Connected Car Solutions Based on IoT

With the aim of achieving a prosperous society in which people and vehicles exist in harmony, the connected car is recognized for its potential as a platform for creating new value and businesses through the recording and analysis in a cloud system of information collected from vehicles. Achieving this will require both highly reliable communication systems that connect to the cloud and analytic techniques able to handle large amounts of data. Hitachi is developing data center services and onboard devices for vehicles that combine automotive technology with IoT know-how acquired through past involvement in the information and communications sector. This article describes key technologies for building connected cars.

Kohei Sakurai, Ph.D.
Mikio Kataoka
Hiroshi Kodaka
Atsushi Kato
Hidetoshi Teraoka
Noboru Kiyama, Ph.D.

1. Introduction

Connected cars with always-on links via the Internet to data centers and other infrastructure have attracted attention as a next generation of vehicles able to provide services that deliver greater safety and comfort. Because of their role as platforms for advanced driver assistance systems, including autonomous driving, connected cars need high levels of reliability and information processing capacity.

By combining know-how in automotive systems with information and communications technology acquired through involvement in a variety of product fields, Hitachi is developing a diverse range of center services and onboard devices to provide a platform for connected cars.

This article summarizes the trends and technical issues associated with connected systems, and describes key technologies for the wireless updating of software, security for protecting information, and in-vehicle edge computing.

2. Trends in Connected Systems

The main services for connected cars in the 2000s were based on data analysis, with the provision of information on traffic congestion being a typical example. When first introduced, the service worked by implementing a communication module that can be connected to a mobile communication network in commercial vehicles such as taxis. These were called telematics control units (TCUs). Improvements to service convenience in recent years have seen vehicle manufacturers installing TCUs in cars as a standard feature to provide connected car services to the general public.

With Internet connections having become commonplace in vehicles, infotainment services have

also spread, such as those that obtain information from social networking services (SNSs) and display it on the navigation system screen. Services have also emerged that provide a limited form of remote vehicle operation by issuing commands to the vehicle via a data center. Remote door unlocking is one example. It is likely that closer interoperation between data centers and vehicles, with various services using the results of analysis at a data center to provide feedback to vehicle control, will become commonplace (see left side of **Figure 1**). Security will be vital to implementing these feedback services, and Hitachi is working on the development of gateways for handling security in the vehicle.

It is anticipated that future links between vehicles and data centers will have a system architecture like that shown on the right of **Figure 1**. Hitachi is working on the development of the underlying technologies that will make these systems possible. The data center will use Hitachi's Lumada Internet of Things (IoT) platform.

The following sections provide details of technologies for over-the-air (OTA) software updating, security, and in-vehicle edge computing that will be essential for building the platforms that support connected car solutions.

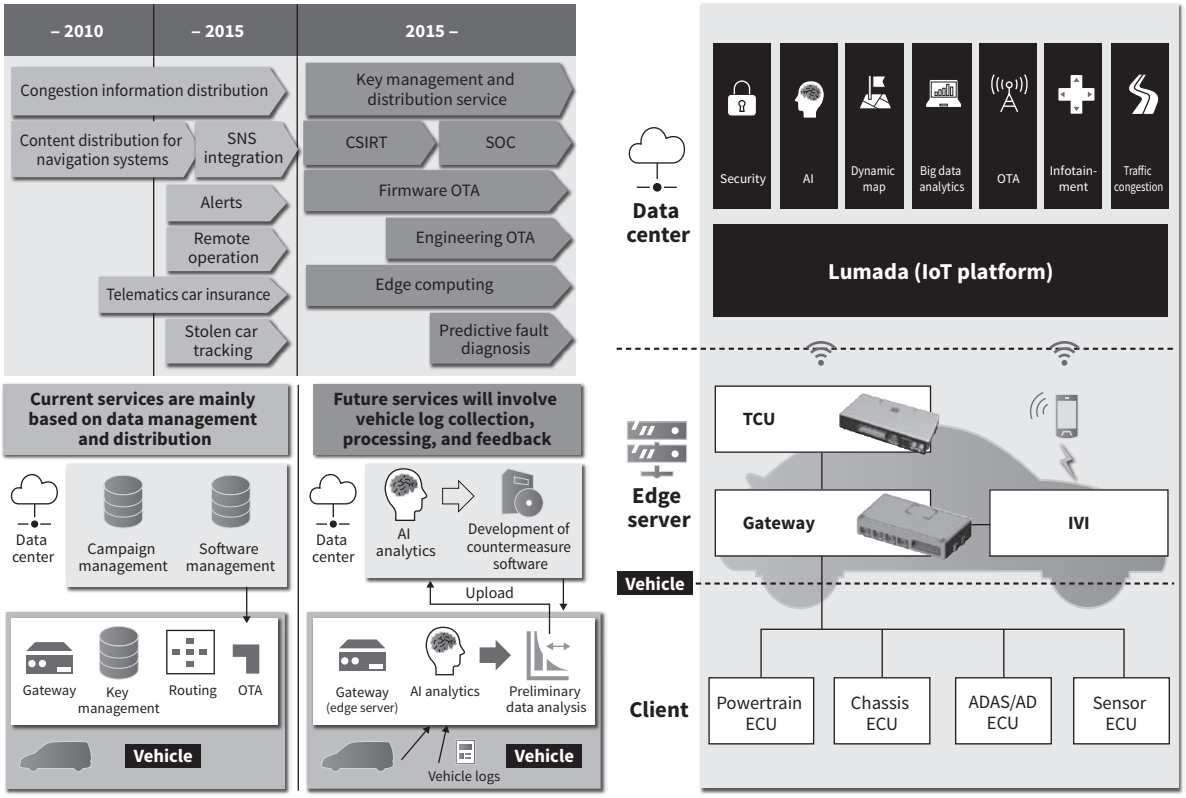
3. Controlling Software Updates by OTA

3. 1
Background and Challenges

Recent years have seen a shift from hardware to software as the primary means of vehicle control, with the software on automotive electronic control units (ECUs) playing an increasingly important role. While this central role for software in control opens up new opportunities for the automotive industry, including

Figure 1 — Roadmap and System Architecture for Connected Car Services

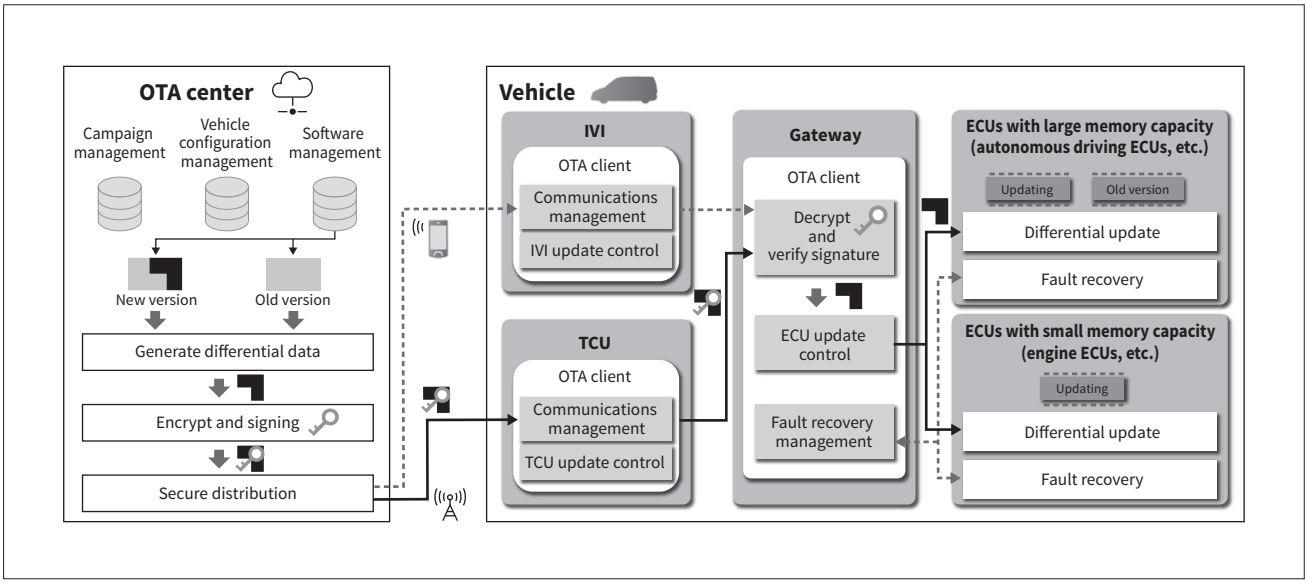
The diagram on the left expresses the shift from data analysis and simple information distribution services to services that provide the results of analysis as feedback, while that on the right shows how TCUs, gateways, and IVI provide edge server functions for edge computing.



SNS: social networking service CSIRT: computer security incident response team SOC: security operation center AI: artificial intelligence OTA: over the air
TCU: telematics control unit IoT: Internet of Things IVI: in-vehicle infotainment ECU: electronic control unit ADAS: advanced driver assistance system AD: autonomous driving

Figure 2 — Block Diagram of OTA System

Hitachi has developed a total system that extends from the data center system to the ECUs being updated, and identified the requirements for each function from a system perspective. For functional safety and security, control ECU updating is managed by a gateway. Standardized technologies are used for the interfaces between the data center and vehicle and between the onboard ECUs to enable a multi-supplier system to be configured.



the ability to provide after-sales upgrades, recalls due to software are also a major concern. The increasing number of connected cars also brings concerns about greater security risks such as the risk of remote attacks. One technology that has attracted attention as a way to deal with these changing circumstances is the use of wireless communications for controlling software updating by OTA.

The use of OTA updates for vehicles requires the following features. The first one is a high level of reliability to avoid vehicle problems such as software upgrades failing or impacting on safety. The second one is to shorten update times to avoid draining the battery while minimizing the period of time that vehicles are unavailable. The last one is to deal with diverse and complex systems made up of a large number of ECUs that behave differently.

3. 2
Hitachi's OTA Software Update Technique

Hitachi has developed the following techniques for utilizing OTA for automotive systems in a way that overcomes the above problems (see **Figure 2**) [(1), (2)].

• Differential updating for shortening update times on automotive systems with limited network bandwidth and memory resources

• Recovery from update problems in accordance with ECU specifications and cost factors, including safety requirements and memory resources

• End-to-end security from data center to vehicle, with multi-layered protection for distribution of updates

• Update control techniques that can cope with update procedures that differ between vehicle models and ECUs

• Support for multiple suppliers, with updates from different suppliers being packaged for distribution together with the use of standardized technologies for the interfaces between the data center and vehicle and between onboard ECUs

Hitachi has developed TCUs, gateways, ECUs, and data center systems that incorporate these techniques, with the intention of supplying a one-stop OTA solution made up of these components and systems.

3. 3
Future Developments

Software updating must be suitable not only for vehicles that are already in the marketplace; it also needs to work for components that are still in the development, manufacturing (production line), or distribution (ports or vehicle storage yards) processes of vehicle manufacturers, or in the manufacturing, distribution, or storage processes of parts suppliers.

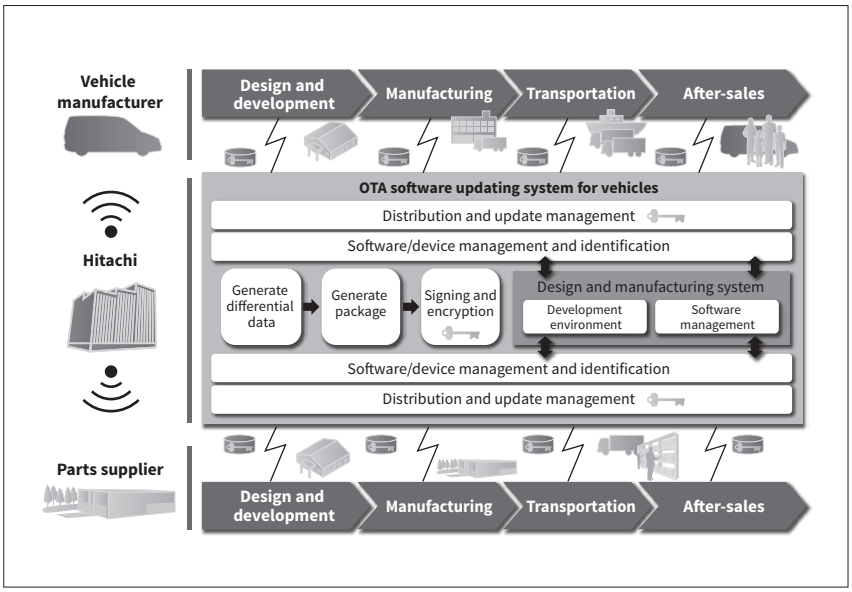


Figure 3 — OTA in Development and Manufacturing Processes

As for after-sales upgrades, the use of wireless communications to update software during development and manufacturing makes the work more efficient.

The aims for the future are to boost the efficiency of software updating and management across the entire lifecycle, facilitate recalls, and improve traceability by coordinating vehicle identification and software/device management by the software updating system with product lifecycle management (PLM) and manufacturing execution systems (MESs) (see **Figure 3**).

4. Security Technology

4. 1
Background and Issues

As vehicles become more connected, networks that previously did not extend beyond the vehicle itself are now being connected to the Internet and other external networks. This has led to concerns about attacks on vehicles from these external networks, raising the issue of how to reduce security risks such as unauthorized remote operation or interception of communications between a vehicle and data center.

Hitachi sees gateways as being a key component of the next generation of vehicles. In addition to acting as a router for communication between different network domains in a vehicle, these gateways are also equipped with functions for maintaining security within the vehicle by monitoring its internal communications, and the security of interoperation with the security operation center to improve quality and security through the lifecycle of the vehicle.

4. 2
Onboard Communications Security

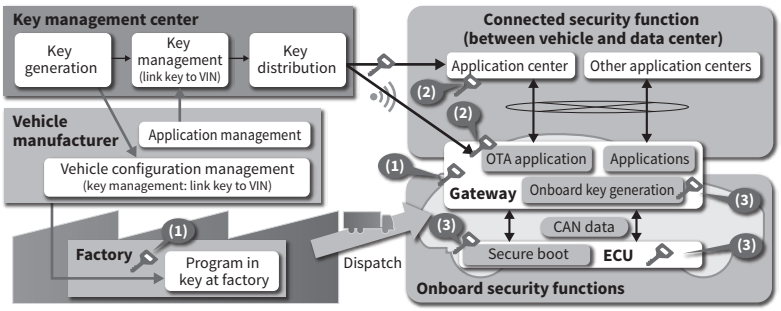
The gateway is implemented with the following security functions to protect against the internal and external threats to the vehicle identified by threat analysis. The gateway uses these security functions to prevent external attacks from gaining access to onboard networks.

- Filtering of unauthorized communications
- Secure boot to detect unauthorized attempts to overwrite software
- Device authentication to prevent connect of unauthorized devices
- Message authentication to verify that messages are valid
- Countermeasures against denial-of-service (DoS) attacks

4. 3
Security of Interoperation with Security Operation Center

Security requires countermeasures not just against anticipated attacks but also against forms of attack that are becoming increasingly sophisticated. Along with the security measures provided at the time of development, this also calls for the monitoring of vehicles in the field to provide a quick response to any issues that arise.

The following security solutions for interoperation with a security operation center maintain security through the lifecycle of the vehicle.



Key type	Description
(1) Base key	(1) The primary key for ensuring vehicle security (trust anchor) Generate at key management center and program into vehicle at factory
(2) Application key	(2) Key used for device authentication and to encrypt and decrypt data in data transfers between center and gateway Using the base key, this key is sent from the key management center to the service center or gateway (periodically updated)
(3) On-vehicle key	(3) Used on onboard network and ECUs for inter-ECU authentication, message authentication, and secure boot Generated from base key by gateway and distributed to onboard ECUs (periodically updated)

VIN: vehicle identification number CAN: controller area network

Figure 4 — Key Management Solution

Hitachi supplies a key management solution that handles everything from generation to use of the keys needed for authentication and encryption in connected services and between onboard ECUs, anticipating all aspects from vehicle manufacture to use.

(1) Key management solution

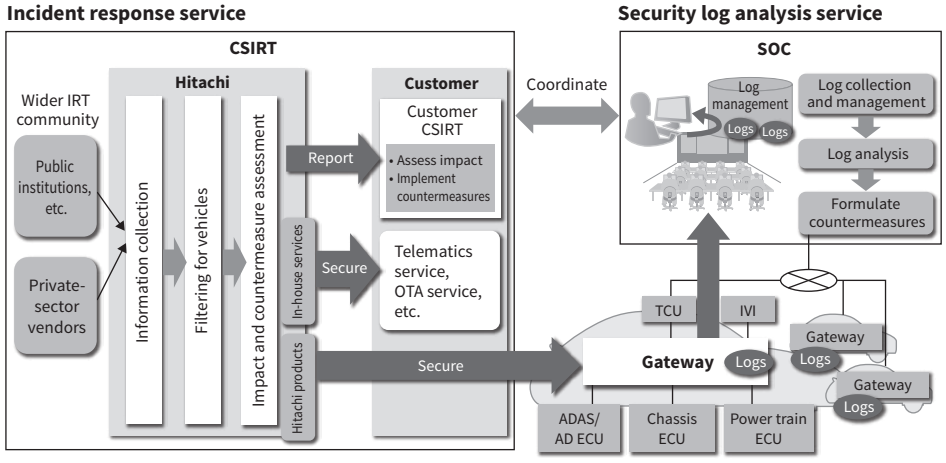
Security implementations require a way to manage the encryption keys used for the mutual verification of communications between the data center and vehicle and between vehicle ECUs, and also to protect the communication paths. Hitachi supplies a key management solution for the entire vehicle lifecycle from manufacturing to disposal (see **Figure 4**) [3].

(2) Security service solution

Hitachi utilizes technology developed for information technology (IT) systems to provide a security operation center with the ability to collect and analyze logs of attacks detected by the gateway, and to offer vehicle manufacturers timely countermeasures in the following forms (see **Figure 5**).

• Incident response service

This service collects information on vulnerabilities and incidents relating to products and services and provides it to vehicle manufactures so that they can implement practices for maintaining vehicle security through early identification and response to attacks.



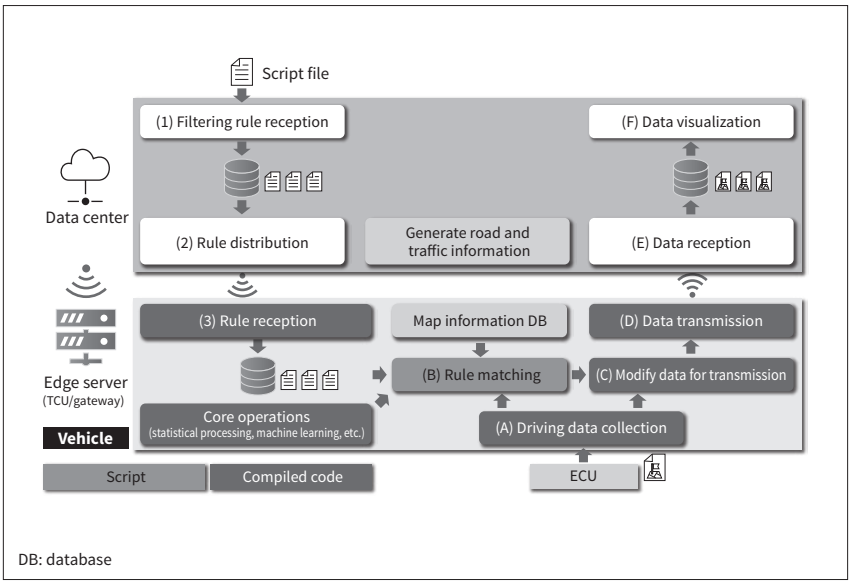
IRT: incident response team

Figure 5 — Security Service Solution

Prevents ever more sophisticated security attacks by taking precautions based on incident information collection and analysis, and through the use of log analysis for early identification and response to attacks.

Figure 6 — Edge Computing Platform Based on Script Distribution

The platform combines ease of program updating with a low processing load by using low-overhead compiled code for core statistical operations but using script to specify how those statistical operations are to be combined.



• Security log analysis service

To minimize the impact of incidents and achieve a quick recovery, this service assists vehicle manufacturers to analyze causes and implement countermeasures to security attacks by collecting and analyzing vehicle logs.

5. In-vehicle Edge Computing Technology

It is anticipated that the amount of data collected from each vehicle will grow considerably in the future due to functions such as the security log analysis service described above. As more cars become connected, this increasing volume of data communications will become an issue. Accordingly, Hitachi believes that future platforms for the connected car will require functions like the following for reducing data volumes.

• During normal driving, onboard devices only collect a limited amount of sensor and log data at low frequency for forwarding to the data center.

• When a problem occurs, or when so instructed by the data center, onboard devices collect a large amount of sensor and log data at high frequency for forwarding to the data center.

This is the same principle as used by edge computing on the IoT, minimizing the amount of data collected from the vehicle while still maintaining service quality.

Statistical processing functions that operate based on these data collection rules run on the gateway that collects sensor and log data from the various ECUs. However, because this gateway is an embedded system that also handles other functions, including security and routing, it suffers from a lack of central processing unit (CPU), memory, and other resources. For this reason, Hitachi has developed in-vehicle edge computing technology that can run on resource-limited hardware (see **Figure 6**).

This technology provides a way to modify rules on onboard devices and uses a mix of script and compiled code to reduce resource use by these devices. While script typically makes program changes easier because no compilation is required, it also requires more CPU and memory resources to execute. Compiled code, in contrast, uses fewer resources, but is more difficult to modify because of the need for compilation when making program changes. In response, Hitachi succeeded in achieving both ease of modification and low resource use by using the following two programming languages.

(1) Compiled code is used for operations such as machine learning and statistical processing that are resource-heavy but do not require frequent modification.

(2) Script is used for operations such as comparisons or function calls that are modified frequently but do not use many resources.

Changes to rules can be implemented immediately by sending a script file containing the new rules from the data center to the gateway and overwriting the old script file.

6. Conclusions

This article has described platform technologies that Hitachi is developing for connected cars.

By supplying solutions that combine TCUs, gateways, and other onboard devices; OTA software updating, security, and other data center services; and computing techniques for the pre-processing of large amounts of information on the vehicle, Hitachi intends to help provide society with smart mobility that brings prosperity as well as harmony between people and vehicles with greater safety and comfort.

References

1) H. Teraoka et al., "Incremental Update Method for In-vehicle ECUs," IPSJ Transactions on Consumer Devices & Systems (CDS), 7(2), pp. 41–50 (May 2017) in Japanese.
2) H. Teraoka et al., "Incremental Update Method for Resource-constrained In-vehicle ECUs," IEEE 5th Global Conference on Consumer Electronics (2016).
3) N. Morita et al., "Proposal for Security Analysis Support Tools for In-vehicle Systems," Symposium on Cryptography and Information Security (SCIS) (2014) in Japanese.

Authors

Kohei Sakurai, Ph.D.
Information & Communication Design Department, Safety & Information Systems Division, Hitachi Automotive Systems, Ltd. *Current work and research:* Mass production development of in-vehicle information and safety systems. *Society memberships*: Society of Automotive Engineers of Japan, Inc. (JSAE) and The Physical Society of Japan (JPS).

Mikio Kataoka
Information & Communication Design Department, Safety & Information Systems Division, Hitachi Automotive Systems, Ltd. *Current work and research:* Design and development of in-vehicle security technologies. *Society memberships*: JSAE and the Institute of Electronics, Information and Communication Engineers (IEICE).

Hiroshi Kodaka
Safety & Information System Communication Development Department, Safety & Information Systems Business Promotion Division, Clarion Co., Ltd. *Current work and research:* Product development of telematics control units.

Atsushi Kato
Mobility and Manufacturing Systems Division, Industrial Solutions Division, Industry & Distribution Business Unit, Hitachi, Ltd. *Current work and research:* Planning and development of connected car services.

Hidetoshi Teraoka
System Productivity Research Department, Center of Technology Innovation – Systems Engineering, Research & Development Group, Hitachi, Ltd. *Current work and research:* Research and development of in-vehicle systems. *Society memberships*: Information Processing Society of Japan (IPSJ).

Noboru Kiyama, Ph.D.
Customer Co-creation Project, Global Center for Social Innovation — Tokyo, Research & Development Group, Hitachi, Ltd. *Current work and research:* Research and development of connected car services. *Society memberships*: IPSJ.