WHITE PAPER

DYNAMIC TYPE APPROVAL FOR AUTOMOTIVE SOFTWARE UPDATES

Vehicles the world over are required to be certified according to specific regulations in order to be fit for sale and fit to be on the roads. The procedures and regulations around vehicle approvals are known as homologation or Type Approval. Type Approval regimens differ between countries but all of them draw on a set of 100+ United Nation rules that are issued by the United Nations Economic Commission for Europe (UNECE).

One of the core tenets of these UN rules is that once type-approved components or systems may not be changed, neither in software nor in hardware, unless there is a new or updated Type Approval. This ensures that all vehicles on the road operate with approved safety and environmental performance. The component may not be changed by the OEM before the car is sold, and the component may not be changed by the customer after the car is purchased. This however, is creating a dilemma for car manufacturers and regulators alike -- How to ensure compliance of software updated throughout the vehicle lifecycle? New regulations are expected to be ratified by the end of 2019 that will enable a changed component to be brought into compliance with a new or amended Type Approval. The recommendations note that only new functionality constitutes a change to the type-approved component, and not a fix to an existing, approved component. Therefore, bug fixes and cyber security patches do not require an amended Type Approval.

With software expected to reach 40 percent of the car value by 2025 and some analysts predicting over 600m lines of code in future vehicles, it is no doubt that the challenge of certifying automotive software updates and managing it throughout the vehicle lifecycle is becoming of paramount importance. Couple this with the Type Approval costs of $40B to the global OEMs of which 40 percent is software driven ($16B) and it is clear that homologation is an expensive and growing problem that is in desperate need of efficiencies.

This document will clarify the role of the UNECE WP.29, and the specific position on Type Approval of over-the-air (OTA) updates. Finally, this document will outline the solution that Aurora Labs is bringing to the vehicle manufacturing market to facilitate efficient and dynamic Type Approval.

UNECE WP.29

The UNECE was set up in 1947. The organization's major aim is to promote pan-European economic integration: "Helping governments and stakeholders make the Sustainable Development Goals (SDG) a reality."

UNECE includes representatives from 56 member states from Europe, North America and Asia. Over 70 international professional organizations, including auto forums, vehicle manufacturers and other nongovernmental organizations also take part in UNECE activities.

Within the UNECE, transport is a major issue. Key areas of work in transport are:

- Vehicle Regulations
- Dangerous Goods
- Road Safety
- Climate Change and Sustainable Transport
- Intelligent Transport Systems (WP.29)
- Transport Health and Environment
- And more

Within WP.29 is the Working Party on Automated / Autonomous and Connected Vehicles, GRVA. GRVA's priorities are the definition of regulations for the safety and security of vehicle automation and connectivity:

- Framework
- Functional requirements
- New assessments and test methods
- Cyber security and software updates
- Data Storage System for Automated Driving (currently)
- ADAS
- Dynamics (Steering, Braking etc.)

Overall, the regulatory framework developed by the UNECE WP.29 allows the market introduction of innovative vehicle technologies, while continuously improving global vehicle safety. While the regulations that are set in place are not binding, they do serve as a reference to simplify and accelerate national (binding) legislative and regulatory work. However, since the majority of the UNECE participants are government officials, the UNECE discussions and decisions set the tone later when these officials return to their country and participate in legislative work.

WHOLE VEHICLE TYPE APPROVAL

Vehicle Type Approval is the confirmation that production samples of a design will meet specified performance standards. In Europe, India, China, Japan, and many other countries, compliance with the rules must be demonstrated to the national regulation authority. Regulators, AKA Type Approval Authority (TAA) test a sample batch of the new vehicle model for compliance with the regulations and issue a Certificate of Conformity (CoC) to the Type Approval requirements. In the U.S. and Canada, the car manufacturer self-certifies that the vehicle model complies with the regulations. This CoC is the basis of the Type Approval, and it allows the car to be sold and operated.

TYPE APPROVAL FOR SOFTWARE UPDATES

Since 2016, stakeholders around the world have been discussing how OTA updates should be considered in the realm of compliance. A final regulation that would make OTA updates acceptable in regions subscribing to the UNECE ruleset is possible by the end of 2019. At that point, countries and regions would have to adopt the new regulation into their laws - expected within 2020.

It is widely expected that the final OTA UNECE regulation will continue the requirement that Type Approval relevant updates need an updated Type Approval. "Manufacturers should be required to submit relevant documents to the approval authority/technical services from the requirement analysis phase to the implementation phase," states the position paper circulated among OTA stakeholders.

Due to the differing nature of types of changes to software, ranging from fixes for existing software functionality, patches for cyber-breaches and new functionality added throughout the software lifecycle roadmap, the UNECE WP.29 differentiated the need for amended Type Approvals. Specifically, "The vehicle manufacturer shall contact the relevant Type Approval Authority to seek an extension or new certification for the affected systems, for all updates, except for: If the update does not impact the compliance of any type approved systems, for example to fix software bugs, the vehicle manufacturer may conduct the update without need to contact the Type Approval Authority but shall ensure the update process employed is safe and secure."

In order for the need for Type Approval and the need for ongoing software updates to work in tandem without crippling progress in the automotive industry, a system is required that provides evidence that:

- The software update is only fixing bugs or applying a security patch, and not introducing new functionality – nullifying the need to apply for an updated Type Approval
- The new software functionality that has been added has only affected a limited and defined sub-section of the installed software in the vehicle – limiting the tests that are required to be run in order to receive the amended Type Approval

Based on a position paper circulated among OTA stakeholders, obtaining Type Approval for required software updates will be a lengthy and expensive process. Manufacturers are required to inform the approval authorities that a new version of software is available for an approved component. Depending on the nature of the software update, manufacturers are required to declare if the new software change results in any deviation from existing Type Approval conditions and notify the TAA of the same. Should new functionality be added, the manufacturer shall submit the updated component and all the relevant documentation to the TAA to undergo re-testing. While an amended Type Approval is not required for a fix to existing functionality, the manufacturer will have to produce evidence for the TAA that the new software is such an update.

While a Type Approval was previously obtained once for each car model, in the world of the software-defined car it is widely expected that amendments for Type Approval will be required on a regular basis for updates to vehicles already sold.

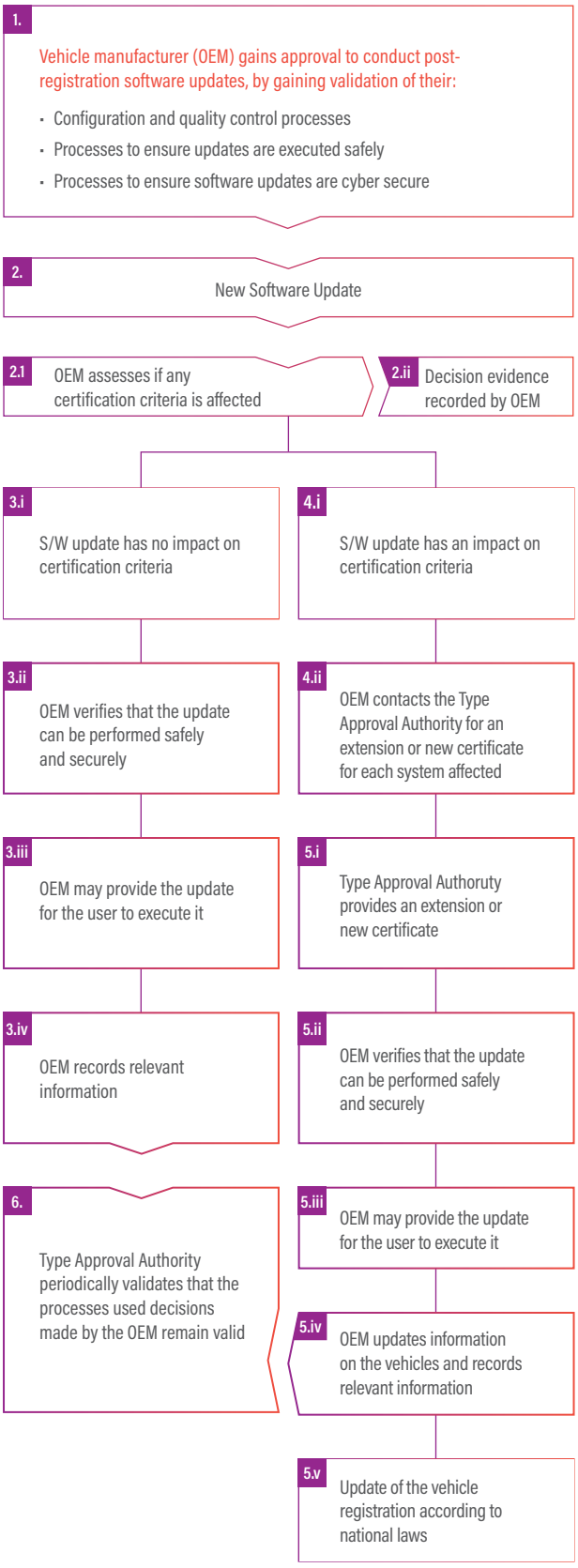

Figure 1: WP.29 - Flow diagram representing the process to certify and update vehicle software

AURORA LABS' AUTO VALIDATE

IN-VEHICLE EVIDENCE OF CHANGES TO THE SOFTWARE FUNCTIONALITY

Aurora Labs' Line-Of-Code Behavior™ machine learning technology analyses new software as it is created and generates a map of the software functionality relationships and behaviour. This dynamic map enables transparency into the ECU functionality in real-time that was previously lacking for the vehicle manufacturers. The Software Functionality Relationship Map includes the relationships between the software functions in a specific ECU and the relationships between software functions on different ECUs enabling a system-wide awareness of changes to the software configuration and behavior. This map, the functionality blocks within it and the dynamic behaviour of the software functions are then represented by unique digital thumbprints. Unlike current solutions used by the car manufacturers that simply calculate a HASH value for the entire software image as part of the certification process, Aurora Labs' Auto Validate generates a digital thumbprint of the software functions and their behavior providing evidence of changes to the functionality of the software in the new version, both for new software updates and for changes that may occur once the car has been certified and sold. For example, to fix a bug in the software, new code will be added to the software image. A simple HASH of the software image will identify this as a change in the software requiring an amended Type Approval. However Aurora Labs' Auto Validate analyses the functionality behavior of the new software at a line-of-code resolution giving the car manufacturer insights into the actual outcome of the change in software on the type-approved functionality. If the new software is deemed to have no effect on the behaviour of the software functions, Auto Validate supplies the evidence required for the vehicle manufacturer's documentation department to submit to the Type Approval Authority for a Type Approval waiver.

Further, using this technology, should a change to the functionality behaviour of a specific ECU be identified, interdependencies of the updated ECU software with other systems may also be identified. This method determines whether a particular software update affects other systems or software (e.g., a braking ECU may potentially affect a airbag ECU, etc.). This may be used by the OEM to narrow down the specific system software functions that have been affected by the new functionality in the software update, and hence determine which system functionality needs to be tested by the Type Approval Authority for the updated certification. More importantly, Aurora Labs' Auto Validate provides evidence and transparency of the software functionality behavior that have not been affected by the new and updated software and therefore do not require retesting for the updated Type Approval. This technique enables Dynamic Type Approval for homologation throughout the lifetime of the vehicle, requiring far less time and resources.

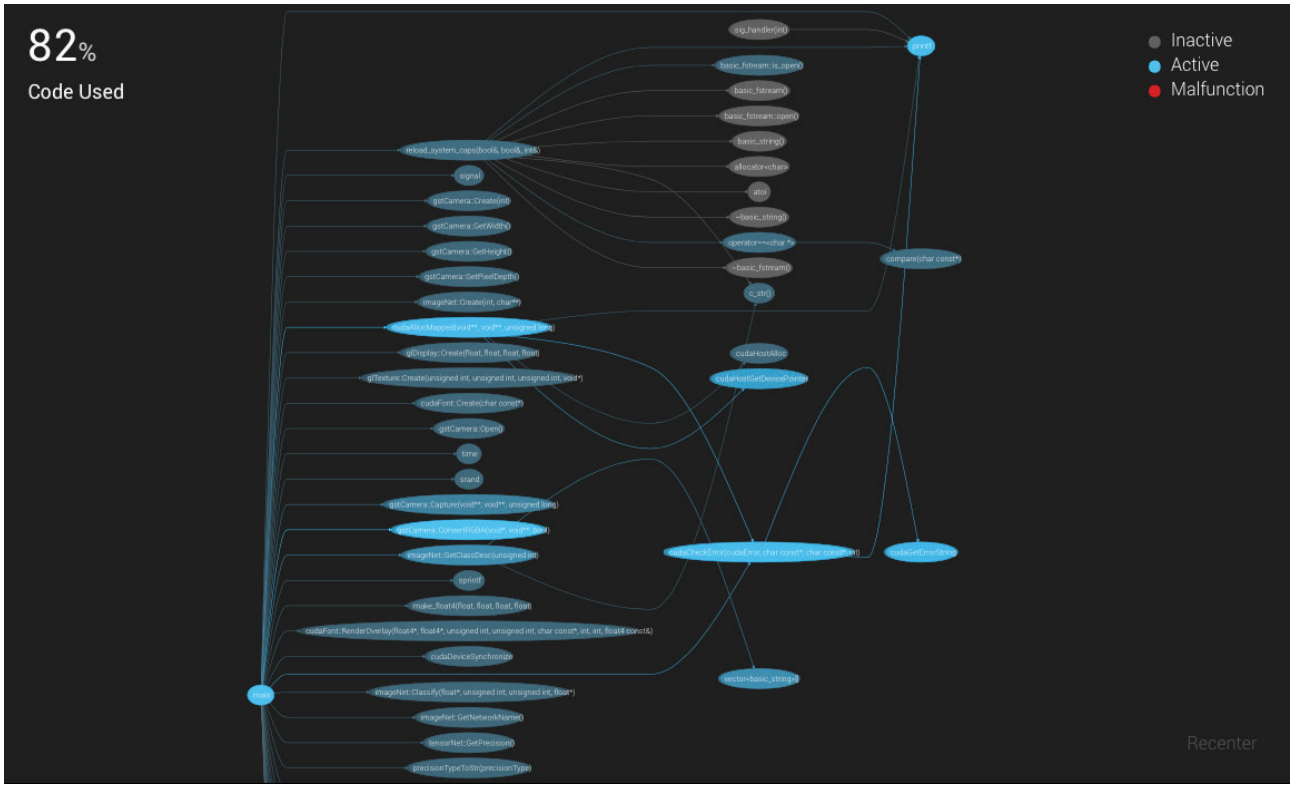

Figure 2: Software Functionality Relationship Map

COMPLIANCE WITH THE TYPE APPROVAL - LIABILITY

Auto manufacturers that want to bring a new car to market apply for Type Approval for the new car model and are required to prove that the vehicle complies with the relevant regulations.

However, in order to maintain compliance with the homologation regulations, the auto manufacturer is required to prove that no changes have been made to the vehicle functionality post certification, without the necessary authorisation. Auto Validate's ability to create a digital thumbprint of the actual behaviour and relationships of the software functions that receive the required Type Approval, coupled with the ability to create a digital thumbprint of the actual software running in the vehicle at any stage of its lifecycle, gives the TAA the ability to compare the digital thumbprints and thereby confirm whether the software functionality running in the vehicle is identical to the software that received the Type Approval.

For example, unlike existing solutions that compare the code in the software image, Auto Validate can identify a change to the response time between software call functions or even a call between functions that were not previously connected. The software image is the same however the behavior and activities have changed and may now not meet the certification. If the digital thumbprint is not identical, it may be confirmed that the software functionality has been altered (e.g., through an uncertified software update, a cyber security attack, or a malfunction in the code) and is no longer compliant with the Type Approval previously received. In other words, Auto Validate gives transparency into what is actually running on the ECU and how, and not simply what is flashed to the ECU.

WARRANTY DISPUTE RESOLUTION

This same functionality can also serve the auto manufacturer when resolving warranty disputes. By comparing the digital thumbprint of the software functionality behaviour of the car that is being investigated with the original digital thumbprint of the vehicle when it left the production floor, the auto manufacturer will be able to determine if the vehicle has been altered and tampered with in such a way that may void the warranty. Such deterministic evidence will be essential in resolving warranty disputes.

HARDWARE CONFIGURATION VALIDATION

By comparing the digital thumbprint of the vehicle software functionality behaviour with the digital thumbprint of the software that was approved at production and certified by the TAA, the vehicle can self-identify if a new ECU has been added to the vehicle. This will alert the OEM that unauthorized hardware has been installed in the vehicle or an authorized ECU that causes changes to the vehicle functionality, voiding the warranty and even stopping the vehicle from starting so as not to endanger the passengers.

SECURITY - TAMPER-PROOF

A common cyber attack known as a man-in-the-middle attack is performed by intercepting the software while it is on the network and changing it before it reaches the vehicle. Auto Validate's ability to calculate the digital thumbprint of the software functionality and relationships before it is deployed (at rest, on the server) and compare it with the digital thumbprint of the software that is deployed on the vehicle, a moment before it is installed, ensures that the software has not been tampered with on-route.

DYNAMIC TYPE APPROVAL

As software development is decoupled from hardware development and software roadmaps become the standard method for evolving functionality in the vehicle, the frequency of software updates will increase. According to the UNECE WP.29 recommendations: "The vehicle manufacturer shall contact the relevant Type Approval Authority to seek an extension or new certification for the affected systems, for all updates, except for: If the update does not impact the compliance of any type approved systems, for example to fix software bugs, the vehicle manufacturer may conduct the update without need to contact the type approval authority."

Aurora Labs, using the approach defined above, can provide the evidence required to distinguish between software updates that add new functionality and those that simply fix malfunctions in already-certified functionality.

Alternative approaches may require OEMs to resubmit the vehicle for WVTA (Whole Vehicle Type Approval) with every change made to the functionality of the vehicle software. Aurora Labs' approach however, enables Dynamic Type Approval by analysing the behaviour of the software functions and supplying evidence of the software functions that have been added or affected by the software update or ECU replacement during maintenance, greatly streamlining the Type Approval process for frequent software updates as are the norm in a software lifecycle.

ABOUT AURORA LABS

Aurora Labs is pioneering Self-Healing Software for connected cars to enable automotive manufacturers to proactively support to future vehicle software architectures, processes, and services. Aurora Labs' Line-Of-Code Behavior™ technology is the foundation of its In-Vehicle Software Management solution. Using machine learning algorithms to uniquely address all four stages - detect, fix, update and validate - of a software management solution, Aurora Labs future-proofs the next generation of software-driven automotive features. From detecting line-of-code faults to predict downtime events, fixing errors on-the-go to provide a safety-net for new software rollouts, enabling reliable and cost-effective rollouts of new automotive features to all ECUs in the vehicle without any downtime for the user and validating changes to the software to facilitate homologation, Aurora Labs is paving the way for the age of the self-healing car.

For more information please visit auroralabs.com

AURORALABS
SELF-HEALING SOFTWARE