehicle is type approved, that necessary insurances exist and to link the vehicle with its owner or user. This link will be used for taxation, crime detection or notification in case of a recall.

All motor vehicles are uniquely identified by a vehicle identification number (VIN), also called a chassis number. Consequently, the VIN directly relates to one person.

6 Germany

Germany is a member state of the EU and contracting party to major agreements and regulations of the UN. Therefore, the legal framework in Germany in many ways depends on the superior regulations, e.g. for type approval on the Agreement 1958 and the annexed UN-Rx and for traffic regulations on the Vienna Convention. Nevertheless, those international treaties require the adoption of implementing legislation to become effective as a matter of domestic law.

Germany is actively contributing to the relevant international bodies as well as driving its national strategy for digitization, which also incorporates the "Strategy for Automated and Connected Driving" of the German Federal Ministry of Transport and Digital Infrastructure (Bundesministerium für Verkehr und Digitale Infrastruktur, BMVI).[30]

6.1 Law on automated driving

In general, automated or even autonomous driving is mainly governed by the applicable road traffic regime in Germany. The latter is based on German national law but is also strongly influenced by European and international law.

Consequently Germany effectuated an Act to implement the amendment to the Vienna Convention on Road Traffic in December 2016 (Act to Amend Articles 8 and 39 of the Convention on Road Traffic of November 8, 1968), which served as a basis for legalizing autonomous vehicles.

In May 2017, both houses of the German parliament (Bundestag and Bundesrat) approved the amendments to the German Road Traffic Act (Straßenverkehrsgesetz, StVG) to allow automated driving, which became effective as of June 2017.

To ATS, the BMVI explained that an automated vehicle must be able to meet all current traffic regulations (Straßenverkehrsordnung, STVO) at all times, just like a human driver. This applies over the full lifetime of the car.

The German government stated in its notes to the German Road Traffic Act: "Importance and frequency of software updates will increase with wider adoption of automated vehicles".[31]

They expect the industry will ensure that in-car software is up to date over the entire lifetime of a vehicle without being mandated by a regulation.

Impact for automotive OTA updates:

> The German Federal Government is well aware of the importance of software updates for automated vehicles. It even requires that current regulations be installed in the vehicle at any given time, which is in practice possible only with over-the-air updates. Nevertheless, at this stage it avoids mandating OTA updates, presumably to avoid dictating a specific technology.

[30] www.bmvi.de/SharedDocs/EN/publications/strategy-for-automated-and-connected-driving.pdf
[31] http://dip21.bundestag.de/dip21/btd/18/115/1811534.pdf

Vienna Convention on Road Traffic

The **Convention on Road Traffic was signed 1968 in Vienna**, commonly called “Vienna Convention” (VC), under control of the United Nations Economic and Social Council (ECOSOC). It has been ratified by 74 countries.[32] The UNECE **Global Forum for Road Traffic Safety (WP.1)** is responsible for amendments to the VC.[33] The VC is designed to harmonize international traffic rules and to increase road safety.

On 23 March 2016, following amendment to the VC was enacted, enabling automated driving.[34]

Article 8, paragraph 5bis:

“Vehicle systems which influence the way vehicles are driven and are not in conformity … shall be deemed to be in conformity … when such systems can be overridden or switched off by the driver.”

In other words: “Automated driving technologies transferring driving tasks to the vehicle will be explicitly allowed in traffic, provided that these technologies are in conformity with the United Nations vehicle regulations or can be overridden or switched off by the driver.”[35]

In Germany the Lower House of Parliament (Bundestag) applied the amendment Article 8, paragraph 5bis VC on 29 September 2016.[36]

This adoption gave legal certainty for new automated driving functionalities and even existing advanced driver assistance systems (ADAS) like autonomous cruise control (ACC).

Based on the Vienna Convention, additional UN Regulations have to be modified to pave the way for type approval of automated vehicles, e.g. UN-R79.

6.2 Ethics Committee

The BMVI appointed an Ethics Commission for "automated and connected driving". In June 2017 it published a report with 20 principles for level 4/5 of automated driving.[37]

The commission emphasized that product liability guidelines will oblige car makers to update self-driving systems over their entire lifecycle. Furthermore, the commission proposes a check against a backend before setting off on a journey, to ensure that all critical software updates have been successfully installed. It again reflects the awareness at the German government of the need for OTA updates.

Eventually in August 2017 the German government enacted an action plan to implement these principles of the Ethics Commission for "automated and connected driving".[38]

[32] www.unece.org/trans/conventn/legalinst_08_rtrss_rt1968.html
[33] www.unece.org/trans/main/welcwp1.html
[34] www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/ECE-TRANS-WP1-145e.pdf
[35] www.unece.org/info/media/presscurrent-press-h/transport/2016/unece-paves-the-way-for-automated-driving-by-updating-un-international-convention/doc.html
[36] http://dip21.bundestag.de/dip21/btd/18/097/1809780.pdf
[37] Full report (German): www.bmvi.de/SharedDocs/DE/Pressemitteilungen/2017/084-dobrindt-bericht-der-ethik-kommission.html | Short version (English): www.bmvi.de/SharedDocs/EN/PressRelease/2017/084-ethic-commission-report-automated-driving.html
[38] www.bundesregierung.de/Content/DE/Artikel/2017/08/2017-08-23-ethik-kommission-regeln-fahrcomputer.html

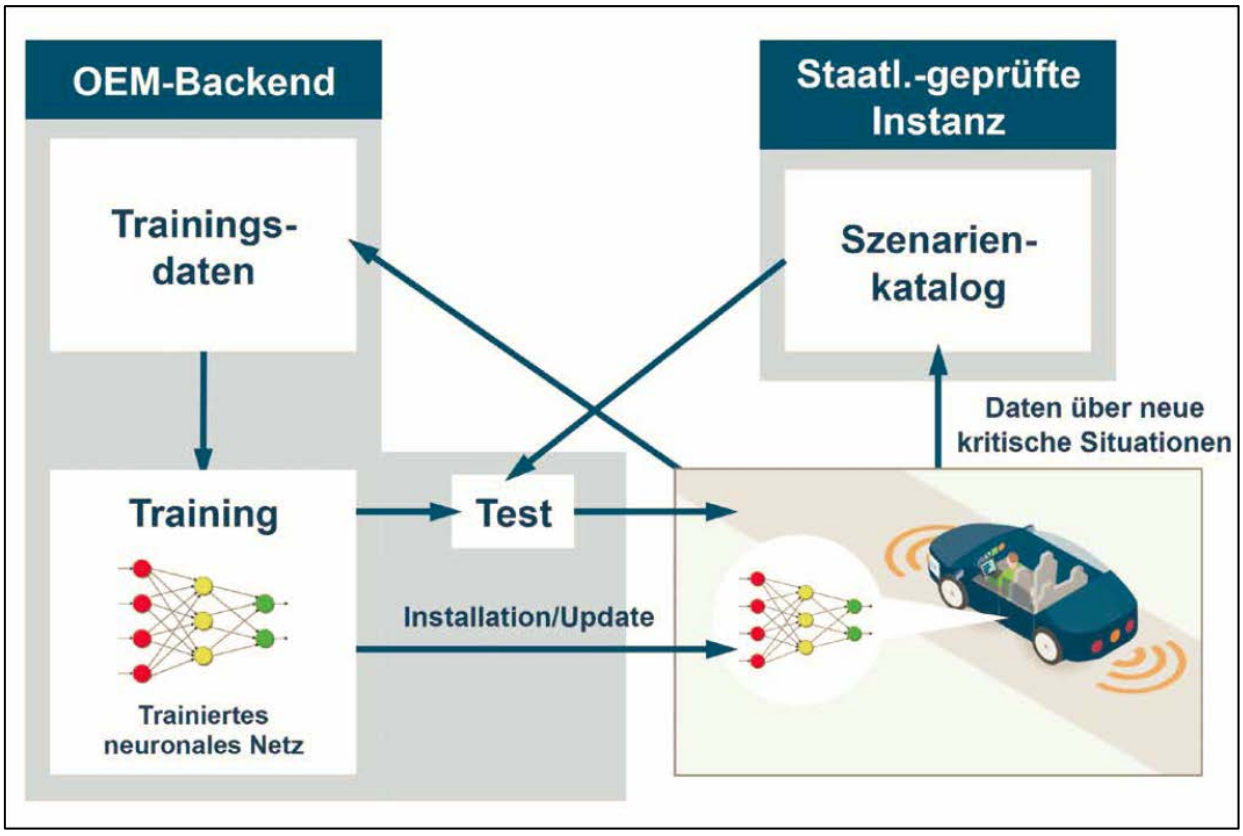


Figure 2: Principle for OTA backend check for automated vehicles (Report of Ethics Commission of BMVI, 2017)

Impact for automotive OTA updates

> The Ethics Commission's principles are non-binding, but relevant as they focus on the protection of the human being. They could potentially provide orientation for German courts regarding liability issues, which might involve questions about whether software is updated correctly in the car.

6.3 Allowance of OTA updates for recalls

Car manufacturers may be held liable under the strict liability regime of the German Product Liability Act (Produkthaftungsgesetz) for any damage occurring from a product defect. A recall is a procedure to eliminate dangers resulting from a faulty vehicle. The car manufacturer has to report recalls to the Federal Motor Transport Authority (Kraftfahrt-Bundesamt, KBA). In case of minor faults, the recall might be voluntary. With severe dangers, however, the KBA will mandate it.[39]

The KBA can require a success rate tied to a deadline. If the car maker doesn't achieve this goal, the KBA can fine them as well as reject the type approval.

Therefore, all parties have a strong interest to fulfill the recall efficiently.

The KBA explained in a meeting with ATS that they accept for recalls any feasible way to fix the defect, namely over-the-air updates under consideration of regulations for type approval.

[39] § 26 Abs. 2 ProdSG

7 United Kingdom (UK)

UK is a contracting party to major agreements and regulations of the UN. Therefore, the legal framework in UK in many ways depends on the superior regulations, e.g. for type approval on the Agreement 1958 and the annexed UN-Rx and for traffic regulations on the Vienna Convention.

The UK body developing definitive core specifications is the Department for Transport (DfT).

7.1 Automated and Electric Vehicles Bill

The UK government in February 2017 proposed the “Vehicle Technology and Aviation Bill 2016-17” (Bill 143). It proposed the insurer’s liability for automated vehicles and that it may be excluded or limited in case of “a failure to install software updates to the vehicle’s operating system that the insured person is required under the policy to install or to have installed" (Bill 143, Part 1, paragraph 4). Then Bill 143 was dropped when Parliament was dissolved after the calling of the 2017 General Election.[40]

However, its core proposal of motor vehicle insurance to cover the use of automated vehicles has been carried forward into the new “Automated and Electric Vehicles Bill” as part of the Queen's Speech on 21 June 2017.[41]

Impact for automotive OTA updates

> Even if the Automated and Electric Vehicles Bill is not drafted yet, the core principles of insurance for automated vehicles are known from the formerly proposed bill. If it gets enacted, secure and reliable software updates will become crucial for liability determination.

7.2 Principles of cyber security for connected and automated vehicles

In August 2017, the DfT published eight key principles as cyber security guidelines for connected and automated vehicles.[42]

Therein the UK government demand secure software updates over the vehicle lifetime for connected and automated vehicles. Principle 6 states:

"The security of all software is managed throughout its lifetime." ... "It must be possible to ascertain the status of all software, firmware and their configuration, including the version, revision and configuration data of all software components." ... "It is possible to safely and securely update software and return it to a known good state if it becomes corrupt."

Principle 1.2 emphasizes its importance: “Personal accountability is held at the board level...”

Impact for automotive OTA updates

> These principles are not binding as of yet. But the UK government with the recent bill defined a wider push on the development of connected and automated vehicles. Therefore, the principles might be considered as integral part of upcoming regulatory framework for autonomous and connected cars.

[40] https://services.parliament.uk/bills/2016-17/vehicletechnologyandaviation.html
[41] www.gov.uk/government/publications/queens-speech-2017-what-it-means-for-you/queens-speech-2017-what-it-means-for-you
[42] www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

Principle 6

The security of all software is managed throughout its lifetime.

Principle 6.1:

Organisations adopt **secure coding practices** to proportionately manage risks from known and unknown vulnerabilities in software, including existing code libraries. Systems to manage, audit and test code are in place.

Principle 6.2:

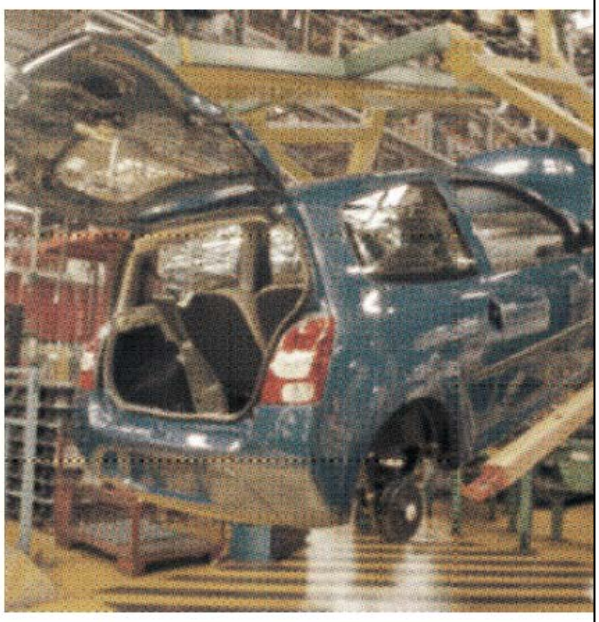
It must be possible to ascertain the status of all software, firmware and their configuration, including the version, revision and configuration data of all software components.

Principle 6.3:

It is possible to **safely and securely update software** and return it to a known good state if it becomes corrupt.

Principle 6.4:

Software adopts **open design practices** and peer reviewed code is used where possible. Source code is able to be shared where appropriate.



References: Microsoft SDL, SAFE Code best practices, OWASP CLASP, ISO 12207, PAS 754

13

Figure 3: Principles of cyber security for connected and automated vehicles (UK DfT)

8 United States of America (USA)

The USA tends to act independently. Even as a founding member of the UNECE, they didn't sign the 1958 Agreement, but only the 1998 Agreement. This is due to their unique approach of applying self-certification instead of type approval. Furthermore, in the US several federal regulations compete with state law.

8.1 Automated Driving Systems 2.0: A Vision for Safety

On September 20, 2016, the NHTSA in support of the U.S. Department of Transportation (DOT) released its Federal Automated Vehicles Policy (FAVP) for the testing and deployment of highly automated vehicles (HAVs) on public roads.[43] NHTSA envisions that manufacturers will make significant changes to the capability of the automated vehicle system also by over-the-air software updates. Therefore, it allows for software updates, also OTA updates and post-sale software updates which may change levels of automation over the vehicle's lifecycle.

In September 2017 NHTSA replaced FAVP with the new guidance "Automated Driving Systems 2.0: A Vision for Safety".[44]

NHTSA replaced its 15-point "Safety Assessment" from FAVP with 12 safety design elements for Automated Driving Systems (ADSs) – maintaining the important role of software updates. They "apply to both ADS original equipment and to [...] updates (including software updates/ upgrades) to ADSs".

System safety (1.) requires processes to "detect and correct unexpected results from software updates". For vehicle cybersecurity (7.) entities should "establish robust cyber incident response plans". Considering the varying federal, state, and local laws (12.) vehicles "should be able to follow all laws that apply to the applicable operational design domain".

On the one hand a Vision for Safety calls for remote updates to comply with all safety elements. On the other hand it also recommends state officials for registrations to "consider requiring notification of ADS upgrades if the vehicle has been significantly upgraded post-sale."

NHTSA announced: "This work lays the groundwork for the Department to launch FAVP 3.0". [45]

Impact for automotive OTA updates

> With a Vision for Safety, NHTSA clearly confirms its commitment made with FAVP to support OTA updates even for updating safety-relevant driving control functionalities in highly automated vehicles. Albeit voluntary, this federal policy strengthens the position of car manufacturers against more restrictive state laws.

8.2 UPTANE automotive OTA update security framework

The U.S. Department of Homeland Security (DHS) in October 2016 made following statement:

"The ability to update vehicle software is essential to both safety and security, but it also could be a key attack vector for adversaries."[46]

Preceding to that statement, DHS undertook a cyber security evaluation and thereupon funded a joint research project with New York University (NYU), the University of Michigan Transportation

[43] www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf
[44] www.nhtsa.gov/document/automated-driving-systems-20-voluntary-guidance
[45] www.nhtsa.gov/es/manufacturers/automated-vehicles-manufacturers
[46] www.dhs.gov/science-and-technology/news/2016/10/13/snapshot-cybersecurity-needed-autos-too

Research Institute (UMTRI) and Southwest Research Institute (SwRI) to secure vehicle software updates.

The security researchers , with input from major vehicle manufacturers and suppliers, developed Uptane, the "first compromise-resilient software update security system for automotive".[47]

During a workshop of FTC and NHTSA in June 2017[48], over-the-air updates were seen as a necessary tool for connected cars. Uptane was discussed as an appropriate approach.[49]

The US government also presented Uptane at the UN Task Force on Cyber security and OTA issues.[50]

Impact for automotive OTA updates

> Considering the funding from DHS for Uptane, in addition with the promotion at national and international regulatory bodies, no other OTA security framework sees comparable publicity and institutional support. As Uptane is developed as an open standard with open source reference implementations, it might increase adoption.

8.3 Restrictions for OTA updates in the USA by dealership laws

Car makers (OEMs) in the USA face difficulties when providing direct OTA updates to vehicles due to certain state franchise laws regulating relationships between OEM and dealership.

Lobby groups at the national and state level pressure state legislatures to protect dealer business.[51] Any challenge to dealer profit margin, including repairs, servicing, financing, is met with strong opposition. As a result, direct retail sales channels or other competition from OEMs to dealer business is prohibited in most states.[52]

Legacy OEMs face more resistance when offering OTA updates directly, be they service updates paid for by the OEM or value-added updates where the customer pays directly to OEM: dealers are mandated to receive their cut.[53]

In contrast, Tesla overcomes those burdens by selling vehicles directly without a dealer network to compete with. This limits Tesla in setting up retail locations in many states, but allows them to distribute OTA updates without restrictions.

The situation reflects ongoing controversy between levels of government and various agencies. The Federal Trade Commission (FTC) staunchly opposes current dealer protection and seeks to remove anti-competition regulation for the benefits of consumers and automakers.[54]

8.4 Federal Motor Vehicle Safety Standards (FMVSS)

Federal Motor Vehicle Safety Standards (FMVSS) are a set of standards developed and enforced by the National Highway Traffic Safety Administration (NHTSA) pursuant to authorization by the National Traffic and Motor Vehicle Safety Act.[55]

[47] https://uptane.github.io/
[48] www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected
[49] www.ftc.gov/system/files/documents/videos/connected-cars-privacy-security-issues-related-connected-automated-vehicles-part-3/ftc_connected_cars_transcript_segment_3.pdf
[50] (USA) UPTANE project overview ; https://wiki.unece.org/download/attachments/44269826/TFCS-06-15-Rev1%20%28USA%29%20UPTANE%20overview.pdf
[51] National Automobile Dealers Association (NADA); www.nada.org
[52] Example State Law: Michigan Public Act 354; www.legislature.mi.gov/documents/2013-2014/publicact/pdf/2014-PA-0354.pdf
[53] www.arstechnica.com/cars/2017/07/gm-to-offer-ota-software-updates-before-2020-but-only-for-a-new-infotainment-platform
[54] www.ftc.gov/news-events/blogs/competition-matters/2015/05/direct-consumer-auto-sales-its-not-just-about-tesla
[55] https://en.wikipedia.org/wiki/Federal_Motor_Vehicle_Safety_Standards

On December 13, 2016, NHTSA released **FMVSS No. 150** for public comment. This new safety standard would mandate V2V Communications on new light-duty vehicles and passenger cars.[56]

The Standard No. 150 requires OTA updates for certificates and software to ensure security and safety:[57]

“The agency is also proposing to require that vehicles be capable of receiving over-the-air (OTA) security and software updates” [...]

“V2V devices allow for over-the-air (OTA) software and certificate updates [...] The agency believes that over-the-air devices updates will be viable and commonplace by the time a final rule to this proposal is finalized. We anticipate this highest potential for periodic updates will come in two primary forms: device software updates and security credential updates.“ [...]

“Over the air updating will provide significant flexibility for updates, not only to V2V devices but many vehicle-resident components” [...]

“Given that V2V operational and security software may need to be updated securely and widely while systems are in service, it may be unreasonable to expect that non-OTA software updates may have the desired impact and effectiveness (based on experiences in non-OTA domains for recalls).” [...]

“Because false positive issues with V2V-based safety applications are typically a software issue rather than a hardware issue. Manufacturers may even be able to solve by deploying solutions to such problems through over-the-air software updates, rather than requiring vehicles to be brought in for adjustment.”

Impact for automotive OTA updates

> The FMVSS No. 150 currently is a proposal. The moment it gets enacted it will deeply integrate mandatory OTA updates into all new vehicles in the USA. As it will be used for safety-critical purposes, the security requirements are evident.

[56] www.federalregister.gov/documents/2017/01/12/2016-31059/federal-motor-vehicle-safety-standards-v2v-communications
[57] www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/v2v_nprm_web_version.pdf

Dominating principles of type approval vs. self-certification

Vehicles which are sold and put into service require (depending on the country) either prior type approval or self-certification by the manufacturer or importer. Both processes provide mechanisms for ensuring that vehicles meet relevant environmental, safety and security standards.

A) Type Approval (Homologation)

One production vehicle is tested as being representative of the 'type'. Once all of the system and component approvals are in place, the vehicle will be considered as a whole by a national **Type Approval Authority (TAA)**.

An initial assessment by the TAA verifies the quality standards (e.g. ISO 9001 or ISO/TS 16949) at the manufacturer's production plant ensuring that vehicles or components when in production will conform to the approved type. The TAA then grants the **Conformity of Production (COP)**.

An independent technical institute certifies if a representative example of a type meets the relevant regulations. If the certification and the COP are in place, the TAA grants type approval.

Once type approval has been granted, the manufacturer will be responsible for ensuring COP. He issues a **Certificate of Conformity (CoC)** for each vehicle produced of that type which documents the existing type approval. A CoC ensures the free movement of a car within the territory of application.

Globally the majority of nations follow the 1958 Agreement for type approval.

China has its own type approval denoted by the China Compulsory Certificate mark (CCC Mark). It gets testified by the China Certification Centre for Automotive Products (CCCAP).[58]

B) Self-certification

The United States and Canada are the two significant exceptions, virtually alone in the world, without type approval but with self-certification.[59] Here the manufacturer or importer has to "self-certify" that his vehicle system or parts comply with the US Federal Motor Vehicle Safety Standards (FMVSS)[60] – respectively Canada Motor Vehicle Safety Standards (CMVSS)[61] – and applicable regulations from U.S. Environmental Protection Agency (EPA).[62]

[58] https://en.wikipedia.org/wiki/China_Compulsory_Certificate
[59] https://en.wikipedia.org/wiki/World_Forum_for_Harmonization_of_Vehicle_Regulations
[60] https://one.nhtsa.gov/cars/rules/import/FMVSS/index.html
[61] Motor Vehicle Safety Act (1993, c. 16) https://www.tc.gc.ca/eng/acts-regulations/acts-1993c16.htm
[62] www.epa.gov/vehicle-and-engine-certification/overview-certification-and-compliance-vehicles-and-engines

9 China

China has an exceptional role as it severely limits its adoption of the UNECE agreements and only signed the 1998 Agreement. Furthermore, it observes a national type-approval process which does not permit foreign type approvals.

So far China's legal and regulatory system does not address key legal issues arising from connected and autonomous cars. However, in 2017 China released two legislative initiatives, and it remains to be seen how they will affect cyber security and over-the-air updates for connected cars.

Intelligent & Connected Vehicles

In June 2017 the Ministry of Industry and Information Technology (MIIT) and the Standardization Administration of China (SAC) issued draft Guidelines for the Establishment of National Standards System of Telematics Industry (Intelligent & Connected Vehicles).[63]

It plans low-level automated driving for 2020 and high-level automated driving for 2025 in accordance with standards for functional safety and information security.

Cybersecurity law

In June 2017 the Cyber-security Law of the People's Republic of China (the "Law") was enacted. The Cyberspace Administration of China (CAC) issued regulations focusing on Network operators with "critical information infrastructures"(CIIs), which also includes information infrastructures for transportation. It defines prohibitions and security assessments for cross-border transfers of local data outside of China.

In addition, the National Information Security Standardization Technical Committee (TC260) published a series of draft technical standards for the implementation of the Law.[64]

[63] http://www.chinalawinsight.com/2017/06/articles/corporate/china-put-self-driving-cars-into-gear/
[64] Chinese draft: www.tc260.org.cn/zqyj.jsp

Questions?

Please visit www.advancedtelematic.com

Or get in contact:
ATS Advanced Telematic Systems GmbH
Kantstrasse 162
10623 Berlin
Germany
Tel.: +49 30 959 997 540
Email: ats.berlin@advancedtelematic.com

Author:
Timo Littke, Chief Analyst

About ATS Advanced Telematic Systems

ATS Advanced Telematic Systems is a German automotive-focused software company specializing in open source and open standards based software solutions for the mobility industry.

ATS developed OTA Plus, the only open source client/server solution for over-the-air software updates for OEMs and Tier1s.

ATS collaborates with international industry alliances of leading automotive OEMs and suppliers: it is the first cloud-only service provider to be accepted into the German Association of the Automotive Industry (VDA), and leads the OTA activities inside GENIVI and Automotive Grade Linux.

Headquartered in Berlin, ATS operates a regional hub in Tokyo.

Note:

ATS participates in the UN Task Force on Cyber security and OTA issues and implements Uptane.