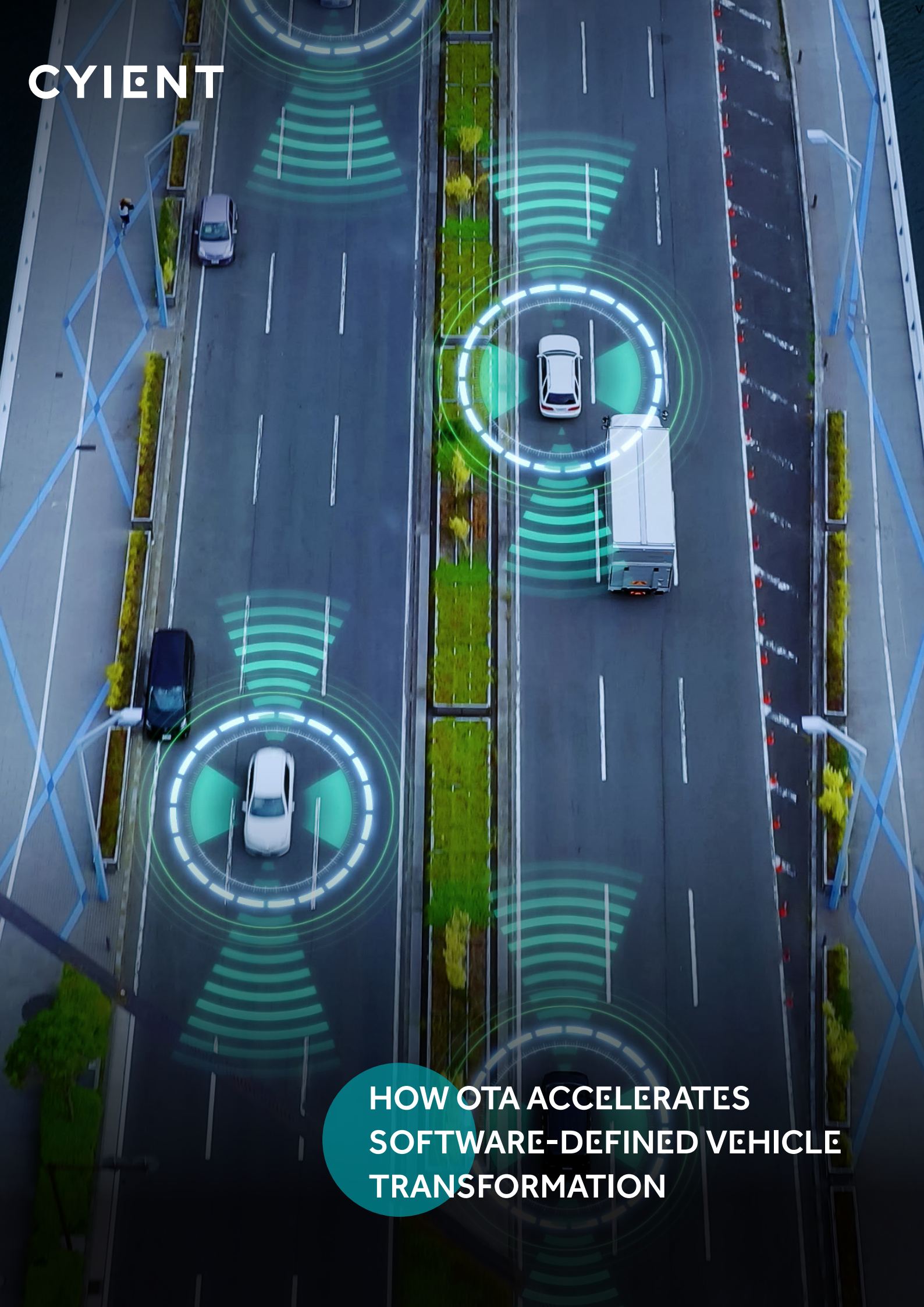
CYIENT



HOW OTA ACCELERATES SOFTWARE-DEFINED VEHICLE TRANSFORMATION

CONTENTS

Abstract

Digital technologies have significantly disrupted the transportation industry. ACES, the acronym coined by the Center for Automotive Research, which stands for autonomous-connected-electric-shared, refers to four major technology-driven mobility trends that are enabling alternative mobility and new business and revenue models for enterprises.

Technology disruptions and changing user expectations have long driven transformation in the automotive industry. The safety and comfort features of a vehicle have now gone beyond just automotive engineering. Today's automotive vehicle comprises several high-performance computing systems, which enable the implementation of complex software to resolve complex mobility problems to provide intelligent solutions that evolve from time to time. As it evolves, the quantum and value of the software exceed the value of mechanical hardware subsystems in a vehicle. This shifts the automotive vehicle from hardware-centric to software-centric, or a software-defined vehicle (SDV). An SDV enhances customer experience and creates an opportunity for automakers to maximize the value of a vehicle throughout its life cycle.

Why OTA is imperative to accelerate SDV transformation

A software-defined vehicle has the ability to add value throughout the life cycle of the vehicle. To make this happen, it is imperative that bi-directional data flow infrastructure is in place for both feature upgrades and data fetched from the vehicle to mine insights. Such infrastructure must support secure data transactions and be scalable and dependable in the competitive connected vehicle space.

Historically, automakers have been addressing firmware or software upgrade requirements through channels such as dealer networks, service centers, or field service engineers. With the growing need for an increase in the frequency of upgrades, automakers are challenged with

- timely upgrade;
- increasing cost of upgrade; and
- training channels in various upload/download systems.

Over-the-air (OTA) systems provide bi-directional operations between a cloud and a vehicle enabling both OTA updates and data upload. An OTA update enables downloading of content over a mobile or cellular network and installing it into a vehicle. Starting with firmware and software, OTA updates can support different content, including command control, configuration, map, service, rule, and AI model. Data upload transfers content from a vehicle back to the cloud. Data upload content can contain data such as the processing log, vehicle data, map, and environment data.

The OTA updates market for automotive was around $2.83 billion in 2021 and is estimated to grow by a CAGR of 16.7% to $4.5 billion in 2024. This growth is attributed to increasing demand for connected car devices compliant with government regulations for the safety and security of vehicles.

Benefits of OTA

- **Regular software updates:** Today, there are more software recalls than hardware-related recalls. If all software recalls were to require dealership involvement, it would result in a huge waste of time (for owners and OEMs) and money. Some software recalls relate to vehicle safety, and any delay in updates might lead to unacceptable results. In a frequent software update scenario, the dealer could easily become the bottleneck.

- **Easy access to new features:** In the new gen automotives, software updates don't just fix an existing function or feature but also add enhancements. When subscribing to a service, the associated features can be activated in the vehicle or updated to the vehicle. OTA can be used to activate or update a feature in a specific condition, such as a disaster.

- **Obtain vehicle data in real-time:** Through OTA data upload, the cloud system can acquire vehicle data in real time. Real-time vehicle data enables the cloud system to track the status and analyze the vehicle's streaming data. It can conduct a broader, collective analysis of the data collated from connected vehicles.

- **Predictive maintenance:** Through OTA data upload, vehicle data can be transferred to the cloud. An AI algorithm can process vehicle data and detect potential issues. An action script can be sent to a vehicle if certain vehicle data needs to be processed locally or transferred back to the cloud for further analysis. OTA can support continued diagnosis for the maintenance of vehicles.

- **Support after-market solutions:** With OTA, OEM and third-party solution providers can deliver new solutions to a vehicle. Examples are fleet management, shared mobility, and usage-based insurance. These solutions and services increase the value of a vehicle.

- **Must-have for autonomous driving:** While autonomous driving requires a high degree of safety, it also requires the ability to update the car's software quickly and easily. OTA updates allow the car's software to be updated without the need to physically visit a garage or dealership. This is important for autonomous cars, as they need to be able to receive updates on a regular basis to keep up with the latest in the law, technology, and driving conditions.

How does OTA work?

OTA consists of bi-directional operations:

- OTA update: Pushing content from the cloud to vehicles.
- Data upload: Transferring data from the vehicle to the cloud.

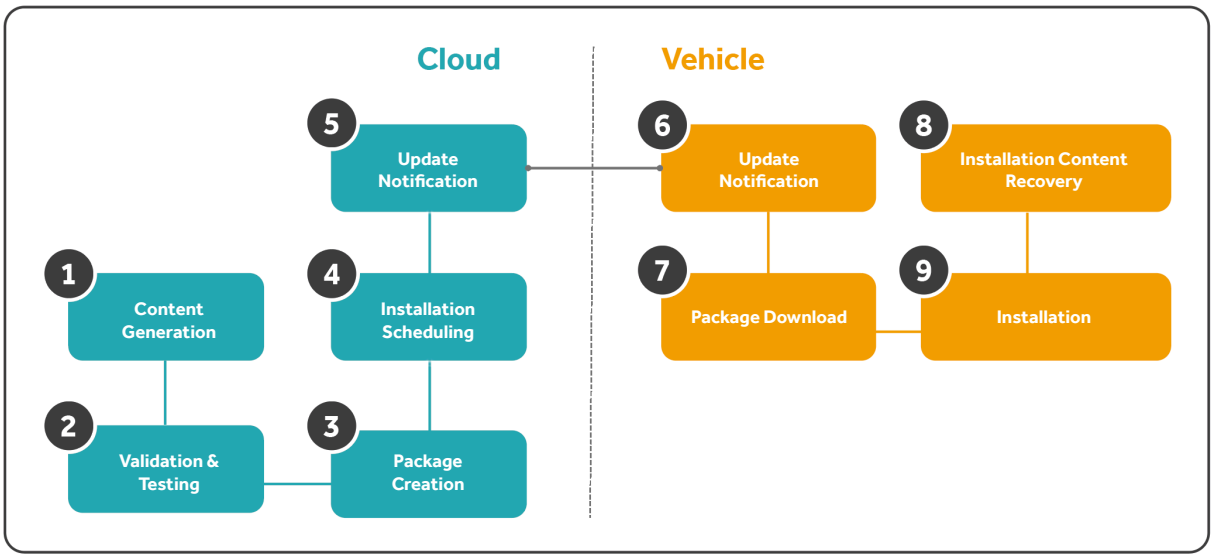


Figure 1. OTA update process flow

Figure 1 shows an OTA update process flow with the following steps:

1. **Content generation:** The update content can be data, firmware, software, configuration, rules, AI model, or action scripts. It can be loaded manually or generated automatically by other applications.
2. **Validation and testing:** As OTA updates are directly related to safety, the update content must be validated and tested before updating vehicles.
3. **Package creation:** Creating an appropriate package for the update content. Sometimes, a package might include multiple update content. Compression is required for large content, particularly a software package, to reduce data volume for transformation.
4. **Installation scheduling:** A content update can involve millions of vehicles. To optimize the utilization of resources (cloud resources and agents for resolving update issues) for a content update, the update needs to be scheduled. A trial installation with limited vehicles might be required before a mass vehicle update.
5. **Update notification (cloud):** The cloud system needs to send an update notification to a vehicle as required.
6. **Update notification (vehicle):** The vehicle checks the availability of content updates.
7. **Package download:** The vehicle downloads the update package when it is safe (parked, with enough battery, and convenient for the driver).
8. **Installation content recovery:** If the update content has been compressed or encoded, the gateway or edge device needs to recover the content.
9. **Installation:** The last step is to install the update content. After installation, local testing is needed. If the testing fails, rollback to the previous version of the content is necessary.

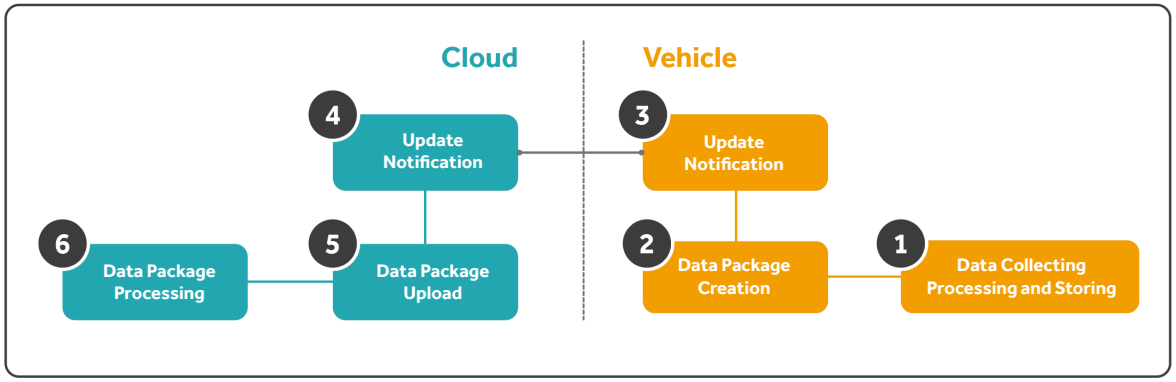


Figure 2. OTA data upload process flow.

Figure 2 presents an OTA data upload process flow with the following steps:

1. **Data collection, processing, and storing:** Collect data from the vehicle, process the data, and store processed data in the vehicle.
2. **Data package creation:** Create a data package for upload.
3. **Upload notification (vehicle):** Send "data package ready" notification.
4. **Upload notification (cloud):** Receive "data package ready" notification.
5. **Data package upload:** Upload the data package, which can be pushed to the cloud from the vehicle.
6. **Data package processing:** Process the streaming data from the data package.

Key Challenges

Remote issue resolution: The cloud side needs to handle OTA-related issues remotely. If an update installation fails, the rollback process and content need to be prepared by the cloud.

Unstable connectivity: Connectivity cannot be guaranteed for data upload. The vehicle must be able to resume the process if the connectivity is broken.

Safety, security, and trust: The safety of a vehicle is critical—and OTA can be a potential security threat. An OTA update must guarantee safety first. Therefore, it is important to ensure that the OTA is secure. The data loaded from the vehicle can belong to different owners. The use of this data needs to be GDPR-compliant to safeguard privacy.

Scalability: An OTA update could involve millions of vehicles. The OTA platform must support the scalability to reach such a vast number.

Large data package volume: The data package to be uploaded from a vehicle can be huge. It needs to upload the data based on urgency and usage.

Is secure OTA a cakewalk for connected vehicles?

Cybersecurity is paramount in OTA updates. Security is addressed at each layer of the system architecture right from the device to the cloud OTA server with the following measures:

- Secure boot, secure firmware, secure OS, secure configuration, secure containers, secure apps/APIs.
- Hardware crypto/hash, secure firmware installation, and secure boot secure firmware update at the device or gateway hardware level.
- Encrypted firmware images to the gateway and all the way to downstream devices.
- Firmware sign and hash verification via certificate signatures.
- TLS encryption with three-level Certificates Authority (Root CA, Intermediate CA, and Client/Server CA) using SHA256/SHA384/SHA512/RSA cryptography algorithm.
- Role-based access control (RBAC) and salted and encrypted login credentials in OTA server.

Potential use cases

OTA for firmware

ECUs and gateway software and hardware framework provide the opportunity to upgrade with additional functions/ features and improvise features safely or add comfort features on a need basis from time to time. This requires firmware upgrades for a large population of devices. A secure OTA system enables the orchestration of updates to a large population. The OTA system also helps in fixing bugs remotely.

The cycle time to complete such a massive update can be effectively handled through either compression of the binary file to reduce the size or differential update instead of a completely new binary file. This can save significant space and bandwidth while downloading the new firmware.

OTA for software

Traditionally, software updates for navigation or infotainment systems in a vehicle require the vehicle to be taken to the dealer or authorized service. Software OTA enables the secure downloading and updating of software in a connected vehicle at a user's convenience, eliminating the need to visit the service center.

OTA for battery monitoring;
The battery system in a vehicle should be fully monitored and controlled to avoid any potential hazard. It is important to acquire real-time usage status, power consumption, current, voltage, temperature, and so on. OTA enables access to such information for data analytics to get insights into battery health. It can provide an early warning to the user in case of potential abnormality or possible failure.

OTA for intrusion detection and prevention system (IDPS)

With the variety of connectivity options (4G/5G, W-Fi, Bluetooth) in a vehicle, it is imperative to have an in-vehicle cybersecurity system in place for secure transaction of functions and safety-critical data. IDPS is a leading approach to in-vehicle security, which enhances its ability to detect new anomalies through federated learning at the cloud level from peer vehicles in the same virtual group. The software/firmware element of IDPS needs to be updated with enhanced learning from time to time, and OTA makes it possible to do upgrades for the large population of vehicles in the virtual group.

OTA for shared mobility

A secure end-to-end OTA platform promises faster software development cycles, reduced recalls, and warranty costs, and enables newer business models and revenue streams through personalized, value-add services.

OTA for usage-based insurance

The advent of connected features of software-defined vehicles has led to the development of usage-based insurance (UBI). A driver with a high safety score can avail of insurance at a low premium. The score is arrived at based on the driver's behavior with respect to parameters such as acceleration, deceleration, speed, and driving patterns. The bi-directional data flow supported by OTA systems is key to remote access of such critical parameters for processing in the cloud for UBI estimation.

OTA reference implementation

The implementation of an end-to-end OTA system can be visualized into three major sub-systems—cloud administrator, cloud control unit, and gateway.

Cloud administrator:

The device administrator is responsible for

- Uploading the update firmware binary along with configuration, diagnostic, and metadata to the cloud control unit.
- Building the update firmware image and manifests.
- Managing bug fixes and firmware rollouts.
- Verifying update logs and diagnostic data.

Cloud Control Unit:

The cloud control unit is central to the overall system and does the following:

- Responsible for HTTP, COAP, and MQTT server and client services to connect with gateway devices.
- Execution of firmware or software updates, meta information, rollbacks, configuration management, and verifying integrity and failures.
- Gateway certificate and keys management.
- Data encryption and decryption over HTTP, MQTT, and COAP requests between admin, cloud, and gateway communication.
- Rights management: Handling the device, admin, and user rights.
- Reporting and analytics: Converting FOTA update logs to useful analytics for admin use and reporting the same.

Gateway:

- Gateway runs HTTP, COAP, and MQTT services to communicate with the cloud control unit.
- Gateway queries the cloud control unit to fetch new firmware image and manifests (configuration, meta, diagnostic sequences) via HTTP REST API, COAP, and MQTT methods.
- It identifies the new firmware based on meta information to update the firmware on ECU device groups and disallows improper firmware versions.
- OTA Firmware Flash download secures memory location.
- Gateway pushes ECU device firmware update image to device/device groups in wired/ wireless network with the following steps:
  1. Gateway downloads the DFU TCP/IP segment over wireless connectivity—4G/5G or Wi-Fi.
  2. Gateway sub splits and broadcasts to devices with firmware update messages for particular device or device groups.
  3. Device decrypts the gateway messages and stores the DFU image in secure flash.
  4. Gateway completes transfer of DFU image over wired/wireless to devices with “transfer complete” message.
  5. Device verifies DFU image authenticity in flash memory and performs the updates via SBSFU Engine.
  6. Device reboots and launches updated firmware image over bootloader.
- Firmware update log messages (diagnostic data) sent to the cloud control unit via Gateway.

Development of OTA and related services

OEMs such as Tesla, BMW, Mercedes-Benz, GM, and Volkswagen have developed in-house OTA platforms to provide updates for their vehicles. Vehicle manufacturers have also partnered with other companies to provide OTA platforms for their vehicles. Ford has partnered with Telenav for FordPass Connect, Toyota has partnered with software company Agero for Toyota Safety Connect, and Honda has partnered with software company Airbiquity for HondaLink to provide updates for Ford, Toyota, and Honda vehicles.

Off-highway OEMs are slower to adopt OTA despite the advantages it provides. Safety concerns are the major restraint for the adoption of OTA in off-highway vehicles. On the other hand, the benefits of OTA in off-highway vehicles are higher than in automotive vehicles, as off-highway vehicles do not have to follow stringent guidelines.

While OTA has been implemented as part of an automotive platform, other functions, such as security, predictive maintenance, and battery management, need the support of OTA.

Cyient has rich experience in developing OTA services based on an OTA platform.

Cyient can:

Develop OTA for an automotive platform to meet the specific requirements for business and technology strategy

Develop solutions based on OTA

Develop and validate OTA updates

Conclusion

Autonomous, connected, electric, and shared (ACES) mobility is the trend in the new generation of automobiles. With ACES, software-defined vehicle solutions transform automotive vehicles from hardware-based to software-centric devices, and OTA is essential for supporting software-defined vehicle solutions.

The OTA system resolves the issue of software recalls. Today, OTA enables OEMs to enhance the features and functionality of vehicles through software and content updates, adding to the value of a vehicle. OTA uploads vehicle data to the cloud in real time for cloud-based collaborative data analytics and machine learning. With the bi-directional operations of OTA, the vehicle mobility platform can be self-adaptive to the environment faced by vehicles.

OTA also enables third parties with solutions such as shared mobility and fleet management. However, it increases the risk of safety, security, and privacy. OTA programming must provide standard APIs that can meet the requirements for safeguarding safety, security, and privacy.

While OTA provides fundamental services for an OEM's mobility platform, its implementation must meet the specific requirements of OEM. Cyient, with its vast OTA experience, is well-positioned to be your solution partner for such implementation.

As a technology services provider, Cyient works closely with industry experts, equipment manufacturers, and aftermarket customers to align with automotive industry trends through our focus areas of megatrends "Intelligent and Meta Mobility," "Digital Healthcare," and "Industry 4.0 and Smart Operations."

About the Authors

Dr. Tao Lin
Chief Architect and Technology Evangelist

Tao Lin is a chief architect/tech evangelist in Cyient CTO office. Dr. Lin supports automotive, aerospace, rail, UAM, and high-tech areas. Dr. Lin has over 29-year experience as technology strategist, technical and business architect, research scientist, and engineering manager. Dr. Lin has worked in CSIRO, SGI, SAP, PARC Research Lab, and Aptiv, and 5 startups. Dr. Lin holds 18 US patents.

Ilango Ganesan
Senior Director - Technology

Ilango Ganesan leads solutions for Automotive & Off-highway industry clients. He has vast experience in the end-to-end development of products, systems, and solutions for the Automotive, Industrial and Utility sectors.

About Cyient

Cyient (Estd: 1991, NSE: CYIENT) is a leading global engineering and technology solutions company. We are a Design, Build, and Maintain partner for leading organizations worldwide. We leverage digital technologies, advanced analytics capabilities, and our domain knowledge and technical expertise, to solve complex business problems.

We partner with customers to operate as part of their extended team in ways that best suit their organization's culture and requirements. Our industry focus includes aerospace and defense, healthcare, telecommunications, rail transportation, semiconductor, geospatial, industrial, and energy. We are committed to designing tomorrow together with our stakeholders and being a culturally inclusive, socially responsible, and environmentally sustainable organization.

For more information, please visit
www.cyient.com

Contact Us

North America Headquarters
Cyient, Inc.
99 East River Drive
5th Floor
East Hartford, CT 06108
USA

T: +1 860 528 5430
F: +1 860 528 5873

Europe, Middle East, and Africa Headquarters
Cyient Europe Limited
Apex, Forbury Road,
Reading
RG1 1AX
UK
T: +44 118 3043720

Asia Pacific Headquarters
Cyient Limited
Level 1, 350 Collins Street
Melbourne, Victoria, 3000
Australia

T: +61 3 8605 4815
F: +61 3 8601 1180

Global Headquarters
Cyient Limited
Plot No. 11
Software Units Layout
Infocity, Madhapur
Hyderabad - 500081
India

T: +91 40 6764 1000
F: +91 40 2311 0352

Follow us on: