Why are OTA Updates Needed for Intelligent Transport Systems?

Author:
François-Frédéric Ozog
Director of Edge & Fog computing group
Linaro
francois.ozog@linaro.org

Over-The-Air (OTA) updates are routinely used in IT, telecom and media industries. Updating a smartphone looks like a natural and desired feature for the end-user, but it is a very complex task due to the diverse nature of the updates (SIM card, phone software and isolated trusted software for micro payments to name a few) and the demographics of smartphones. The motivation behind these updates ranges from security enhancements or bug corrections to behavior changes that go beyond "cosmetics" including:

- Wireless speaker power increased from 1200W to 2000W[1]
- Augmented reality added navigation application

Until recently, Intelligent Transport Systems (ITS) players have not seen an imperative need for OTA. Reasons range from the lack of connectivity to high quality small software and the risks of compromising safety. Updates in ITS have gradually evolved, and some car makers allow full updates of many systems including Advanced Driver Assistance Systems (ADAS).

OTA in ITS is evolving from cost savings to business opportunities including:

- Feature enhancements
    - A car can autonomously pick up a user where they are[2]
    - 5%[3] increase in peak power (0-60mph in 2.9s instead of 3.2s—23% more efficient)
- Regulatory changes
    - As EU regulations have dramatically changed in Robotics,[4] the same will happen in ITS as the regulator is exposed to new situations
- Future business models
    - Engine power adjusted as per flexible subscription.

Furthermore, OTA has changed from "unknown" to "business critical" at the CxO level.[5]

OTA CHALLENGES FOR ITS

An ITS OTA solution is nothing without authoring, campaign design and deployment components. While it is clear that the operational aspects will be complex, the most challenging aspects appear at the device level. Solutions will involve hardware evolutions and will impact all components of the OTA value chain. At the device level, the OTA challenges arise depending on whether

[1] https://help.devialet.com/hc/en-us/articles/360009457019-Migration-DOS-2-and-Phantom-Premier

[2] https://www.tesla.com/blog/introducing-software-version-10-0

[3] https://www.tesla.com/blog/35000-tesla-model-3-available-now

[4] https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf

[5] Dr. Markus Heyn, a member of the Bosch board of management: https://www.bosch-mobility-solutions.com/media/global/highlights/connected-mobility/updates-over-the-air/internet-connectivity_press-information.pdf

a device is robust, trusted, transparent and traceable.

Robust

One is used to reading "don't turn off your computer while the update is being performed." This is not acceptable in an ITS context, so Electronic Control Units (ECU) have been offering robust and resilient updates through proprietary mechanisms. But this proprietary (siloed) approach is reaching its limits as software layers become more interdependent (i.e., an AI driven ADAS that needs FPGA and software changes in lock step). As a result of these dependencies, intra-ECU transactional updates need to be developed. In the future, there will be inter-ECU dependencies calling for system-wide transactional updates. This requires both standardization of new interfaces and open source reference implementations.

Trusted

Trust has always been a driving force for OTA solutions. To ensure trust, many signatures are used on software or data. Today, the multiplication of those signatures and layers of authority lack industrial scale processes to fully automate the chain of trust. This accumulation of hand-crafted integrations introduces weaknesses by construction. The security of hand-crafted integrations is analogous with a glass case wrapped in chains to protect a diamond—the glass is the weakest element.

There are scattered efforts in standard bodies to address this issue, and the processor ecosystem is currently making efforts to standardize code and update signing methods. But there is also a need to maintain a holistic view to ensure continuity of trust throughout the lifecycle of the transport systems themselves involving software companies, tier-1s, tiers2s and OEMs.

Transparent

Application software allows for fine grained live updates when leveraging frameworks such as OSGi. [6] Unfortunately, operating systems and hardware may not allow for fine grained or less live updates. In one example, the lack of dynamic, fine grain updates in an ITS led to a driver stuck on the roadside because he thought he could update his car while in a traffic jam. [7] OTA transactions need update schemes to be perfectly orchestrated for a seamless deployment of interdependent components, and there is currently no solution that can fully orchestrate such a comprehensive OTA.

Traceable

Cars are equipped with recorders for future forensics activities. While necessary, this is not sufficient as some intra-ECU activities need to be logged in a non-repudiable way. For instance, an insurance company may want to know when an Artificial Intelligence (AI) model has been received by the car and what happened in the ECU that controls the

[6] See dynamic updates in https://www.osgi.org/developer/benefits-of-using-osgi/

[7] https://www.theverge.com/2019/1/31/18205774/nio-ota-update-traffic-china-es8

various AI accelerators. The intra-ECU non-repudiable self-logging has yet to be fully standardized.

THE ROLE OF THE INDUSTRIAL INTERNET CONSORTIUM

The challenges presented above have one thing in common: collectively solving issues in using a holistic approach. A single vendor, single standard or single open source project cannot address them. The Industrial Internet Consortium (IIC) is in a unique position in that it can catalyze efforts in both standardization and open source efforts driven by car manufacturers and regulators. Several IIC groups are collaboratively contributing on the OTA topic in the context of the ITS Focus Program:

- The OTA Special Interest Group (OTA-SIG) focuses on automotive OTA issues with a goal to find applicable technologies and best practices in a broader industrial context
- The Security Working group, along with the Automotive Task Group, studies the relationships between security and safety
- Groups within the IIC are currently collaborating on the authoring and publication of an IoT distributed computing framework technical report that describes technical aspects of an overall detailed architecture and where OTA fits in

Lastly, IIC test beds are a perfect vehicle for assessing the end-to-end value of standards and solutions through their formal execution and reporting methodology.

➢ Return to IIC Journal of Innovation landing page for more articles and past editions