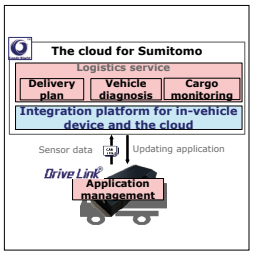

Fleet Management System for Connected Vehicles

Junji YANO*, Kentarou TAKAKI, Tomoyuki MURAYOSHI, Tsuyoshi HAGA, Shuhei TAKIMOTO, and Ryo TANAKA

Many motor vehicle manufacturers around the world are shifting from the vehicle sales business to the mobility service business. Participating in the connected business area, the Information Network R&D Center is developing a prototype solution for managing and analyzing in-vehicle devices, in-vehicle software, and in-vehicle sensor data together with the Systems & Electronics Division, CAS-EV Development Promotion Division, and AutoNetworks Technologies, Ltd. This paper introduces our efforts in commercializing fleet management systems for connected vehicle in the future.

Keywords: CASE, connected, fleet management, OTA

1. Introduction

In the next-generation connected vehicles, to realize connected services responding to the age of Connected, Autonomous, Shared, and Electric (CASE), it is expected that the vehicle's electrical/electronic (E/E) architectures will be centralized and centrally controlled,[1] and software, including applications, will be frequently added and updated from outside the vehicle through OTA.*1 However, due to the long life cycle of vehicles, in the transitional period until the full-fledged connected era, when all vehicles will be equipped with connected devices, it is anticipated that non-connected vehicles that are already on the market will be converted into connected vehicles. One of the means to do so is to retrofit non-connected vehicles with in-vehicle devices. We have already commercialized an in-vehicle device that is retrofitted to existing vehicles to make them connected (*Drive Link**2), and we are about to enter this business field in earnest.

In the meanwhile, the increased interface with the outside of the vehicle increases the risk of the vehicle being exposed to threats. It may easily be imagined that applications and service software will run on in-vehicle devices to respond to diverse mobility services that are advancing every day, and thus they are just as likely to become targets for malicious third parties as ordinary web servers and smartphone applications.[2] To provide safety and security, managing applications and software running in vehicles is considered to be one of the essential items to reduce risks.

To address this challenge, we have developed an in-vehicle application management technology for managing applications and software running in vehicles. We also developed an in-vehicle application life cycle management system, which is a system for the continuous operation and maintenance of applications and software running in vehicles using the in-vehicle application management technology.

By taking the lead in technological development, prototyping, and commercialization in this field, we plan to develop and launch an in-vehicle system to promote logistics digital transformation (DX)*3 by linking it with our logistics solutions[3] and our vehicle operation management system (*Eagle Sight**4)[4], which are our fields of expertise.

Chapter 2 provides a description of the in-vehicle application management technology, Chapter 3 explains the in-vehicle application life cycle management system, and Chapter 4 describes future actions as a conclusion.

2. In-Vehicle Application Management Technology

The in-vehicle application management technology is a technology for managing applications running in vehicles through integration between in-vehicle devices and the cloud. Specifically, it consists of functions of execution status monitoring, configuration information monitoring, update management, identity and access management and log management. Figure 1 shows a conceptual drawing of the application management technology applied to an in-vehicle device.

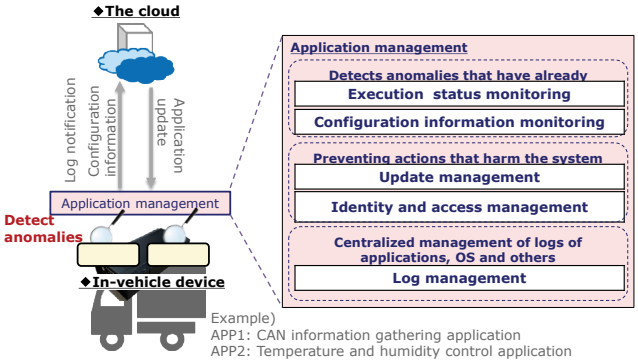

Fig. 1. In-vehicle application management technology

This technology allows for quick detection of abnormalities occurring in the vehicle and prevention of actions that could harm the system (robustness).

As a summary of this chapter, the processing of each function is described below.

2-1 Execution status monitoring function

To detect application abnormalities, monitor whether a state transition error or control flow error has occurred.

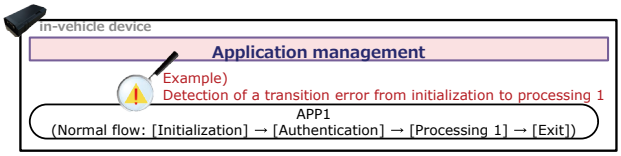

Fig. 2. Detecting that authentication has been bypassed

2-2 Configuration information monitoring function

To ensure stable operation of the vehicle, monitor the configuration information (version, etc.) in the vehicle and periodically notify it to the cloud.

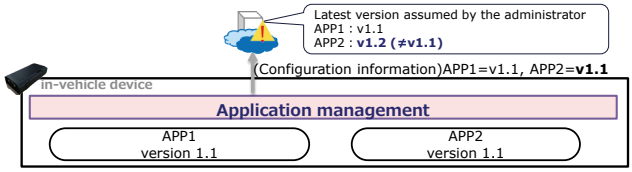

Fig. 3. Sending information on application versions

2-3 Update management function

To prevent unauthorized applications from entering the vehicle, verify whether each application is authorized or not by using digital signatures and other means.

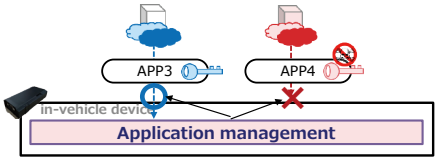

Fig. 4. Blocking untrusted signatures

2-4 Identity and access management function

To prevent unauthorized access, manage the protected assets by controlling access to them from applications.

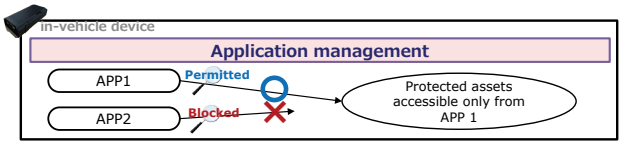

Fig. 5. Blocking access from unauthorized applications

2-5 Log management function

To quickly check system operation and analyze abnormalities when they occur, manage the log configurations and locations of applications and systems.

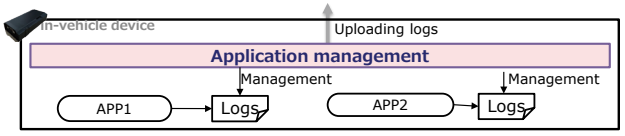

Fig. 6. Keeping track of locations of application logs

3. In-Vehicle Application Life Cycle Management System

The in-vehicle application life cycle management system is a system based on the in-vehicle application management technology described above, which is designed to ensure traceability and continuous operation and maintenance of applications and software installed in the vehicle.

The main functions that make up the system are the OTA function, the configuration management function, the data accumulation function and the analysis function, which can be called an integration platform for an in-vehicle device and the cloud for realizing the integration between the in-vehicle device and cloud. Figure 7 is a drawing showing a configuration of the in-vehicle application management system.

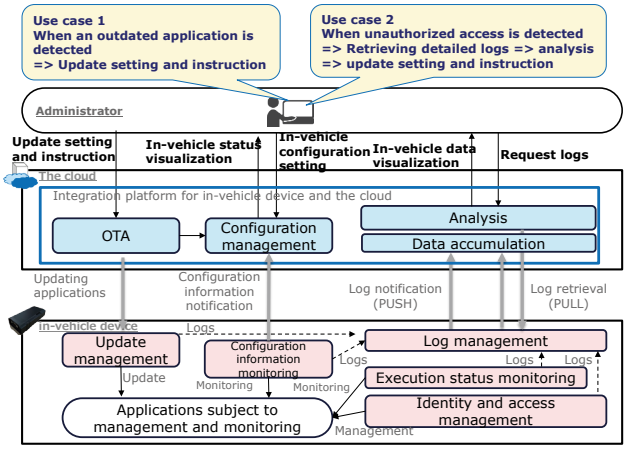

Fig. 7. In-vehicle application life cycle management

Each function is described as follows.

3-1 OTA function

It provides a mechanism for remotely updating in-vehicle software. Specifically, it manages the software for updates and the update schedule, and when there is an update, it notifies the vehicle of it.

3-2 Configuration management function

This is a function of managing the in-vehicle software configuration (e.g. software name and version) and the

hardware configuration (e.g. devices connected to the hardware interface) in order to understand the operation status of the in-vehicle software and hardware (e.g. whether they are operating appropriately).

3-3 Data accumulation function

This function is to accumulate sensor data and system log data uploaded from the vehicle for the purpose of understanding and analyzing the status of the vehicle.

3-4 Analysis function

This is a function of visualization and analysis of accumulated data for the purpose of investigating the causes of abnormalities and planning and improving data-driven services.

As a summary of this chapter, typical use cases (1) and (2) that are extremely important during system operation are introduced.

The screens shown below are snapshots taken from the PC used for visualization when the in-vehicle application life cycle management demonstration system was actually built. (* Some text has been added for this paper to make it easier to read.)

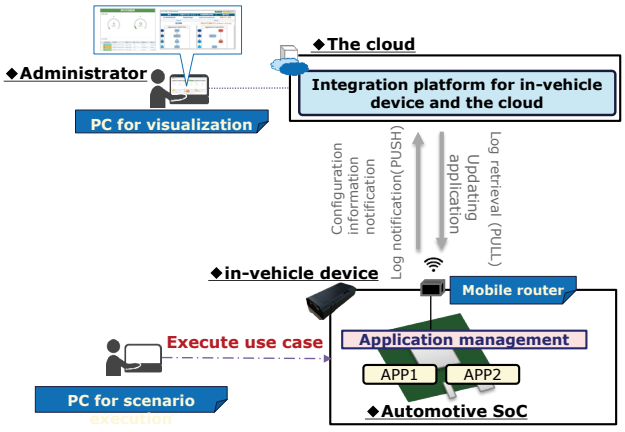

Fig. 8. In-vehicle application life cycle management Demo system

(1) Detecting and updating an outdated application

a) The system detects that an application in an older version is running in a particular vehicle.

b) The administrator selects the application for updating.

c) The system instructs the vehicle to update the application.

d) The vehicle updates the application as instructed and issues a completion notification to the cloud upon completion.

The following is an example of the transition of the management screen.

Fig. 9. The system detects that the version of the BodyCtrlSubApp, an application installed on the ECU X, is not the latest version (area enclosed by dashed lines in the figure). The administrator clicks on the area in question to view the details.

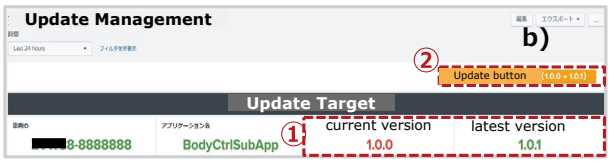

Fig. 10. The administrator decides that it is best to update the application to the latest version (area enclosed by dashed lines in the figure ①) and instructs the system to update the application (clicks on the area enclosed by dashed lines in the figure ②).

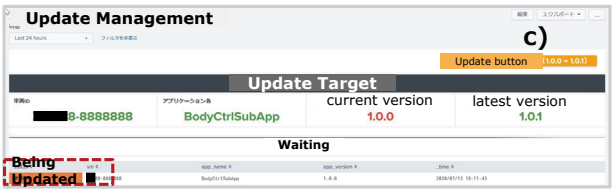

Fig. 11. Upon receiving the instructions from the administrator, the system issues instructions to the vehicle to update the application in question (OTA). On the screen, the state becomes “Being updated” (area enclosed by dashed lines in the figure).

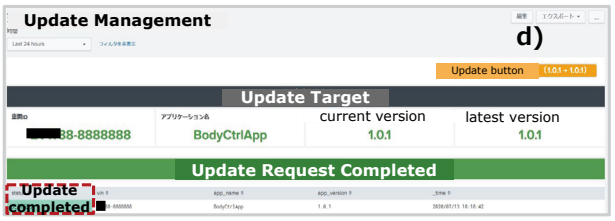

Fig. 12. Upon receiving instructions from the system, the vehicle updates the application in question and issues a completion notification to the system upon completion. On the screen, the state becomes “Update completed” (area enclosed by dashed lines in the figure).

(2) Detecting an unauthorized access and retrieving and analyzing detailed logs

a) The system detects unauthorized access.

b) The administrator grasps the situation from the existing data and instructs the system to retrieve relevant detailed logs to further grasp the situation.

c) The system instructs the vehicle to retrieve detailed logs and displays the logs received from the vehicle, and the administrator analyzes them based on the logs retrieved.

The following is an example of the transition of the management screen.

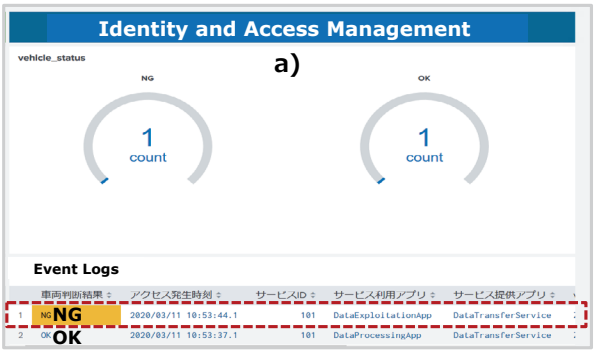

Fig. 13. The system detects unauthorized access (area enclosed by dashed lines in the figure). The administrator clicks on the area in question to view the details.

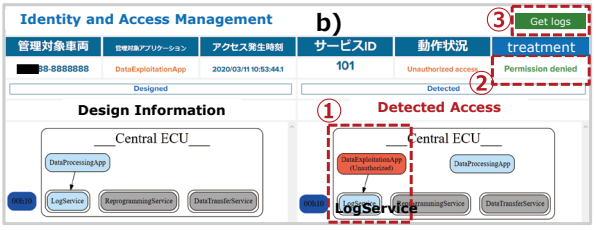

Fig. 14. The administrator confirms that a DataExploitationApp that has no access authority is trying to access the LogService, which can only be accessed by applications with administrative privileges (area enclosed by dashed lines in the figure ①), and that access was denied by the ID/access management function (area enclosed by dashed lines in the figure ②). To further grasp the situation, the administrator instructs the vehicle to retrieve logs of the relevant application (area enclosed by dashed lines in the figure ③).

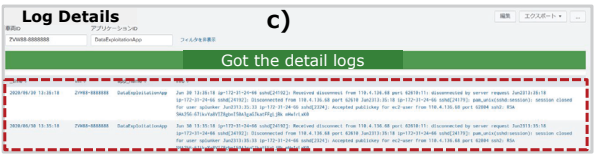

Fig. 15. The system instructs the vehicle to retrieve the log data of the relevant application and displays it on the screen after receiving the data from the vehicle (area enclosed by red dashed lines in the figure). The administrator conducts analysis and determines the cause based on this log data.

4. Conclusion

In this paper, we introduced the in-vehicle application management technology for managing in-vehicle applications and the in-vehicle application life cycle management system that applies this technology.

We believe that applying this technology and system and our logistics solution expertise to our product, Drive Link, will help to accelerate logistics DX. We are currently working to develop a fleet management system for connected vehicles for commercialization and plan to launch it as a successor to Drive Link.

Technical Terms

∗1 OTA: Abbreviation for Over-The-Air. It refers to the technology of sending and receiving data wirelessly.

∗2 Drive Link: This is a device manufactured by Sumitomo Electric System Solutions Co., Ltd. to be retrofitted to a vehicle for transmitting GPS data, Controller Area Network (CAN) data and other data to the cloud.

∗3 Logistics DX: To revolutionize the conventional way of logistics through mechanization and digitalization.

∗4 Eagle Sight: Total fleet management solution system manufactured by Sumitomo Electric Industries, Ltd.

References

(1) BOSCH, Mobility topics
https://www.bosch-mobility-solutions.com/en/mobility-topics/ee-architecture/
(2) Information-Technology Promotion Agency Security Center, Security Design Guide in IoT Development
https://www.ipa.go.jp/files/000052459.pdf
(3) Sumitomo Electric System Solutions Co., Ltd., Logistics solution
https://www.seiss.co.jp/ms/logistics/index.html
(4) Sumitomo Electric Industries, Ltd., started providing the delivery planning function to vehicle operation management system “Eagle Sight®”
https://sumitomoelectric.com/jp/press/2022/01/prs006

Contributors

The lead author is indicated by an asterisk (*).

J. YANO*
• Manager, Information Network R&D Center

K. TAKAKI
• Information Network R&D Center

T. MURAYOSHI
• Information Network R&D Center

T. HAGA
• General Manager, Information Network R&D Center

S. TAKIMOTO
• General Manager, AutoNetworks Technologies, Ltd.

R. TANAKA
• Manager, AutoNetworks Technologies, Ltd.