Approaches for Vehicle Information Security

Information Security for "Networked" Vehicles

Aug. 2013

IT Security Center,

INFORMATION-TECHNOLOGY PROMOTION AGENCY, Japan

This page intentionally left blank.

Contents

Figures

Tables

Background of the Guide

As most of the things are in this age, a vehicle is a collection of computers and software. People may surprise to know just one vehicle needs more than one hundred electronic control units (ECUs) and 10 million lines of code to function. What's more is that the on-board equipment like a car navigation system or telematics device are now connected to the Internet via smartphone and people can enjoy various services unavailable in the pre-Internet era.

In the field of automobiles, developers have been accumulating hi-tech and know-how to ensure the safety of passengers, and even if failures occur due to erroneous operations and malfunctioning, "safety" is warranted by fail-safe mechanism. On the other hand, with regard to "security" - protecting assets from malicious attacks by attackers, it's impossible to reduce the risk to zero. So, different ways of thinking than those for conventional safety are required, including balancing risks and costs.

In the case of information systems, to address security problems, developers design and implement security based on threat analysis results of their systems, and then handle vulnerabilities (security holes) detected in the system operation phase. Likewise, in the field of automotive systems, developers should leverage conventional safety feature as well as security knowledge obtained from information systems in handling security issues.

This guide presents potential threats faced by automotive systems and security measures against those threats, aiming at helping automotive system developers improve their security design. It also describes security efforts in each phase of automotive systems' lifecycle (i.e., planning, development, operation and disposal), so that developers can implement total security management throughout the lifecycle.

We hope that this guide is used as reference by the automotive system industry to provide high-quality products to consumers, both in terms of "safety" and "security".

Information-technology Promotion Agency, Japan	Hideaki Kobayashi
Information-technology Promotion Agency, Japan	Chisato Konno
Information-technology Promotion Agency, Japan	Makoto Kayashima
Information-technology Promotion Agency, Japan	Manabu Nakano

1. Preface

1.1. Current Status and Challenges Surrounding Vehicles Information Security

While the use of information technology in vehicles is advancing, the importance of vehicles information security is also increasing. Behind this background is the increase in the opportunities of and threats by malicious attacks that exploit the following three elements:

1) Use of software and networks by automotive systems

In addition to vehicles' inherent functions (run, turn and stop), to realize a variety of functions, software and network are used by vehicles and the software scale and network connectivity keeps expanding. Moreover, "openness of automotive systems", as represented by Window/Linux used for vehicles' operating system, and Ethernet and TCP/IP for in-vehicle LAN is advancing. While this enables the provision of various services to users, it may lower the level of difficulty of attacks.

2) Permeation of smartphone usage

Backed by the rapid permeation of smartphone, the provision of a cloud service in which smartphone and vehicles are interoperated has already started. Smartphone is an easy-to-use mobile computer with network connectivity, on which highly-functional applications run. So, when incorporating smartphone into vehicles, developers need to take into account the same security threats as those for PCs.

3) Emergence of new utilization forms of automotive systems

As car sharing and cloud services have become popular, there is a possibility that automotive system-related information is used by cloud. This may pose a risk in which sensitive information leaks to the other users of the shared car; the GPS data sent to the cloud is sniffed by an attacker and the driver's privacy is violated (e.g., his favorite places to visit are identified)

In 2010, researchers in the U.S demonstrated that an attacker could exploit vulnerability within in-vehicle software by manipulating inbound/outbound communications and cause troubles to the vehicle's control etc. [1]. Compromise of "Security" (i.e., protecting the vehicle and its passengers and information from malicious entities) could lead to compromise of "Safety" (i.e., protecting the vehicle and its passengers from rough roads, accidents and erroneous operations). To avoid this, "security" measures for automotive systems are urgently required.

1.2. Purpose of This Guide

This guide is intended for those involved in the vehicle industry, including vehicle manufacturers and vehicle parts manufacturers, and introduces efforts to achieve better security in automotive systems as well as security efforts levels, with which organizations can measure their level.

Firstly, to help readers get the concrete images of threats against automotive systems and countermeasures, description is given in the main body and "Appendix I: A Mapping Table for Functions, Threats and Countermeasure Techniques" is attached to the end. We hope that this guide is used as reference by developers to understand potential threats against the functions they are going to implement, and then consider countermeasures.

Secondly, security efforts in each phase of the lifecycle (i.e., planning, development, operation and disposal) and in the management that governs those phases are described. Each security effort has four levels, derived from hearing to embedded device vendors, and is described in the main body as well as "Appendix II: A Table for "Security Efforts" Levels in the Lifecycle" at the end of this guide. Organizations can use this to assess their security level, and learn what to do to improve their level for the items with a low level. By making upper-level efforts, organizations can achieve better security in their automotive systems and maintain it.

This guide assumes the following people to be readers:

- Those involved in planning and development, budgeting, personnel management at vehicle manufacturers and vehicle parts manufacturers, including decision makers (management executive);
- Providers of various services for vehicles
  (Developers of add-on in-vehicle equipments, developers of smartphone applications that work together with in-vehicle equipments, and developers and managers of in-vehicle systems-related services)

This guide was created based on "Security in Embedded Systems"[2], "Vehicle Information Security" and "Approaches for Embedded System Information Security" [3], all of which was released by IPA in the past.

2. Automotive Systems and Security

In this Chapter, we define "automotive systems" and based on the definition, we sort out threats and countermeasures.

2.1. Automotive System Model

When considering vehicles information security, developers need to take into account not only the vehicle itself, but also equipments that can be attached to and removed from the vehicle, equipments that communicate with the vehicle, and the services provided through those equipments, and then advance consideration. So, in this guide, "automotive systems" is defined as a system that consists of "vehicles" supplied by vehicle manufacturers, "add-on equipments" such as ETC (Electronic Toll Collection System) in-vehicle equipment and car navigation, and "peripheral services" such as ETC and telematics. Figure 2-1 Automotive Systems shows the internal architecture of the "automotive systems" defined in this guide. The purpose of this guide is to realize secure implementation and maintenance of automotive systems.

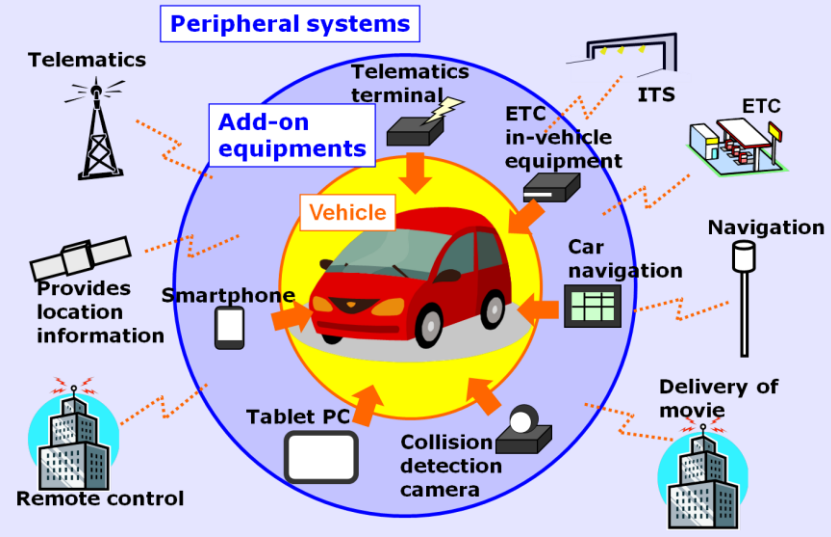

Figure 2-1 Automotive Systems

2.1.1. Internal Architecture of a vehicle

To consider vehicle information security in detail, this section performs more detailed sorting-out regarding "vehicle" and "add-on equipments" in Figure 2-1. In the case of vehicles, their internal architecture and functions vary depending on the manufacture and price range (grade), so it is difficult to define a common car model across the industry. For this reason, IPA established a car model called "IPA car", as shown in Figure 2-2, to conduct analysis of automotive systems security. For "IPA car", in-vehicle LAN was abstracted as much as possible, with all the functions connected with a single bus. "IPA car" has the following functions: "Basic control functions" such as "run" "stop" and "turn"; "Expanded functions" to enhance comfort and user-friendliness; and "General functions" such as devices brought into vehicles by users. Externally-connected ports may be included in each function, but here, we assumed them to be between "Expanded functions" and "General functions" and extracted and sorted out. Note that in this guide, "Basic control functions" plus "Expanded functions" is referred to as "in-vehicle systems", and these two functional categories are divided further into "drive-train", "infotainment", etc. This guide intends to consider threats against "in-vehicle systems" and countermeasures.

The functions included in "Expanded functions" are broadly divided into two groups. One is "Control-relevant function" ("Body", "Functions for safety and comfort" and "Diagnosis and maintenance"), which is closely related to vehicles' physical functions (i.e., run, stop and turn). The other is "Information-relevant function" ("ITS feature", "Telematics" and "Infotainment"), which is closely related to the functions for providing information to drivers. As for these two functional groups, there are gaps in functional behavior, services provided by using those functions, and risks arising when security problems occur. So developers need to consider security which is appropriate for the functions to be incorporated and the information handled.

Generally, for the functions that are related to vehicles' control and that fall in the categories of "Basic control functions" or "Control-relevant function", availability is valued, and for "Information-relevant function", confidentiality is valued.

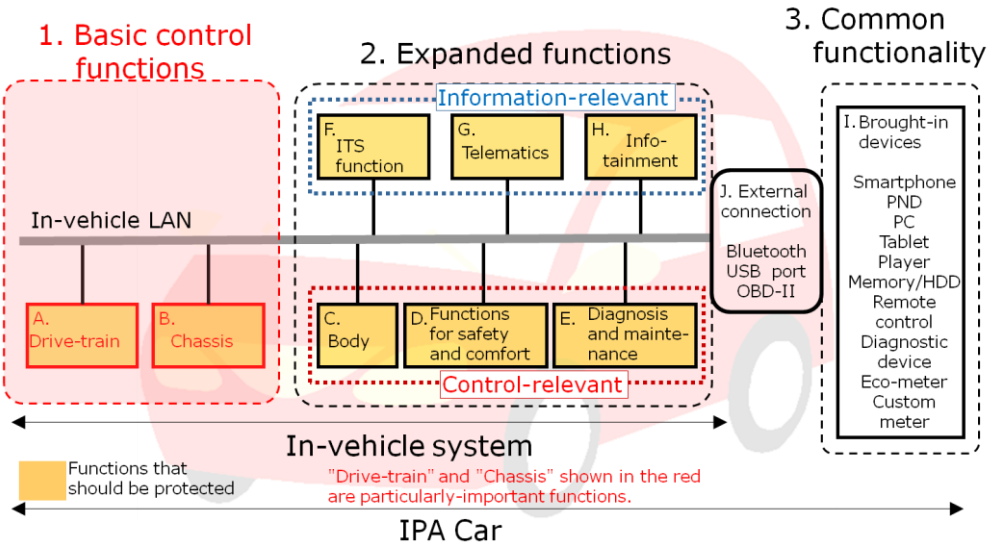

Figure 2-2 IPA Car System Model

Table 2-1 outlines "Basic control functions", "Expanded functions" and "General functions"

Table 2-1 "IPA Car" Functions

Functions	Description
1. Basic control functions	Functions that are related to vehicles' essential feature (i.e., run, stop and turn). Equipments for these functions are developed by vehicle manufacturers and upper-class vehicle parts manufacturers (Tier 1 suppliers) and safety mechanism is strictly incorporated. From the standpoint of security, how to ensure availability should be considered.
2. Expanded functions	Functions that are related to drivers' comfort and user-friendliness. These may be developed by vehicle manufacturers or service providers other than suppliers, and may be added to vehicles after the shipment in the form of add-on equipments. As a variety of information is stored and handled, not only availability but also confidentiality should be considered.
3. General functions	Functions that are provided by not only vehicles parts, but also brought-in devices such as smartphone, tablet and PND (Portable Navigation Device). Hardware and software to realize these "General functions" are developed by various service providers, so security measures based on the form of the brought-in devices are required.

"Basic control functions" should most strictly be protected in terms of security. Developers need to limit access from "Expanded functions" and "General functions", such as by using gateway. It is also important to be able to separate "Basic control functions" from "Expanded functions" and "General functions" in the event of an incident, and to maintain "Basic control functions" through the fall-safe mechanism.

Each functional category consists of the functions shown in Table 2-2.

Table 2-2 Capability of "IPA Car"

Functions			Description
1. Basic control functions	A. Drive-train		A control function which is related to "run", including the control of engine and motor, fuel/electric battery, and transmission.
	B. Chassis		A control function which is related to "stop and turn", including the control of brake and steering.
2. Expanded functions	Control-relevant	C. Body	A control function which is related to car body, including the control of door lock, air conditioner, light and direction indicator.
		D. Functions for safety and comfort	A function to automatically realize safety and comfortable driving, working together with automatic brake, lane-keeping control, inter-vehicle gap control and other functions to control vehicles.
		E. Diagnosis and maintenance	A function which is related to diagnosis and maintenance, including failure diagnosis by OBD (On-Board Diagnostics)-II
	Information-relevant	F. ITS feature	A function which is realized by roadside equipment and car-to-car communication such as ETC and ITS (Intelligent Transport System) spot.
		G. Telematics	A remote service feature, including collecting location information through mobile telephone network or other communication functions, and locking the doors or turning on the lights.
		H. Infotainment	A function which provides entertainment and information to passengers, including car navigation and audio equipment.
3. General functions	I. Brought-in devices		A function which is provided by brought-in devices such as smartphone, portable car navigation, and eco-meter.
	J. External connection		External connection interface for in-vehicle LAN (Bluetooth, Wi-Fi (Wireless Fidelity), OBD-II, USB (Universal Serial Bus) port, SD slot)

In the case of "I. Brought-in devices" alone, organizations can use security measures for PCs and smartphone, whose analysis has been advancing. However, when it comes to the case in which smartphone is used in combination with functions of an in-vehicle system, organizations need to include smartphone in their security consideration for "Expanded functions".

Though "J. External connection" can be exploited as an avenue for attacks, this guide assumes that it does not become the target of an attack. Therefore, this guide focuses on threats against and security measures for the functions covering "A. Drive-train" to "H. Infotainment" and sorts out and analyzes them.

2.1.2. Services Realized by Including Peripheral Systems

Services used by automotive systems are realized with in-vehicle systems and brought-in devices and peripheral systems working together, and easiness of implementing security measures varies depending on the service provision form. This guide classifies "services realized by including peripheral systems" into the three groups shown in Table 2-3. This can be used when considering a service that uses automotive systems.

Table 2-3 Service Classification

Service type	Description
X. Single-vendor service	This service is provided by a single company such as a vehicle manufacturer. ・Since the service is provided by a single company, considering security is easy. ・A vendor-specific protocol can be used (i.e. , closed within the developers).
Y. Multi-vendor service	This service is provided by multiple business entities in cooperation, with a vehicle manufacturer etc. taking initiative. ・Considering security requires information sharing among the multiple business entities. ・It is necessary to ensure compatibility among the service providers.
Z. Other service	This service is provided to the public via the Internet. A variety of business entities may provide this service. ・Ensuring security is up to the business entity, so considering unified security is difficult. ・An open protocol can be used, so if vulnerability is detected, the impact could be wide-ranging and fixing all within the range of the impact would be difficult.

2.1.3. Information and Other Assets Vehicles Should Protect

The objective of security measures is to ensure confidentiality (to prevent information leakage), availability (to be able to use when needed) and integrity (to protect from destruction and falsification etc. of information). When considering confidentiality and availability, organizations need to clarify what should be protected. So in this section, the objects that vehicles should protect are summarized in Table 2-4. The information and other assets that should be protected include: information generated while the vehicle is moving; information that the user registers in the vehicle; and communications with in-vehicle software and the outside.

Table 2-4 Examples of Information and Other Assets Vehicles Should Protect

Objects that should be protected	Description
Operation of "Basic control functions"	Coherence and availability of "Basic control functions", execution environment of "Basic control functions", communications for the operation.
Information unique to the vehicle	Information which is unique to the car body (vehicle ID, device ID, etc.), authentication code, and accumulated information such as running history and operation history.
Vehicle status information	Data representing the vehicle's stratus such as location, running speed, and destination.
User information	Personal information, authentication information, billing information, usage history and operation history of the user (driver/passengers).
Software	Software which is related to vehicles' "Basic control functions" and "Expanded functions". Examples include firmware for ECU (Electronic Control Unit).
Contents	Data for applications for video, music, map, etc.
Configuration information	Setting data for the behavior of hardware, software, etc.

2.2. Potential Security Threats against Automotive Systems

This section presents examples of potential security threats against vehicle systems.

When considering threats, in addition to the threats caused intentionally by attackers, the threats caused accidentally by users (e.g., by making mistakes) must not be overlooked. In this guide, the former is referred to as "threats posed by attackers' interference" and the latter "threats posed by user operation". This guide assumes that users do not have malice and never intentionally performs prohibited operations, and regards anyone (even the driver) performing operations with malice as an attacker.

2.2.1. Threats Posed by User Operation

Table 2-5 gives the outline and case examples of "threats posed by user operation" (For more details, see "Appendix I: A Mapping Table for Functions, Threats and Countermeasure Techniques".)

Table 2-5 Threats Posed by User Operation

Threat	Description
Incorrect settings	Threats caused by incorrect operations or settings by users, done through the user interface within the vehicle. Examples include: accidentally sending personally identifiable information to an unintended service provider while using infotainment feature; and disabling cryptic functionality of telematics communication, allowing the communications to be sniffed.
Virus infection	Threats caused by the infection of viruses or malicious software (malware etc.) to the in-vehicle systems, via a devices or storage medium brought into by the user. Examples include: a virus which infected an infotainment device spreads to the other in-vehicle equipments via the in-vehicle LAN.

2.2.2. Threats Posed by Attackers' Interference

Table 2-6 gives the outline and case examples of "threats posed by attackers' interference" (For more details, see "Appendix I: A Mapping Table for Functions, Threats and Countermeasure Techniques".) Attackers, with malice, interfere with the target system. They intentionally perform prohibited operations, abnormal operations and data entry to induce vulnerabilities.

Table 2-6 Threats Posed by Attackers' Interference

Threat	Description
Unauthorized use	The automotive system's functions may be used by an unauthorized individual, such as through spoofing or an attack to vulnerability within the equipment. Examples include: an attacker unlocking the vehicle by spoofing as the driver and performing the communication to unlock the vehicle.
Unauthorized setting	The automotive system's setting values may be altered by an unauthorized individual, such as through spoofing or an attack to vulnerability within the equipment. Examples include: an attacker altering network settings to make normal communication impossible.
Information leakage	The information that the automotive system should protect may be obtained by an unauthorized individual. Examples include: an attacker accessing accumulated contents or user information for various services, through the intrusion to the equipment or communication sniffing.
Sniffing	Communications between the in-vehicle equipments within the vehicle or communications between the vehicle and the peripheral systems may be sniffed or intercepted. Examples include: an attacker sniffing the vehicle's status information (running speed, location information etc.), while it is on the way from the vehicle to the peripheral systems for services such as navigation and traffic jam forecast.
DoS attack	The system may go down or the service may be denied due to unauthorized or excessive connection requests Examples include: an attacker performing excessive communications with the smart key to make a request for door lock and unlock by the user unaccepted.
Tampered message	A tampered message may be sent by an attacker to cause false move/display of the vehicle. Examples include: an attacker tampering a TPMS (Tire Pressure Monitoring System) message, so that the caution-advisory indicator of a normal vehicle blinks.
Loss of logs	The operation history may be deleted or altered by an attacker to make after-the-fact inspection impossible. Examples include: an attacker altering logs to destroy the evidence of the attack.
Unauthorized relay	The communication path may be manipulated by an attacker to hijack legitimate communications or to improper communications. Examples include: an attacker relying the smart key's electric wave and unlocking the vehicle from a remote site.

2.2.3. Direct and Indirect Threats

When an in-vehicle system' functions are attacked, the attack may be carried out via in-vehicle LAN or the physical connection interface linked directly to each function. The extent of impact of threats and the parts for which measures can be taken vary depending on the case.

In this guide, when considering threats, we assumed the followings:

Assumption (1): For "A. Drive-train", "B. Chassis", "D. Functions for safety and comfort" and "E. Diagnosis and maintenance", interface is limited to in-vehicle LAN. Hence, they shall not receive direct attacks.

Assumption (2): Functions other than the listed above have a physical connection interface linked directly to the outside. Hence, they may become the target of direct attacks.

For more details on the assumptions of the physical connection interfaces to the outside, see "Appendix I: A Mapping Table for Functions, Threats and Countermeasure Techniques".

■Direct Threats

In this guide, we refer the threats posed by attacks via the physical connection interface excluding in-vehicle LAN (e.g., wireless communication, USB port) as "direct threats". For example, "Body"-related functions can have wireless interface for smart key or TPMS (Tire Pressure Monitoring System), while "Infotainment"-related functions can have USB ports. In the past, an attack case was reported in which "a TPMS warning messages was tempered by an attacker to cause a vehicle's caution-advisory indicator to blink." Another reported case was that: "A telematics or infotainment connected to a mobile telephone network received DoS attack from the outside and used by an unauthorized individual." Figure 2-3 shows the functions that may receive "direct threats" (based on the prior incidents) and specific threats.

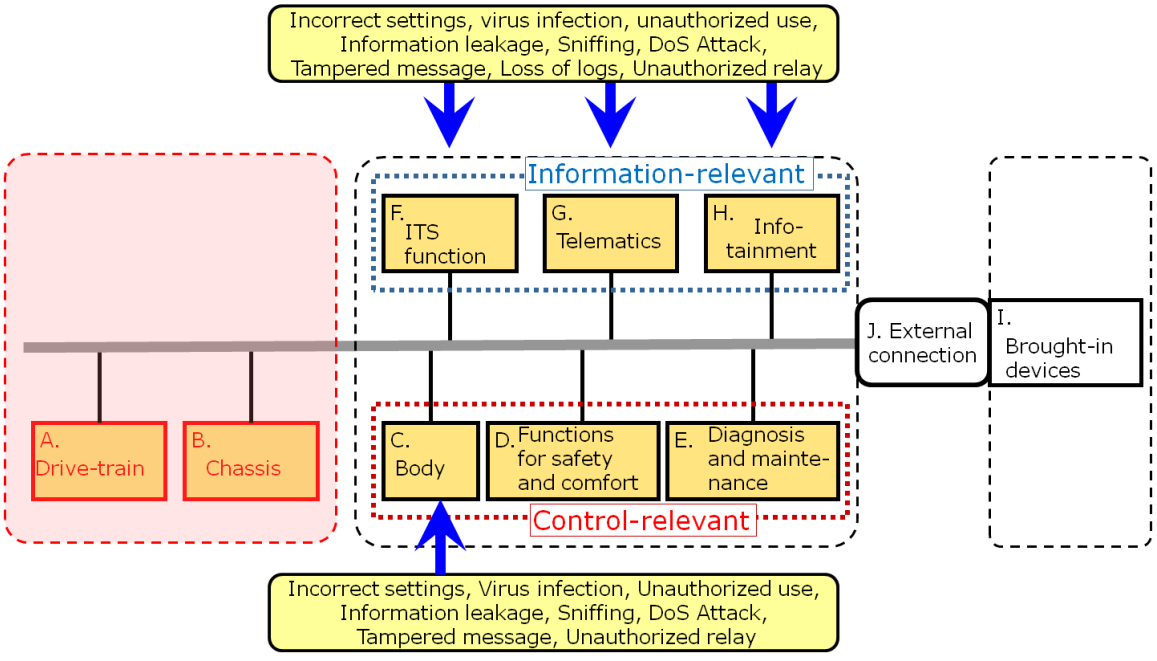

Figure 2-3 Potential Threats against Automotive System (Direct Threats)

■Indirect Threats

In this guide, we refer the threats posed by attacks via in-vehicle LAN as "direct threats". For example, generally, "Drive-train"-related and "Chassis"-related functions have no other external interfaces than in-vehicle LAN, so it is assumed that all communications are done through in-vehicle LAN. For this reason, it is less likely that these functions receive direct attacks from the outside. However, if the other functions receive such direct attacks and are infected with a virus, they may allow improper commands to be issued or malicious programs to be embedded through in-vehicle LAN. In this way, "Drive-train"-related and "Chassis"-related functions may also receive attacks via the other functions within a vehicle that are supposed to be reliable. Figure 2-4 shows the functions that may receive "indirect threats" (based on the prior incidents) and specific threats.

Entry paths to in-vehicle LAN include the functions that have physical ports of an attack via in-vehicle LAN from OBD-II (On Board Diagnostics). In the case of IPA Car whose all functions are linked to in-vehicle LAN, attacks against "Drive-train"-related functions and "Chassis"-related functions are possible, but in the actual internal architecture of a vehicle, generally gateways are placed between these "Basic control functions" and other functions, and thus safety is established.

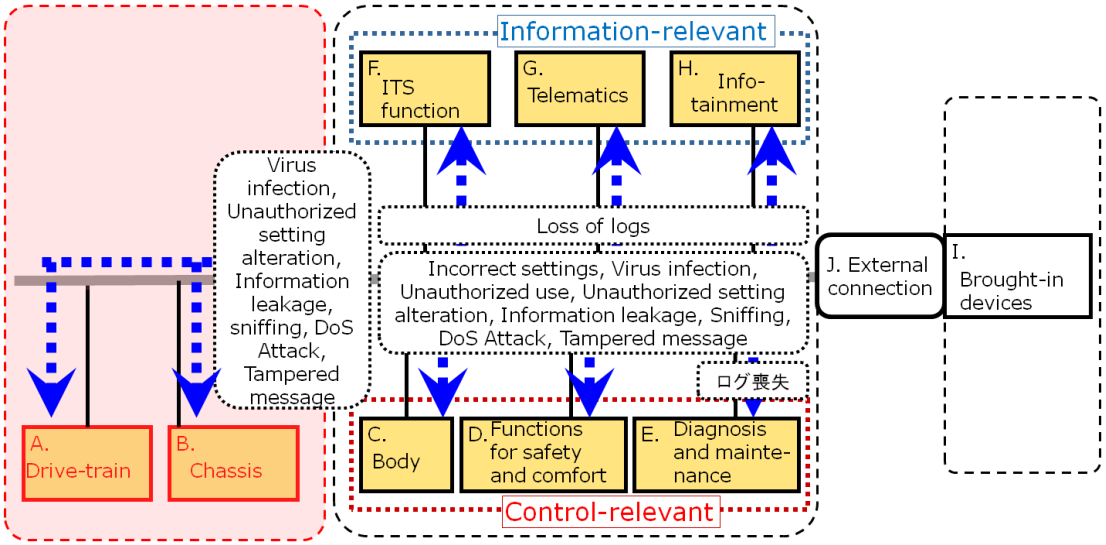

Figure 2-4 Potential Threats against Vehicles (Indirect Threats)

2.3. Security Measures against Threats

Security measures techniques that can be taken against threats to in-vehicle systems are described below. For more details on each technique, see Appendix I.

Table 2-7 Security Measures against Threats

Type	Security measures		Description
Security requirement definition	Requirements management tool		This tool enables users to sort out complex program requirements and manage the mapping of requirements and design/functions. By applying this tool to security requirements, organizations can prevent the omission of required security functions
Security function design	Security architecture design		This technique involves: clarifying the system's use case and model; conducting threat and risk analysis; and deciding how to respond and where to apply according to the security policy. It can prevent vulnerability creation due to the omission of required security measures
	Use of security functions	Encryption	As for encryption, there are "contents encryption" and "communication channel encryption". The former is for protecting information assets etc., and the latter for preventing communication sniffing. Processing speed and data volume vary depending on the encryption method, so organizations must select appropriate one based on their requirements.
		Authentication	A means for checking if the user/communicating end or the program to be added is legitimate one and not falsified. For authentication, password or software processing such as hash value, or specialized hardware such as integrated circuit chip can be used.
		Access control	Managing users' execute authority and executable functions and communications. By appropriately setting the extent of the impact of users and functions, organizations can prevent unexpected use, and then protect key functions from the problems arising in the other functions.
Secure implementation	Secure coding		A programming technique to prevent known vulnerabilities such as buffer overflow. It includes banning the use of the functions that may become the source of security holes as well as confusing code notation.
Security assessment	Security test		A means for making sure that a completed system has no vulnerability. There are some tools to detect known vulnerabilities and a technique to scan for unknown vulnerabilities (e.g.., fuzzing).
Other actions that can be taken	Provision of Manuals etc.		It is important to let users know correct usage and how to respond to security problems, such as through manuals. It is necessary to ensure that no security problem arises with factory default settings.

【Coffee Break】Security from the aspect of hardware

In these days, as typified by zero-day attack in which unknown software vulnerability is detected and exploited by a malicious third party to carry out an attack, attack methods are becoming more and more sophisticated. Given this situation, as fundamental countermeasures, an attempt to build a security infrastructure with not only software-based countermeasures but also hardware is considered, so that the safety of their computer systems and ultimately, the safety of information processing are ensured.

TPM (Trusted Platform Module), which is a technique for building hardware-based security infrastructure like this, is already manufactured and sold. TPM was developed by TCG (Trusted Computing Group) [4] and provides features such as random number generation, and encryption with public and private keys. To counter falsification or alteration, TPM checks if the software products used on the computer are legitimate ones and only when their legitimacy is proved, it allows their use. TPM calculates systems' legitimacy and checks if they are not falsified by malware etc. It does not allow the execution of programs whose legitimacy is not proved.

With regard to TCG, in the past, in the EVITA project, TCG members and European automotive industry exchanged information many times, and in March 2012, Toyota Motor joined TCG. As the need of vehicle information security increases, this effort will become more brisk

2.4. Map on Functions & Threats & Countermeasure Techniques

2.4.1. How to View the Mapping Table for Functions, Threats and Countermeasure Techniques

Up to here, we explained IPA Car, security threats and security measures against those threats. The relation among them is shown in "Appendix I: A Mapping Table for Functions, Threats and Countermeasure Techniques".

Each axis of the table is as follows:

(1) The vertical axis on the left side of the upper half indicates in-vehicle systems' functions;
(2) The horizontal axis on the left and right sides of the center indicates threats faced by in-vehicle systems;
(3) The vertical axis on the left side of the lower half indicates security measures against those threats.

The upper half in the table shows the mapping of (1) in-vehicle systems' functions and (2) threats faced by in-vehicle systems. In the table, ● indicates "direct threats" and ▲ indicates "indirect threats" (As for "direct threats" and "indirect threats", see Section 0.) Note that, though threats to "A. Drive-train" and "B. Chassis" are possible, both are generally strictly protected under the safety mechanism, and even if security threats arose, the effects would not be as severe as those in the case of other functions. For this reason, ash color is used for those threats

The lower half in the table shows the mapping of (2) threats faced by in-vehicle systems and (3) security measures against those threats. Here, ○ indicates security measures deemed effective in tackling that threat. By applying any of these countermeasure techniques (alone or in combination), organizations can have certain level of security measures in place, so that they can prevent threats from arising or minimize the extent of the impact should threats arise.

The table in "Appendix I: A Mapping Table for Functions, Threats and Countermeasure Techniques" is designed in that way that readers can begin with (1) in-vehicle systems' functions, and move on to (2) threats faced by in-vehicle systems and (3) security measures against those threats (See Figure 2-5 How to Use the Mapping Table for Functions, Threats and Countermeasure Technique).

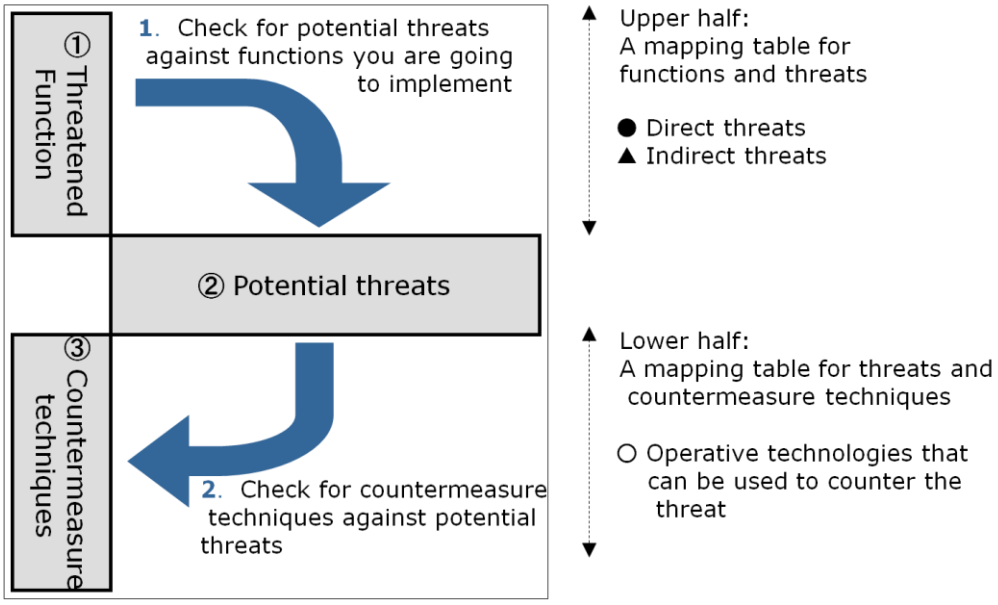

Figure 2-5 How to Use the Mapping Table for Functions, Threats and Countermeasure Techniques

3. Security Efforts for Automotive Systems

3.1. Lifecycle of Automotive Systems

3.1.1. Definition of Lifecycle of Automotive Systems

To improve vehicle information security, organizations need to include various information assets related to the vehicle in security consideration and implement appropriate security measures implemented based on the value of each asset. For this, it is effective to conduct analysis with automotive systems' lifecycle in mind. [3]. In this guide, automotive systems' lifecycle is divided into four phases - "planning", "development", "operation" and "disposal" - and explanation is given. For each phase of vehicles' lifecycle, the organizations and individuals shown in Figure 3-1 are expected to be involved.

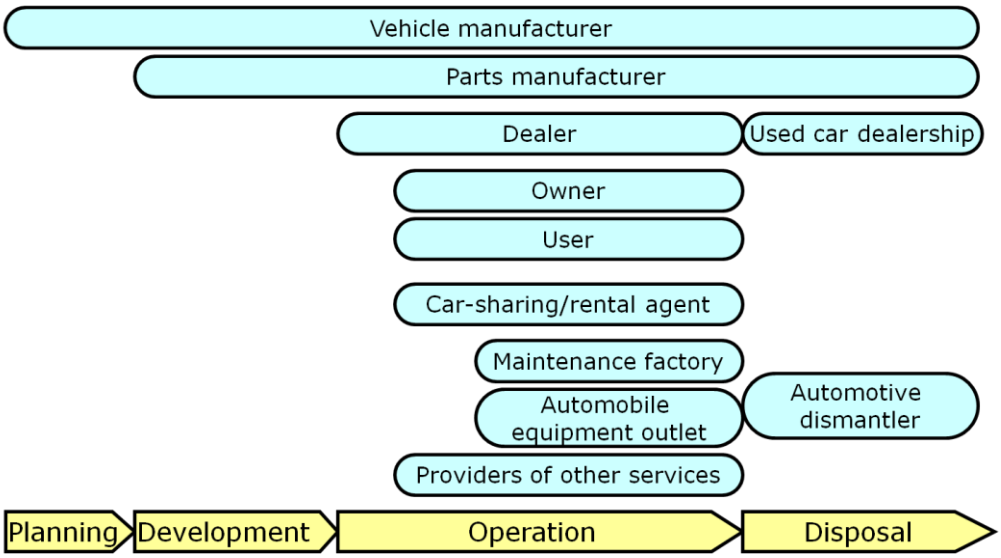

Figure 3-1 Lifecycle of Automotive Systems

Table 3-1 Those Involved in a vehicle during its Lifecycle

Those involved in vehicles	Description
Vehicle manufacturer	The vehicle's manufacturer. It engages in planning and development (design, implementation and manufacturing), sales, maintenance of the vehicle. Vehicle manufacturer is responsible for the manufacturing of the vehicle.
Vehicle parts manufacturer	Upon receiving commission from a vehicle manufacture, it develops and delivers the components of the in-vehicle systems.
Dealer	Sells the vehicle to a customer. It may have a maintenance factory.
Owner	The one who owns the vehicles (excluding car-sharing/rental agents)
User	The one who drives/uses the vehicle (may be identical to the owner)
Car-sharing/rental agent	A business entity that rents the vehicles to a customer.
Maintenance factory	Conducts car inspection, maintenance and repair, etc.
Vehicle equipment outlet	A business entity that sells/installs add-on in-vehicle equipments or vehicle parts. When the vehicle is sold as a used car, it is treated as "disposal", so the description is given in the disposal phase in Figure 3-1.
Provider s of other services	A business entity that develops and distributes software for in-vehicle equipments or brought-in devices, such as for telematics and contents delivery, and that provides services for vehicles.
Used car dealership	Takes the vehicle whose use is terminated and resells it.
Automotive dismantler	Takes the vehicle whose use is terminated and dismantles it

Below are the role and security issues of each phase of the lifecycle.

1. Planning Phase

The planning phase is where the product is planned by vehicle manufacturers. In this phase, for the vehicle to be developed, concept including user base, usage, services to be provided is established, and requirement specifications for functions and non-functions are drawn up and fixed as requirement definition. In this phase, budgets for throughout the lifecycle of the automotive system are considered and thus the level of "security efforts" (i.e., to what degree, the security of the product is emphasized) is determined. It is important to ensure that requirement definition includes security requirements and that requirement definition itself contains no vulnerability.

2. Development Phase

The development phase is where the hardware and software are designed by vehicle manufacturers or parts manufacturers based on the established requirement definition and the vehicle is implemented and manufactured. In this phase, it is important to ensure that: "requirement definition is correctly implemented", "no vulnerability is created during the implementation", and "even if vulnerability is contained, it is detected prior to shipment."

3. Operation Phase

The operation phase is where the vehicle is purchased by the user through dealers etc. and used. While in use, a variety of information, including the vehicle's status information such as location information, downloaded software, the user's operation history and the vehicle's travel history, is generated and accumulated.

In the case of vehicles, like shared cars, rented cars, and company cars, individuals other than the owner may use the vehicle and the driver may be replaced one after another in a short period. In this case, considerations from the standpoint of the privacy protection etc. of the accumulated information are required. Moreover, if any vulnerability is detected after the shipment, the developers should be able to inform the users/owners and respond in cooperation with dealers and maintenance factories etc.

4. Disposal Phase

The disposal phase is where the vehicle is relinquished by the user, for the reason such as purchasing new one or because it is broken. The relinquished vehicle may be sold as a used car to another individual through used car dealerships etc., or dismantled after the deletion registration procedure is performed.

The developers should be able to make users aware of how to remove personal information and other confidential information from the vehicle when they discard it.

3.2. Security Efforts Level and Security Policy for Each Phase

Based on what has been sorted out up to here, we classify each security effort at each phase into four levels (Table 3-2). As for the level classification, IPA conducted hearing to embedded device vendors and performed its own level classification. Here, in addition to the "planning policy", "development policy", "operation policy" and "disposal policy", "management policy" that governs those phases and that is common across the lifecycle is also added. Basic concept for this four-level classification is basically the same as that of "Approaches for Embedded System Information Security"[3], and vehicle-specific items are added.

Table 3-2 "Security Efforts" Levels in the Lifecycle

	Management policy	Planning policy	Development policy	Operation policy	Disposal policy
Level 1	No security effort is done.	Security is not taken into account when planning and designing a product.		No considered that how to respond to security problems arising after the product is shipped.	No Considered that how to handle residual information.
Level 2	Security effort is relegated to the on-the-spot personnel (such as planner, or developer). Issues are dealt with separately at each project.	Security consideration is relegated to the on-the-spot personnel (such as planner, or developer).		It is determined by on-the-spot personnel (such as customer representative, or developer) that how to respond to security problems arising after the product is shipped.	It is mentioned in the specification documents that how to remove residual information.
Level 3	Security effort is considered as an organizational issue. A security policy is drawn up and enforced.	Secure development based on the organization's policy is done.		It is established as an organizational policy that how to respond to security problems arising after the product is shipped.	A disposal procedure that mitigates the security risk is available.
Level 4	Security effort is considered as an organizational issue. A security policy is drawn up and enforced, and an audit is also conducted.	Secure development based on the organization's policy is done. And the contents are evaluated objectively.		It is established as an organizational policy that how to respond to security problems arising after the product is shipped. The organization has a contact point for external parties, which handles security-related information.	A disposal procedure that mitigates security risks, which is recommended by an official body, is available.

In the subsequent subsections, more detailed explanation of these efforts is given.

Note that, as for each effort, level 4 is "the level this guide hopes that the organizations will aim and achieve". What lies ahead of this is a cross-sectional effort within the industry, which is an ideal form. "If the efforts within a department can be expanded to organizational efforts and a check mechanism is in place …," this is what this guide covers. But if the efforts in each organization are unified into industrial efforts, more effective security measures would become possible.

3.2.1. Management Policy

A management policy is an attitude of the management toward the security. The main issues here are that how well the management and the on-the-spot personnel share their vision, draw up and enforce the policy. Note that the on-the-spot personnel include the person in charge of planning and the person in charge of development, the person/division in charge of customer support in the operation phase. The security efforts in each level are summarized below.

Level 1

At this level, no security effort is done.

This could be applied to the case where is no security policy and education that reason why management layer's security awareness is low or developer does not have enough budget and time for security At this level, an organizational policy is not provided and therefore, even if security is taken into account in the development phase, it may result in ad-hoc security measures.

Level 2

At this level, security effort is relegated to the on-the-spot personnel, and the security issues are dealt with separately at each project.

This could be applied to the case where the management and the on-the-spot personnel may consider that security is something both of them should work on together as an organization, yet, they do not know how and the issues are left to the on-the-spot personnel in reality.

At this level, the quality of the response differs per person in charge and the know-how and experiences learnt in one product are unlikely shared with other products, and since the management does not provide an organizational policy, it is difficult for divisions/persons involved to cooperate and for the organization to implement measures that are consistent throughout the lifecycle. .

Level 3

At this level, security effort is considered as an organizational issue, and a security policy is drawn up and enforced.

This could be applied to the case where the management and the on-the-spot personnel share the awareness of the security issues and document the policies, provide security education to the on-the-spot personnel and share problems and issues faced by the on-the-spot personnel.

Since they have an organizational policy and effort, improvement of the product quality can be expected. On another front, they still have challenges to address; that they should review and make sure that the policy is adequate and the rules are properly followed based on some objective evaluation process.

Level 4

At this level, security effort is considered as an organizational issue, and a security policy is drawn up and enforced. In addition, an audit is also conducted. Since the organization has such audit process, continuous review is possible and improvement can be expected.

This could be applied to the case where the management and the on-the-spot personnel share the awareness of the social responsibility and the roles they should assume over manufacturing the product, implement the process to objectively evaluate their effort, and set up a new team to promote their effort. To achieve this level, the management and the on-the-spot personnel must work together hard. Ultimately, this is the level this guide hopes that the organizations will aim and achieve.

3.2.2. Planning and Development Policy

A planning and development policy is an attitude toward security when planning and developing a product. The main issues here are, whether various activities in the planning and development phases are carried out based on the established security rules. The security efforts in each level are summarized below.

Level 1

At this level, security is not taken into account when planning and designing a product.

This could be applied to the case where there is no security standard and security risks are not discussed in the planning phase. The security problems tend not to emerge until the testing or operation phase. Moreover, they will be likely the types of the problems that have not been anticipated and may take very long time and high cost to solve.

Level 2

At this level, security consideration is relegated to the on-the-spot personnel.

This could be applied to the case where the person in charge is aware that reasonable measures are necessary to solve the problems like vulnerability, has knowledge of the implementation of security measures and some method to evaluate them, and implement them.

The quality of the security depends on the skills and knowledge of the parson in charge of development and cooperation among the persons involved is also insufficient. There are concerns such as, the requirement definition established in the planning phase may have security problems; gaps between the assumptions in the planning phase and the implementation in the development phase may become the source of security holes; and procedures established in the development phase may not be followed in the operation phase.

Level 3

At this level, based on the organization's policy, development is done with security in consideration.

This could be applied to the case where development is done based on the organizational policy, so that the security which is based on the vulnerability analysis results is implemented. At this level, it can be expected to eliminate most of the security risks in the upper processes. Moreover, a prompt response to problems (e.g., when an attack to the automotive system is detected) is expected.

Level 4

At this level, based on the organization's policy, development is done with security in consideration. The contents are evaluated objectively. Results of objective evaluation are fed back, and review and improvement are done.

This could be applied to the case where products are developed in accordance with security standard and therefore, reliable product development is possible. Ultimately, this is the level this guide hopes that the organizations will aim and achieve.

3.2.3. Operation Policy

An operation policy is an attitude toward security problems like vulnerability arising after the product is shipped. The main issue here is the implementation status of security measures after the product is shipped. The security efforts in each level are summarized below.

Level 1

At this level, how to respond to security problems arising after the product is shipped is not considered.

This could be applied to the case where the developers do not share vulnerability information within the organization, do not let the users know of voluntarily and when a security problem arises, they look into the matter and decide whether to leave it as a feature or to fix it depending on its seriousness.

Level 2

At this level, how to respond to security problems arising after the product is shipped is decided for each product by the person in charge of the Customer Relations department, the person in charge of development, etc.

This could be applied to the case where the persons in charge of the Customer Relations department deal with security problems within their division; the project managers and systems developers evaluate vulnerability and if it is serious, they let users know.

There are concerns such as, a system for responding to vulnerabilities detected within the product may not be in place; users with low vulnerability awareness may keep using the vulnerable version, making the problem even worse; and vulnerability information is not effectively shared within the organization and the same vulnerability may show up again.

Level 3

At this level, how to respond to security problems arising after the product is shipped is established as an organizational policy.

This could be applied to the case where the developers keep tabs on the vulnerabilities, decide when and how to respond and make sure to let those involved know if it is serious. When a security problem arises after the product is shipped, the organization can prevent the damage from spreading.

Level 4

At this level, how to respond to security problems arising after the product is shipped is established as an organizational policy. In addition, the organization has a contact point for external parties, which handles security-related information.

This could be applied to the case where the developers report the found vulnerability to the relevant organizations, and utilize vulnerability information available outside their company. At this level, when a similar incident occurs, the organization can use the case as reference and provide feedback to its security measures. Ultimately, this is the level this guide hopes that the organizations will aim and achieve.

3.2.4. Disposal Policy

A disposal policy is an attitude of users toward removing confidential information from the vehicle they are going to relinquish. The main issue here is how the developers handle residual information. The security efforts in each level are summarized below.

Level 1

At this level, how to handle residual information is not considered. This could be applied to the case where no disposal procedure is specified, and nothing about disposal is mentioned in the specification documents and the user guide.

Level 2

At this level, how to remove residual information is mentioned in the specification documents and the user guide.

This could be applied to the case where the product developers think it's mandatory to let the users know about the security risks and the recommended procedure when disposing the product. Depending on the product, however, it may be infeasible if it requires a specialized tool to remove the residual information stored on it.

Level 3

At this level, a disposal procedure that mitigates the security risk is available. This could be applied to the case where the product is equipped with a data destruction tool or the company offers a recycling system for in-vehicle systems.

Level 4

At this level, a disposal procedure that mitigates security risks, which is recommended by an official body, is available. With this level, it is assured that the product to be disposed of will have no residual information. Ultimately, this is the level this guide hopes that the organizations will aim and achieve.

4. Details of Security Efforts

In the previous chapter, we described security efforts in each phase of the lifecycle and outlined each level. Below are the specific items that should be implemented at each phase and indication of each level. Indication of levels is also summarized in in Appendix II at the end of this guide.

4.1. Efforts in Management

Here, we introduce specific items that should be implemented in the management that governs each phase of the lifecycle.

4.1.1. Drawing up Security Rules

Security efforts require the participation of all the people involved throughout the lifecycle. Not only the personnel within the organization, but also parts manufactures and the factory to which production is consigned, users, dealers, and maintenance factory etc. should be involved through education, enlightenment, cooperative framework, etc. Moreover, security efforts should be consistent throughout the lifecycle. For this reason, the management needs to establish an organizational policy and draw up security rules to realize it. When drawing up security rules, organization may use ISO/IEC 27002 [5], etc. as reference. Below are the specific items that should be drawn up.

1) Draw up Basic Policy

Draw up organizational information security policy according to its business requirements, and relevant laws and regulations

2) Draw up Measure Criteria and Management Policy

Common throughout the Lifecycle

"Rules on framework and division of roles within the organization", "Rules on human resource within the company", "Rules on relationship with outside the organization", "Compliance with laws and regulations and conformance to standards", etc.

Planning and development phases

"Rules on requirement definition", "Rules on design", "Rules on developmental regime and environment", "Rules on procurement", "Rules on factories to which production is consigned", etc.

Operation phase

"Rules on incident response" "Rules on the provision of information to external parties and format", etc.

Disposal phase

"Rules on discarded products", etc.

Levels concerning drawing up security rules are shown in Table 4-1.

Table 4-1 Levels Concerning Drawing up Security Rules

Level	Description
Level 1	No security rules are established
Level 2	Security rules are established voluntarily by the on-the-spot personnel.
Level 3	Security rules are established as an organization and documented.
Level 4	Security rules are established as an organization and documented. An audit to evaluate the compliance to the rules is also in place

【Coffee Break】Efforts for Control Systems Security

In the field of control systems, like vehicles, plants and management systems are connected to the Internet (i.e., networking) and general-purpose protocols and operating systems are being used (i.e., openness) and such trend is growing. There are also case examples of attacks having an impact on the society. In 2010, at a nuclear facility in Iran, the control program for the centrifuge was made unusable. Given this situation, in Japan, in October 2011, the Ministry of Economy, Trade and Industry set up a government-private sector joint task force. Here, we introduce two efforts currently underway, encouraged by this trend.

1. Cooperation with the Organizations Involved in Control Systems Security

In March 2012, with the goal of enhancing security for control systems of critical infrastructures and promoting export business, Control System Security Center (CSSC) was set up in the cooperation among industry, academic and government organizations [6]. CSSC engages in research on security technology for control systems, evaluation and authentication of control systems, and development of security testbed for control systems.

As of March 2013, CSSC holds the four committee meetings below, and in cooperation with relevant organizations in many different countries, it is advancing efforts for ensuring security for controls systems.

- ●Research and development/testbed committee
- ●Evaluation and authentication/standardization committee
- ●Incident handling committee
- ●Dissemination and enlightenment/human resource development committee

2. Establishing an Evaluation and Authentication Scheme for Control Systems

With the goal of establishing an evaluation and authentication scheme to ensure control system security in the nation and promote business overseas, IPA is acting for establishing an evaluation and authentication scheme for control systems. IPA selected International Standard IEC62443, which is currently being developed, as a unified, international security standard, and is collecting opinions on the standard from the people in the nation. Thus IPA is contributing to standardization activities. In addition, it is suggesting a pilot project (including demonstration experiment) for establishing such evaluation and authentication scheme.

Based on IEC62443-2-1, which was created based on Information Security Management System (ISMS) that is certification standard for general information system, organizations in Japan are advancing activities for establishing a domestic authentication scheme, as part of efforts to establish a conformity assessment system for Cyber Security Management System (CSMS). As for IEC62443-4-1 and 4-2 which are the authentication standard for the products and tools that comprise a control system, Japan is promoting cooperation with organizations overseas, so that it can realize mutual recognition with the overseas (mainly the U.S.A) which has already set up an evaluation and authentication scheme.

This effort servers as a reference when considering security for vehicles themselves and manufacturing lines in the future and thus would be very useful. As a vehicle-related enterprise, Toyota IT Development Center is already affiliated with CSSC.

4.1.2. Providing Security Education

Attack methods are daily researched by researchers and attacks and new vulnerabilities are also daily discovered. To counter new threats, in addition to complying with IEC61508 and IEC26262 to ensure safety, product developers must acquire information security knowledge and become familiar with security implementation and evaluation and secure usage. In security education, basic points should be disseminated, and refresh educations must be provided regularly so that employees can keep up with daily-changing attack methods and advancement of technologies.

It is advisable that security education involve developers, the person in charge of planning who draw up the product's requirement definition, the Customer Relations department, and other people who are involved in the operation phase. Sharing with divisions other than the system development division the knowledge of basic information handling, secure usage of the product, threat instances, and the latest trend, etc., enables secure product planning and development.

Below are the specific items that should be taught in the educations.

1) Security Rules

Educate about the security rules established in the management.

2) Knowledge of Security Technologies

(1) Basic Concept of Security

In the case of information systems, for the reasons such as the presence of attackers and advancement of information technology, it is not possible to fully cover the security in the operation phase during the development phase. For this reason, the developers need to consider the tradeoff between safety and cost and to construct a framework to respond to vulnerabilities detected in the operation phase. This concept may differ greatly from the concept of safety. In developing automotive systems, developers need to comprehend in advance the differences in safety and security concepts.

(2) Types of Known Vulnerabilities, Threats and Attach Methods

There is also a database in which vulnerabilities detected in the past are registered (such as [7]). Moreover, threats and attack methods that exploit vulnerability have certain patterns. These should be educated so that employees can eliminate similar vulnerabilities. In addition to car body, developers should acquire knowledge of vulnerabilities within brought-in devices such as smartphone.

(3) Secure Programming

Vulnerability can be created during the implementation. Developers should be educated about secure programming. Information on secure programming can be found the e-Learning Websites or books on the subject.

(4) Security Assessment/Debug Method

Developers need to test to see if security measures are implemented correctly in the design phase and the implementation phase. Specialized test tools are available. It is advisable to learn in advance the test method and the usage of those tools.

(5) Handling of Privacy Information

Within an automotive system, user information, including authentication information, billing

information, usage history and operation history, is stored. Moreover, utilization of a variety of vehicle status information (Table 2-4) is advancing. This information may be privacy sensitive (i.e., related to the user's privacy). So as not to violate users' privacy, developers should learn about the handling of privacy-sensitive information. It is advisable to acquire knowledge of basic concept and countermeasures against threats, by referring to "Eight Principles of OECD Board of Directors Advice" [8].

Table 4-2 Levels Concerning Providing Security Education

Level	Description
Level 1	No security education is done.
Level 2	A voluntary working session is held. The on-the-spot manager and personnel acquire the knowledge or organize study sessions as needed.
Level 3	Security education is provided as part of daily work. Attending security seminars and taking security training are encouraged.
Level 4	Security education is provided as part of daily work. Taking security training with an expert is required.

4.1.3. Collecting and Disseminating Security Information

It is important to collect the latest security information pertaining to automotive systems and quickly feed-back it to education and activities in the planning and development phases. Moreover, it is advisable to pass on information to not only developers but also users as needed.

Below are examples of items that should be collected and disseminated.

1) Case examples of Vulnerabilities, Threats, and Security Incidents pertaining to Automotive Systems

   Information on security threats against automotive systems can be found in the news and research papers etc. inside and outside Japan, and is delivered by IPA and other security-related organizations . In addition, the results of studies on vehicle security are presented at USENIX [9] and Escar (Embedded Security in Cars) [10]. In their daily work, developers need to pay attention to this information and conduct information collection.

2) Trend of Vehicle Security Standardization

   Vehicle-related industry groups within and outside Japan, such as Society of Automotive Engineers of Japan [11] and PRESERVE (Preparing Secure Vehicle-to-X Communication Systems), SAE (Society of Automotive Engineers) International [12], are conducting studies on vehicle security. Some of their outcomes are not publicized, but in some cases, outline is posted. Developers need to strive for information collection by participating in the industry groups, engaging in information exchange, and attending exhibition etc.

3) Information on Vulnerabilities within Software Products and Open Source

   Some of software products and open sources and brought-in devices such as smartphone may affect automotive systems' security. From the standpoint of security measures, it is important to obtain the latest vulnerability information pertaining to them from their vendors or community.

   In collecting vulnerabilities information pertaining to the IT software products and open source used widely in the nation, the Vulnerability Countermeasure Information Database (JVN iPedia [7]) and the Vulnerability Countermeasures Information Collection Tool (MyJVN [13]), both of which are provided by IPA, are useful. Information can be collected on Websites such as SecurityFocus [14].

4) Trend of Technologies pertaining to Information Protection such as Authentication and Encryption

   As for encryption/authentication technologies, to keep up with advancement of technologies and new attack methods, developers need to always grasp the latest technological trend. A list of cryptographic technologies whose use is recommended in the nation is included in the reports, provided by Cryptography Research and Evaluation Committees (CRYPTREC).

It is important to share this information with those involved, rather than just collecting it.

Table 4-3 Levels Concerning Collecting and Disseminating Security Information

Level	Description
Level 1	No security information is collected.
Level 2	Security information is collected by the on-the-spot manager and personnel as needed.
Level 3	There exists a system where security information is collected as an organization and disseminated to those involved.
Level 4	Security information is actively collected and accumulated and then utilized.

4.2. Efforts in the Planning Phase

In this section, we present specific items that should be implemented in the planning phase. In the planning phase, the product's concept is developed, requirement definition established based on the concept, and budget ensured.

4.2.1. Formulating Requirement Definition Considering Security

In the planning phase, not only the product's capability and performance and marketability, but also security for the entire automotive system is considered. Below are the items that should be considered.

1) How the Automotive System is Used

   For the automotive system to be developed, assume who is going to use it, when and where and how it is going to be used. In doing so, it is advisable to make assumption with the following points in mind.

   - Form of the peripheral systems that provide services (For peripheral systems, see "Table 2-3");
   - Assumption on service provision by add-on in-vehicle equipments;
   - Assumption pertaining to the operation phase and the disposal phase;
   - Assumption on security/maintenance as part of maintenance activity;
   - Impacts the peripheral systems may have on the in-vehicle system' basic control functions and expanded functions.

2) Assets Held by the Automotive System

   Clarify the assets the automotive system should protect (For the examples of assets, see "Table 2-4").

3) Potential Threats to the Automotive System and Risk Assessment

   Assume what threats may arise against the automotive system to be developed, and assess their impact (seriousness)

Table 4-4 Levels Concerning Formulating Requirement Definition Considering Security

Level	Description
Level 1	No security is taken into account when defining requirements.
Level 2	Security requirement definition is done by the department in charge or the person in charge.
Level 3	Security requirement definition is done in accordance with the organizational criteria.
Level 4	Security requirement definition is done in accordance with international standards such as CC.

4.2.2. Securing Security-Related Budget

Responding to security issues at lower processes would result in higher cost than doing so at upper processes. By including security measure cost in the budget at upper processes and implementing security measures, organizations can minimize overall cost and avoid major risks should security problems occur. Since security measures are required in the later phases than the planning phase (i.e., development, operation and disposal), organizations need to secure appropriate budget for security measures. Specifically, it is important to include the followings in their budget consideration.

1) Costs to be Incurred in the Development Phase
   (1) License fee of security libraries, tools, etc.;
   (2) Fee of a Security assessment tool, etc.

2) Costs to be Incurred in the Operation and Disposal Phases
   (1) Cost for designing and building a mechanism for operation and maintenance in the operation phase, including security update;
   (2) Cost for running an information provision site for users/owners and other people who are involved in the operation phase; cost for establishing and maintaining the Customer Relations department;
   (3) Cost for establishing and maintaining a system for incident handling; cost for incident response.

Table 4-5 Levels Concerning Securing Security-Related Budget

Level	Description
Level 1	No budget for security issues is ensured.
Level 2	Budget is considered when the on-site manager or personnel require and ensured if approved.
Level 3	There exists a system where a certain amount of budget is allocated to ensure security at each phase of the lifecycle as part of the development process.
Level 4	Budget is allocated to set up a specialized security team and put it on work.

4.2.3. Security Consideration When Outsourcing System Development

When developing a large-scale system, organizations may outsource part of the development. Likewise, in automotive system development, developers may outsource part of the implementation that is based on the design. To ensure the automotive system's security, organizations need to require the same level of security efforts within the outsourced party. Depend on circumstances, it may be difficult for organizations to apply their rules as they are to the outsourced party, but even in such a case, they should not leave security entirely up to the outsourced party and instead, should establish security rules that the outsourced party should follow.

1) Contract
   (1) Include in the commission of authority security-related items and security requirements;
   (2) Include in the commission of authority articles on the process to realize secure development;
   (3) Specify demarcation point of responsibility, and make clear in the contract document the scope of responsibilities in case security problems occur.

2) Assuring the Quality of the Development Team Members
   (1) Make it compulsory to receive education about security technologies and security rules;
   (2) Establish a mechanism to review security efforts in the development phase, such as joint review.

3) Assuring the Quality of Delivered Products
   (1) Provide criteria for selecting modules, coding conventions, and rules for review and test;
   (2) Decide on security assessment and debugging method, and prescribe the use of verification tools etc.;
   (3) Clarity how to check for the sufficiency of security requirements and the condition for the acceptance.

Table 4-6 Levels Concerning Security Consideration When Outsourcing System Development

Level	Description
Level 1	No security measure is taken into account when outsourcing. Even if the project has security features, the same outsourcing policy is applied.
Level 2	Security measure in the case of outsourcing is up to the voluntary effort by system developers or some project members. No uniformed effort is done even in the same department. Since it is done based on the knowledge and experiences of the project manager and system developers, there are no clear criteria.
Level 3	A contract for software development outsourcing requires an organizational security effort within the outsourced party to ensure security. An audit of the compliance with the contract conditions within or across the departments is included in the development process.
Level 4	In addition to the efforts in the level 3, there is a security team in the organization and it gives advice to the outsourced entity.

4.2.4. Responding to Threats Posed by the Adoption of New Technologies

Nowadays, a variety of services are provided through the combined use of brought-in devices (e.g., smartphone, tablet) and external severs. For these services, various new technologies such as TCP/IP technology (e.g., in-vehicle Ethernet) and vehicle control technology by in-vehicle camera are used. While networking and openness like these produce new ways of using, this may pose new threats.

1) Threats pertaining to in-vehicle Ethernet

After the transmission band for in-vehicle camera was ensured, a movement in which Ethernet and TCP/IP are used for in-vehicle LAN is advancing [15][16]. While TCP/IP facilitates access/connection from outside the vehicle, it also means that, various functions that are used to be separated physically/electrically are integrated on the same network (flattening). So, in order to mitigate threats to the vehicle's basic controls functions, developers need to consider partitioning networks and how to minimize the extent of impacts.

2) Use of Cloud, Threats pertaining to the Use of Smartphone

When cloud is used, the risk of vulnerability within the Web client on the in-vehicle equipment being exploited increases. There is also a high possibility that a virus-infected smartphone is brought into a vehicle. Moreover, like Information home appliances, in-vehicle equipments are expected to incorporate HTTP in the future. So, developers need to assume attacks to their in-vehicle systems and consider security measures, including security functions.

Particularly, with regard to smartphone, while its use with vehicles is in progress, security concerns are pointed out by many people. Since smartphone itself is not provided by vehicle manufacturers, developers need to assume the case in which smartphone becomes the source of threats, and implement security measures for their in-vehicle systems and mounted applications. For smartphone security, information can be found at [17].

3) Threats pertaining to Battery Charge

From now on, permeation of hybrid cars and electric vehicles is expected. In CHAdeMO (CHArge de Move) [18], which is an interface for vehicles' battery charge, not only electric power supply but also communications for battery charge control take place. For this reason, developers need to implement countermeasures against threats such as spoofing of a battery-charge station and alteration of control instructions. Vehicles' battery charge should readily be available in environments such as car parking areas, and measures to ensure safe use are required. In addition, developers need to assume new way of using (e.g., smart grid used with vehicles), potential threats and countermeasures.

Table 4-7 Levels Concerning Responding to Threats Posed by the Adoption of New Technologies

Level	Description
Level 1	With regard to what security influence may be brought about by the adoption of new technology, no consideration is done in the planning phase. Security requirement definition is not considered either.
Level 2	Consideration in the planning phase is up to the person in charge of planning.
Level 3	Items to consider in the planning phase are established.
Level 4	Items to consider in the planning phase are established. There is an audit process to review the contents.

4.3. Efforts in the Development Phase

In this section, we present specific items that should be implemented in the development phase. In the development phase, based on the requirement definition established in the planning phase, design, implementation and manufacturing are done. In the development phase, developers need to correctly implement the requirement definition, take required vulnerability countermeasures, and be careful not to allow vulnerabilities to be introduced. Should vulnerability be included, they should be able to detect it.

4.3.1. Designing

In the design phase which is an upper process of the development, it is important to design the system with security in consideration. Below are the items that should be implemented when designing.

1) Steady Implementation of the Requirement Definition

When the system becomes complex, developers may fail to design/implement some of defined security requirements, or have difficulty mapping requirements with design and implementation. To avoid this, it is effective to use a requirement management tool that help users sort out requirements and manage the mapping of requirements with design and functions.

2) Designing Security Architecture

In developing a system, developers need to make clear its usage and model, conduct threat and risk analysis, and implement security measures commensurate with the analysis results. A countermeasure against a threat may need to be implemented in multiple locations. It is effective to design the system in the way that consistency is maintained throughout the system, regarding where and how to implement countermeasures.

For a vehicle that is going to be used for a long period, it is likely that software update is required in the phases later than the operation phase for functional and security reasons. So, it is advisable to design software update feature.

3) Use of Security Functions

Based on the security architecture design, developers need to properly use security functions, such as encryption and authentication and access control.

With regard to encryption, there are "communication channel encryption" and "contents encryption". To prevent the leak of the information accumulated on the system, it is effective to use tamper-resistant modules.

With regard to access to a system, in order to check if the communicating end has a legitimate privilege, the system needs to use authentication feature. Authentication methods include: "user authentication" which verifies users' authenticity; "functional authentication" which verifies if the communicating end is a legitimate device; and "program authentication" which identifies malicious programs.

To prevent intrusion by attackers and security problems arising from erroneous operations, it is effective to perform access control. Access control methods include: limiting the range of communication by packet filtering etc.; or performing function/user-based privilege management.

4) Implementation of Audit Feature (Logs, Alert, etc.)

As for users' operations and access from the outside, regardless of being successful or failure, they must be logged in the way that they are not falsified. These logs can be used to identify the cause of

problems and locus of responsibility. In order to be able to notice attacks, it is effective to have a mechanism in place that issues an alert when suspicious communications or suspicious processes are detected.

【Coffee Break】 Watch out for Wireless Communication Channels

Since wireless communication channel are easy to sniff and relay, they may easily become the points of attack, compared to fixed lines. Moreover, depending on the wireless protocol stack or application implementation, like TPMS and GSM (Global System for Mobile communications), spoofing of base stations or the communicating end may be undetectable; moreover, as for generally used protocol stacks such as Bluetooth, a lot of vulnerabilities have been detected and reported[19].

Assuming that wireless communication channels possess low reliability, developers need to take measures, such as limiting their use to the minimum, not sending important information through wireless communication channels, implementing application level measures, and using a reliable wireless technology (e.g., 3G/4G instead of GSM).

Table 4-8 Levels Concerning Designing

Level	Description
Level 1	No security is taken into account in the design phase and it is not included in the specification documents
Level 2	Consideration on security in the design phase is up to the on-the-spot manager and personnel.
Level 3	An organizational security review policy that should be followed in the design phase is established. The design process is preceded following the policy.
Level 4	An organizational security review policy that should be followed in the design phase is established. The design process is preceded following the policy. There is an audit process for the security team to review the implementation process and defined security requirements.

【Coffee Break】 Threat Analysis by EVITA Project

EVITA (E-safety Vehicle Intrusion proTected Applications) project (hereafter EVITA) is a research and development project for in-vehicle LAN security technology and funded by EU. This project ended in November 2011, but in the document released as its outcome, concept of threat analysis adopted in the project is explained. So, this document would serve as a reference.

EVITA clarified the architecture of a system, its use cases, and the devices or other assets on the system that can be targeted for an attack, and then identified threats and conducted risk analysis against each threat.

In identifying threats, a method called Dark-Side scenario analysis was used. To schematize the relevance among threats, attack methods, and attacks to specific devices (asset attack), this method uses an attack tree similar to fault tree, which is used for hazard analysis at ISO 61508 etc.). Figure 4-1 shows the attack tree.

In the schematization by the attack tree, an attacker, attack goal, specific attach methods, and target devices for the attack are presented, and the relevance among them is shown. So the attacker himself is the base of risk analysis. At the lowest level (level 0) of the attack tree is the attack goal (e.g., "Unauthorized Brake", "Engine DoS-Attack"), which are linked to the benefit of the attacker. The attack goal is assumed by taking into account use cases and the attacker's motivation and capability. At Level 1, approaches to achieve this attack goal are shown. Each attack objective is discomposed further into attacks against specific devices and assets (i.e., Asset Attack) to achieve the objective.

In the risk analysis, threatened objects are categorized into "Operational", "Safety", "Privacy" and "Financial", and each category has level 0 through level 4. Since a threat may span multiple categories, the seriousness of each category is added up for the evaluation of the threat.

This threat schematization and risk analysis method would serve as reference when actually designing and developing systems

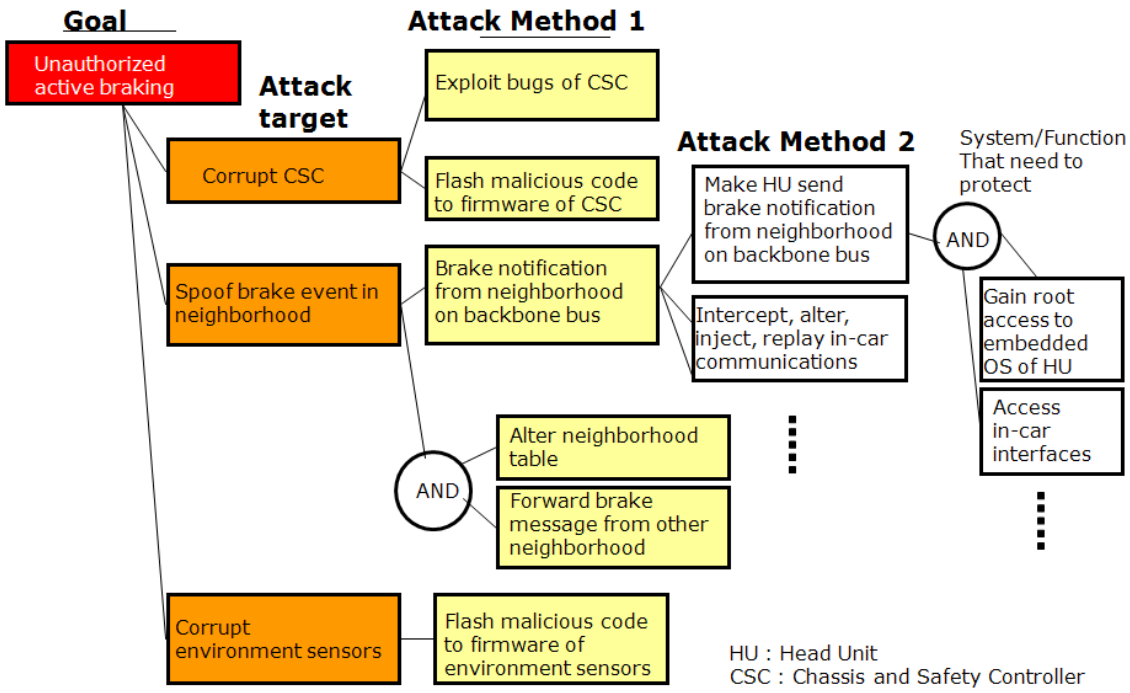

Figure 4-1 An Attack Tree for the Attack Objective "Unauthorized Brake"

4.3.2. Security Measures in the Implementation Phase

Even if security is sufficiently considered during the design, new security holes may be created during the implementation. Below are reference information and precautions.

As a technique to eliminate vulnerabilities, there is secure programming. For example, if a library that provides authentication or encryption is not properly implemented, an attacker may be able to bypass authentication and operate the system or break the encryption. Something that the system does not expect to handle, say, too long strings or unsupported character sets may cause an undesirable behavior of the system as well. For more information on secure programming, check out guidance is also found on the e-Learning Websites or books on the subject. It is effective to use a framework and establish coding conventions.

Table 4-9 Levels Concerning Security Measures in the Implementation Phase

Level	Description
Level 1	No security measure is taken into account when implementing.
Level 2	Security measures in the implementation phase are based on the knowledge and experiences of the project manager and system developers, so there are no clear criteria.
Level 3	There is an organizational policy and rules about coding and reviews that should be followed in software implementation to ensure security. System developers write source code following the rules.
Level 4	In addition to the efforts in the level 3, there is a specialized security team in the organization and it gives supports for secure cording and reviews. The security team is also involved with the rule making.

4.3.3. Security Assessment and Debugging

At the test phase, developers need to perform security assessment and debugging below, and detect and respond to vulnerabilities before the product is shipped by using tools.

1) Reviewing Source Code

In source code review, source code is cross-checked by technical personnel other than the developers to eliminate bugs and vulnerabilities resulting from errors or misconception. This review requires expert knowledge. An organizational effort to share knowhow and rules through security education etc. is required.

2) Applying a Static Analysis Tool for Source Code

For source code check, dedicated tools are available. For example, static analysis tools are capable of checking syntax errors and description errors, and some of them have a feature to measure various indexes such as reliability/maintainability. Though such feature is not directly linked to security, it helps enhance the quality of source code and prevent vulnerability such as bugs from arising.

3) Evaluating the Compliance to Coding Conventions

Through coding conventions, organizations can ban the use of the functions that may become the source of security holes and confusing descriptions. This helps eliminate security holes from the code and enhance maintainability and portability. Organizations may define their own coding conventions, or use publicized conventions for in-vehicle software such as MISRA C [20]. A tool for evaluating the compliance to coding conventions is provided by various vendors. This tool enables a thorough check and is effective in improving product quality.

4) Fuzzing

"Fuzzing" is a technique for detecting security holes in which a large volume of test data is sent to the system to be examined and how it responds or behaves is observed. When implementing fuzzing, organizations need to define the form, pattern, input means and confirmation method of the test data, based on the system. For more details on specific fuzzing, see "Guidance on the Utilization of Fuzzing"[21].

5) Conducting Vulnerability Assessment

A variety of vulnerability assessment tools are available on the Web, including TCP/IP Vulnerability Assessment Tool, "Nessus" (vulnerability scanner) [22], "OpenVAS" [23], "Nmap" (port scanner) [24], "Metasploit" (a vulnerability assessment tool that uses attack code) [25], and "Nikto2" (a diagnosis tool for Web servers) [26]. Based on the protocol used by the system, organizations need to select an appropriate tool and prevent known vulnerabilities from being introduced.

Table 4-10 Levels Concerning Security Assessment and Debugging

Level	Description
Level 1	Security assessment test is not done. There are no security-related test items, either.
Level 2	Security assessment test is planned based on the knowledge and experience of the project manager and system developers. The quality of the security testing depends on system developers' knowledge.
Level 3	There are organization-established security assessment procedure, items and criteria, and evaluation is done based on them.
Level 4	There are organization-established security assessment procedure, items and criteria, and evaluation is done based on them. The internal security team reviews the result.

4.3.4. Preparing for Web Contents to Provide Information to Users

Security problems occur in the operation phase in which the user actually uses the automotive system. For this reason, to users, dealers, maintenance factory, and vehicle equipment outlets and other people involved in the operation phase, information on security functions embedded in the automotive system should be provided, such as through the user guide and the display of precautions and warning messages.

Below is the security-related information that should be provided to users.

(1) Safe Use

It is advisable to explain how to securely use the automotive system (e.g., making appropriate settings such as setting passwords, not subscribing services provided by suspicious providers, and implementing software updates.) It is also necessary to add explanation about the potential risks when those actions are not taken.

(2) Dealing with Problems

It is advisable to explain the actions users can take immediately in the event of security problems, such as turning off the in-vehicle's power and changing the passwords, and to provide information on the contact point, etc.

(3) Disposal Procedure

For a vehicle, the user's personal information and other privacy-sensitive information may be registered. To help users remove such information properly, it is advisable to state clearly the following:

- How to use the data removal function
- How to confirm that the information has properly been removed

Organizations need to consider providing information to people other than users, such as dealers, maintenance factory, vehicle equipment outlets, used car dealership, and car-sharing/rental agents.

Table 4-11 Levels Concerning Preparing for Web Contents to Provide Information to Users

Level	Description
Level 1	No security-related statements are included in the contents for the provision of information.
Level 2	Security-related statements are included in the contents for the provision of information. Security precautions and troubleshooting procedure are posted. What to state is up to the project manager and system developers
Level 3	Security-related statements are included in the contents for the provision of information. Security precautions and troubleshooting procedure are posted. Selection of security-related matters to be posted and decision on what to state is done based the organizational criteria.
Level 4	Security-related statements are included in the contents for the provision of information. Security precautions and troubleshooting procedure are posted. Selection of security-related matters to be posted and decision on what to state is done based the organizational criteria. Their contents are updated on a regular basis and reviewed by the security team.

4.4. Efforts in the Operation Phase

In the operation phase, the product is handed over to and used by the owner. In this phase, dealers, maintenance factories, vehicle equipment outlets, car-sharing/rental agents, and providers of other services are involved in vehicles.

4.4.1. Handling Security Issues

Vehicle information security problems are not limited to the violation of users' privacy and theft and loss, but may jeopardize "safety" and involve human lives. To act swiftly against security problems, the actions below are required.

1) Establishment of an Urgent Contact Point

   Set up a contract point for receiving security-related information from users and those involved. The information received should be disseminated swiftly to those involved. It is effective to perform a regular exercise to see if the flow and procedure work as planned assuming that a security issue is discovered. For incident handling at an organization, see [27].

2) Establishment of a Cooperation Framework with Those Involved

   When a security problem occur, organizations may need to build a cooperate framework with the relevant organizations (e.g., parts manufacturers, dealers, and maintenance factories) to address it. It is necessary to work out arrangements on contact method etc. so that the division of roles and establishment of information sharing framework is swiftly done.

3) User Notification

   Organizations need to establish some kind of a "user notification system", assuming the case in which vulnerability is detected within the automotive system and a security patch is created and distributed. If possible, it is advisable to have multiple notification systems. For example, by reporting vulnerability information to IPA or JPCERT/CC, it is uploaded to the Vulnerability Countermeasure Information Database (JVN iPedia [7]) and the Vulnerability Countermeasure Information Portal (JVN [28]). If the developers wonder what kind of information or how much information should be made public, use the "Vulnerability Information Disclosure Manual for Software Developer" provided by IPA as reference.

Table 4-12 Levels Concerning Handling Security Issues

Level	Description
Level 1	No effort is made to respond to security issues (vulnerabilities) arising or discovered in the operation phase.
Level 2	Security issues arising or discovered in the operation phase are dealt with based on the judgment of the Customer Relations department and there are no unified rules/criteria within the organization.
Level 3	Security issues arising or discovered in the operation phase are dealt with based on the organization’s handling policy and criteria, and information is disseminated to those involved.
Level 4	Security issues arising or discovered in the operation phase are dealt with based on the organization’s handling policy and criteria, and information is released to and shared with industry groups and users.

4.4.2. Providing Information to Users and Those Involved in Vehicles

It is necessary to constantly provide information to users and those involved in the vehicle, rather than doing so only when a security problem actually occurs, and to communicate them repeatedly the new way of using and new services, information on vulnerabilities within the existing products, how to use the product safely, so that their security awareness is raised.

1) Providing Information to Users

It is necessary to disseminate information that users should be aware of in using their vehicle, including security information. It is advisable to consider a mechanism to automatically deliver information to users, rather than letting them to check the Website on their own.

2) Providing Information to Those Involved in the Vehicle

Information that should be provided to those involved in the vehicle includes: new services and their usage; potential threats and countermeasures against them; vulnerability information, incident handling procedures; security updates release information and how they are provided. Organizations may share with dealers etc. the information on new products along with security information. And since dealers and used car dealerships have opportunities to directly explain to users, it is effective to have them inform users of minimum-required matters for safe use.

Table 4-13 Levels Concerning Providing Information to Users and Those Involved in Vehicles

Level	Description
Level 1	Provision of security-related information to users and those involved in the vehicle is not done at all or on an ongoing basis. No mechanism for security update is provided.
Level 2	Security-related information for users and information on coping strategies such as security update as well as vulnerability information for those involved in the vehicle can be obtained actively by users and those involved via the developer's Website. With regard to security update, users can ask their dealer to take care of it.
Level 3	Provision of security-related information to users and those involved in the vehicle is done on a regular basis, through an automatic user notification. With regard to security update, users can ask their dealer to take care of it. Precautions regarding sell-out and delivery are communicated to those involved in the vehicle.
Level 4	Provision of security-related information to users and those involved in the vehicle is done on a regular basis, through an automatic user notification. Security update is provided through a mechanism such as automatic update. Whether or not such information has properly been disseminated to those involved is regularly checked.

4.4.3. Leveraging Vulnerability Information

The vulnerability information reported from the users and relevant organizations should be leveraged effectively in handling users and to prevent reemerging or affecting similar products. If vulnerability is found all too often, it will damage the corporate brand image and may affect management. By leveraging vulnerability information, divisions that received feedback are able to implement countermeasures within the division, and by cooperating each other, they can prevent the occurrence of vulnerabilities.

To fully leverage vulnerability information reported, it is necessary to create a database that summarizes vulnerability information and countermeasures, or establish a work flow to summarize and manage the vulnerability information and countermeasures.

Table 4-14 Levels Concerning Leveraging Vulnerability Information

Level	Description
Level 1	With regard to information on vulnerabilities arising or discovered in the operation phase, no effort is made to leverage it.
Level 2	Vulnerability information is leveraged by the department in charge of the operation.
Level 3	A workflow management system to leverage vulnerability information as an organization is established.
Level 4	A workflow management system to leverage vulnerability information and countermeasures as an organization is established and such information is available to those involved at each phase of the lifecycle.

4.5. Efforts in the Disposal Phase

In the disposal phase, the vehicle is dismantled or sold as a used car. When the vehicle is dismantled, after the deletion registration procedure is performed by the user, recycle part collection is done by a dismantler. When the vehicle is sold as a used car, it is taken by a used car dealership etc.

4.5.1. Drawing up and Disseminating Disposal Policy

Regardless of being dismantled or soled as a used car, the connection between the user and the vehicle is lost, so the information related to the user's privacy needs to be removed. Moreover, when the vehicle is dismantled, its use is terminated, so it is advisable to remove the information unique to the vehicle as well.

Table 4-15 shows examples of information that needs to be removed when the vehicle is dismantled or sold as a used car. Note that information handling varies depending on the case (i.e., being dismantled or sold as a used car).

Table 4-15 Information below should be Removed When the Vehicle is dismantled or Sold as a Used Car

Type	Description	Dismantling	Reselling
Information unique to the vehicle	Authentication information, failure history, operation history (functioning of air-bag, electric charge/discharge, etc.)	Remove	—
	Running speed, operation history	Remove	Remove
User information	Personal information, authentication information, billing information, usage history and operation history of the user (driver, passengers)	Remove	Remove
Contents	Data for applications for video, music, map, etc.	Remove	Remove
Setting information	Setting data for the behavior of software etc.	Remove	Remove

To get users to remove such information properly, the following efforts are required:

1) Providing the Data Removal Function

   Ideally, removal of information should be done with simple procedures. If possible, provide a data removal tool (command). Removal procedure should be undertaken on the responsibility of users/owners. So the user/owner of the vehicle need to perform data removal on his/her own, or to ask a dismantler.

2) Letting Users/Owners know of Data Removal Procedures

   Information that needs to be removed and how to do it should be communicated to users/owners. It is advisable to let them know of the followings at least:

   - Removal of personal information shall be done on the responsibility of users (owners)
   - How to use the data removal function
   - How to confirm that the information has properly been removed

An effort for the removal of personal information from cell phones at the termination of use is described in "The Policy for Removal of Sensitive Data from Cell Phone" provided by Telecommunications Carriers Association. For specific handling examples, see the information on each carrier's approach.

Note that privacy violation due to residual information may take place in the operation phase with a shared/rental car. When the shared/rental car is returned by the user, the car-sharing/rental agent should check and remove residual information, as done with a discarded car.

Table 4-16 Levels Concerning Drawing up and Disseminating Disposal Policy

Level	Description
Level 1	No consideration on security in the disposal phase is done
Level 2	Information about disposal and data removal is proved to the users through the user guide and the Website.
Level 3	Information about disposal and data removal is defined as an organization and proved to the users through the user guide and the Website.
Level 4	Information about disposal and data removal is defined as an organization and proved to the users through the user guide and the Website. The products are being tracked and there is a framework to work as an organization when disposing them

[1]. "Comprehensive Experimental Analyses of Automotive Attack Surfaces", CAESS, Stefan Savage, Tadayoshi Kohno and others, June 3, 2011, http://www.autosec.org/publications.html
[2]. 2010 Smart Home Appliance Security Study Report , IPA, February 1, 2011, http://www.ipa.go.jp/files/000014115.pdf
[3]. Approaches for Embedded System Information Security (2010 Revised Edition), IPA, February 22, 2011 http://www.ipa.go.jp/files/000014118.pdf
[4]. Trust Computing Group, http://www.trustedcomputinggroup.org/
[5]. The Information Security Standard, ISO, 7002, http://www.standardsdirect.org/iso17799.htm
[6]. Control System Security Center, http://www.css-center.or.jp/ (Japanese Only)
[7]. JVN iPedia, http://jvndb.jvn.jp/en/
[8]. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, September 1980, http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[9]. USENIX, https://www.usenix.org/
[10]. Embedded Security in Cars (escar), http://www.escar.info/
[11]. Society of Automotive Engineers of Japan, Inc., http://www.jsae.or.jp/
[12]. Preparing Secure Vehicle-to-X Communication Systems(PRESERVE), http://www.preserve-project.eu/
[13]. MyJVN, http://jvndb.jvn.jp/apis/myjvn/
[14]. SecurityFocus, http://www.securityfocus.com/
[15]. AVnu Alliance, http://www.avnu.org/,
[16]. OPEN ALLIANCE SIG, http://www.opensig.org/,
[17]. Japan Smartphone Security Forum, http://www.jssec.org/English.html
[18]. CHAdeMO, http://www.chademo.com/wp/
[19]. "Codenomicon warns about poor quality of Bluetooth equipment", Codenomicon, September 20, 2011, http://www.codenomicon.com/news/press-releases/2011-09-20.shtml
[20]. MISRA C, http://www.misra.org.uk/Activities/MISRAC/tabid/160/Default.aspx
[21]. Guidance on the Utilization of Fuzzing, IPA, 2012/9/20, http://www.ipa.go.jp/security/vuln/fuzzing.html (Japanese Only)
[22]. Nessus, http://www.tenable.com/products/nessus
[23]. OpenVAS, http://www.openvas.org/
[24]. NMAP, http://nmap.org/
[25]. Metasploit, http://www.metasploit.com/
[26]. Nikto2, CIRT, Inc., http://www.cirt.net/nikto2
[27]. Computer Security Incident Handling Guide, Recommendations by National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
[28]. JVN Japan Vulnerability Notes, http://jvn.jp/en/
[29]. "Hacker Disables More Than 100 Cars Remotely - Threat Level, Wired.com", March 7, 2010, http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/
[30]. "Security and Privacy Vulnerabilities of In-Vehicle Wireless Networks: A Tire Pressure Monitoring System Case Study", "Rutgers Univ"., "WINLAB", 2010
[31]. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars", ETH Zurich, 2011, http://eprint.iacr.org/2010/332.pdf
[32]. "Opportunities, Threats and Solutions for Connected Vehicles and Secure Telematics", Cellport Systems Secure TCU Architecture, http://www.itu.int/dms_pub/itu-t/oth/06/41/T06410000100004PDFE.pdf

Appendix I: A Mapping Table for Functions, Threats and Countermeasure Techniques (for in-Vehicle Systems)

(1) Functions threatened	1.Basic control functions	A. Drive-train		▲		▲	▲	▲	▲	▲		
		B. Chassis		▲		▲	▲	▲	▲	▲		
	2.Expanded functions	C. Body	●	●	●	▲	●*	●*	●*	●*		●*
		D. Functions for safety and comfort	▲	▲	▲	▲	▲	▲	▲	▲		
		E. Diagnosis and maintenance	▲	▲	▲	▲	▲	▲	▲	▲	▲	
		F. ITS feature	●	●	●	▲	●	●	●	●	●	●
		G. Telematics	●	●	●	▲	●	●	●	●	●	●
		H. Infotainment	●	●	●	▲	●	●	●	●	●	●

(2) Threats faced	Major cause of incidents			User operation		Interference by attackers							
	Threats			Incorrect settings	Virus infection	Unauthorized use	Unauthorized setting	Information leakage	Sniffing	DoS attack	Tampered message	Loss of logs	Unauthorized relay
(3) Countermeasure techniques	Security requirement definition	Requirements management tool		○		○	○	○	○		○		
	Security function design	Security architecture design		○	○	○	○	○	○	○	○	○	○
		Use of security functions	Encryption	Communication channel encryption			○		○	○				○
				Contents encryption			○		○					○
			Authentication	User authentication	○		○	○	○					
				Server authentication		○			○			○		
				Equipment and device authentication		○	○	○	○	○	○	○		
				In-vehicle equipment (ECU) authentication		○			○	○	○	○		
				Message authentication (verification)								○		
				Program authentication	○	○	○	○	○	○	○	○		
			Access control	Authority setting and minimization	○		○	○	○	○	○			
				Packet filtering			○	○	○		○	○		
				Domain separation	○		○	○	○	○	○			
				Network partitioning	○	○	○	○	○	○	○			
				Security controller	○	○	○	○	○	○	○	○		
	Secure implementation	Secure coding			○		○	○	○	○			
	Security test	Security assessment	Source code review	○	○	○	○	○	○	○		○	
			Static analysis tool		○		○	○	○	○			
			Evaluating the compliance to coding conventions		○		○	○	○				
			Fuzzing	○	○		○	○					
			Vulnerability test		○		○	○	○	○			
	Provision of Manuals etc.	Smart use											○
		User training		○	○			○	○				○
		Defined value security		○									

●Direct threats: threats posed by attacks via the physical connection interface linked directly to each function.
▲parts: threats posed by attacks via in-vehicle LAN.

Though threats to "A. Drive-train" and "B. Chassis" are possible, both are generally strictly protected under the safety mechanism and even if no security measure was implemented, the effects would not be as severe as those in the case of other functions. For this reason, ash color is used for those threats.
○Possible countermeasures: By applying any of these countermeasure techniques (alone or in combination), organizations can have certain level of security measures in place
The blank columns indicate that as of the date of publication (March 2013), no threat and countermeasure for that item existed.

* Indicates that only smart keys are affected by the threat.

[Assumption of Whether or Not Each Function Has Physical Connection Interfaces (Throughout This Document)]

Functional classification	Function	Has the Physical Connection Interface?
1.Basic control functions	A. Drive-train	No
	B. Chassis	No
2.Expanded functions	C. Body	Yes (e.g., RF for smart keys, wireless for TPMS)
	D. Functions for safety and comfort	No
	E. Diagnosis and maintenance	No
	F. ITS feature	Yes (e.g., Dedicated Short Range Communication (DSRC))
	G. Telematics	Yes (e.g., Mobile telephone circuit)
	H. Infotainment	Yes (e.g., Mobile telephone circuit)

[Threats Posed by User Operation] Due to operations performed by an authorized individual without malice

Threats	Description	
Incorrect settings	Instance	While using the infotainment function, the user accidently sends personally identifiable information to an unintended service provider; due to the telematics' communication encryption feature being disabled, communications are sniffed; and door-lock is not properly done.
	Description	This is the case where user operations unintentionally cause security problems such as abnormal action. Carelessness or flawed guidance is often attributable to such incorrect user operations.
	Condition	This could happen to functions that the user can directly operate or make settings.
Virus infection	Instance	As a result of copying contents from a smartphone to an infotainment device, the device is infected with a virus contained and the infection spreads to the other in-vehicle equipments on the in-vehicle LAN.
	Description	This is the case where the automotive system is infected with a virus or malicious software (such as malware). (Such viruses and malicious software often lurk in external media or portable devices such as smartphone, being part of the contents stored or software programs installed, and if those media or devices are connected to the automotive system, the infection takes place.)
	Condition	This could happen to functions for which a software program runs.

【Threats posed by Interference by Attackers】 Due to operations performed by an attacker with malice

Threats	Description	
Unauthorized use	Instance	A key is manipulated by an attacker who is neither the key owner nor a legitimate user who is permitted by the owner; diagnostic information is obtained, settings are altered, or configuration information is accessed by an unauthorized employee at a maintenance factory or auto supply shop, or by an attacker spoofing as an employee. An actual case was reported where an immobilizer was remotely operated by an attacker who illicitly obtained its account and then one hundred units of vehicles were made inoperative [29].
	Description	This is the case where the function is used by an unauthorized individual.
	Condition	This could happen to functions that users or maintenance personnel at a maintenance factory can directly operate.
Unauthorized setting	Instance	A device's password or encryption setting is cancelled; settings are altered by an attacker so that status information of the vehicle is automatically transferred to him; setting values are set to incorrect ones by an attacker, trying to cause malfunction of ECU or in-vehicle equipments.
	Description	This is the case where settings are altered by an attacker. It is done for the purpose of causing secondary threat such as unauthorized use and information leakage.
	Condition	This could happen to functions that users or maintenance personnel at a maintenance factory can directly operate. If the setting alteration can be done through external interfaces other than in-vehicle LAN, it becomes a direct threat, if done through in-vehicle LAN only (including settings via portable devices such as smartphone through an external interface), it becomes an indirect theat.
Information leakage	Instance	Accumulated software programs, downloaded contents, operation history and the user's accounts for various services are accessed by an attacker through the exploitation of vulnerability or improper settings.
	Description	This is the case where the information accumulated on the vehicle or generated by the vehicle is leaked.
	Condition	This could happen to functions where information is accumulated.
Sniffing	Instance	A TPMS message (in plain, unencrypted) is sniffed by an attacker, and from the tires' serial numbers contained in the message, the attacker finds linkage between the vehicle and a particular individual and violates the driver's privacy; while the vehicle's status information (such as running speed and location) is transmitted from the vehicle to the center of the car navigation/traffic-jam prediction service provider, the information is sniffed, or the driver's credential transmitted to the service provider is sniffed on the way.
	Description	This is the case where the communications among the in-vehicle equipments within the vehicle is sniffed, or the communications between an in-vehicle system and the external service provider's system is sniffed or intercepted.
	Condition	This could happen to functions that involve communication.
DoS Attack	Instance	A large volume of packets are sent by an attacker to a port whose access from the Internet is allowed for telematics and remote operation, in an attempt to impede such remote operation and service An actual case was reported where wireless communication for smart keys received DoS attack and the vehicle's lock operation was impeded.
	Description	This is Denial of Service Arrack. In this attack, the attacker issues extraordinary numbers of connection requests to a target machine so that it becomes unable to provide legitimate services or its system goes down due to excessive access burden.
	Condition	This could happen to equipments that have any interface.

【Threats posed by Interference by Attackers】(Continuation)

Threats	Description	
Tampered message	Instance	It has been pointed out that a TPMS message could be tampered so that the vehicle's caution-advisory indicator is turned on [30]. If the attacker succeeds in tuning on the vehicle's caution-advisory indicator and having the driver stops it, it could lead to a criminal act.
	Description	This is the case where messages are issued by someone other than authorized individuals or by non-legitimate systems
	Condition	This could happen to equipments that exchange messages with the outside.
Loss of logs	Instance	Logs on a system are deleted or altered by the hacker, and its vestige eliminated. Even worse, sufficient log function may not be in place from the beginning.
	Description	This is the case where the logs on the operations performed by the user/attacker are lost, or not generated, making it impossible to conduct after-the-fact inspection. Thus, when a problem arises, the user cannot confirm wheatear hazardous operations or setting alteration are performed; wheatear updates are properly applied, wheatear critical operations linked to the problem are performed, and whether the problem was caused by user operation or the system's malfunction. In such cases, further investigation would be impossible and locus of responsibility would remain ambiguous.
	Condition	For the functions "A. Drive-train" and "B. Chassis" and "C. Body", logs are managed by "Diagnosis and maintenance" function. So, this could happen to the function "E. Diagnosis and maintenance".
Unauthorized relay	Instance	LF bandwidth for smart keys is relayed by an attacker and the vehicle is unlocked from a remote site [31]. This actually happened in the past.
	Description	This is the case where vulnerably within wireless interface is exploited.
	Condition	This could happen to functions that have wireless interface to the outside.

[Security Measures against Threats]

Type	Security measures			Description
Security requirement definition	Requirement management tool			This is a tool for managing traceability from the requirement definition to the implementation. In the case of large-scale/complex systems, it is not easy to grasp the entire system and achieve coherence across the system. Organizations are required to properly conduct requirement definition and designing, as well as to ensure that all the items are implemented correctly and without omission. Requirement management tool enables users to sort out complex program requirements and manage the mapping of requirements and design/functions. By applying this tool to security requirements, organizations can prevent the omission of required security functions.
Security function design	Security architecture design			This technique involves: clarifying the system's use case and model; conducting threat and risk analysis; and deciding how to respond and where to apply according to the security policy. Through the vulnerability analysis, risk analysis and the implementation of those countermeasures across the system, organizations can protect their system with lean, appropriate security measures, and prevent vulnerability creation due to the omission of required security measures or incorrect assumption among the modules.
	Use of security functions	Encryption	Communication channel encryption	This technique involves encrypting data communication channels. In the EVITA project, EVITA HSM was mounted on ECU and the communication channels among ECUs were encrypted. Examples include WPA (Wi-Fi Protected Access) for wireless LAN and IPSec for Internet protocol. Like WPA (for wires LAN) and GSM (for mobile phone), an encryption method thought to be secure at one time may become no-longer-trusted due to a critical vulnerability detected. So organizations should be careful when selecting an encryption method.
			Contents encryption	This technique involves encrypting data flowing through communication channels or being accumulated. Examples include HTTPS, which is used to encrypt data transmitted to and from a HTTP server, and DRM (Digital Rights Management), which is used to protect accumulated video data.

[Security Measures against Threats] (Continuation)

Type	Security measures			Description
Security function design	Use of security functions	Authentication	User authentication	This technique involves authenticating users. In the case of widely-used, string-based "ID and password authentication", care must be taken as that they can be guessed or stolen. Among other examples are: IC card authentication, one-time password, twofold authentication which uses the combination of multiple authentication methods.
			Server authentication	This technique involves a client authenticating its server. It can prevent spoofing of servers. Examples include SSL (Secure Socket Layer), which is used by HTTP clients to authenticate Web servers. For server authentication, electronic certification is used. HTTPS is also an example.
			Equipment and device authentication	This technique involves authenticating the communicating end, such as equipments/devices and smartphone. Characteristics data generated based on product serial number etc. is used for this authentication. Electronic certification (client certification) can also be used.
			In-vehicle equipment (ECU) authentication	This technique involves authenticating in-vehicle equipments. There is no standard method, but there are examples such as EVITA HSM, and TPM can also be used (See Section "4.3.1").
			Message authentication (verification)	This technique involves authenticating messages sent by the communication end. This technique enables users to detect tampered messages or messages from a spoofed sender. A value obtained by applying hash function or block encryption algorithm to the message is used.
			Program authentication	This technique involves authenticating programs within a system. One example is to attach electronic signature to executable programs so that when users installs or upgrades them, they can confirm that they are from a reliable source. This also enables users to detect tampered programs. In addition, by examining the electronic signature attached, users can avoid executing a malicious program and ensure information security for the execution environment.
		Access control	Authority setting and minimization	This involves limiting users and processes that can access resources or that can execute functions, as well as keeping permitted matters to a minimum. SE-Linux, which performs access control based on the importance of each resource accessed at Linux kernel level, and virtual machine are also examples of this technique. Both can be used to reduce attack opportunity to a minimum and prevent threats from materializing.
			Packet filtering	This involves checking communication data that flows through communication paths or that arrived at the receiving end, and then blocking communications that are not permitted. This can be used to prevent unauthorized access from the outside.
			Domain separation	This involves grouping a program's modules based on the criticality in terms of security, and then restricting intergroup data exchange. This separates the parts affected by a failure or an attack from other parts. Gateway which is set up between "Basic control functions" and "Expanded functions" or between in-vehicle equipments is also one example of domain separation.
			Network partitioning	This involves partitioning a network such as in-vehicle LAN based on the criticality in terms of security, and then setting up a gateway in between to prevent unauthorized access. For example, in the case of a vehicle, it is possible to divide its in-vehicle LAN into the parts connected to "Basic control functions" and other parts, and then prohibit direct access from the latter to the former. This separates the parts affected by a failure or an attack from other parts.
			Security controller	This involves an access control function which is mounted on in-vehicle systems. For communications with different security requirements, security controller can be used to isolate sensitive information from the control and communication processing for a vehicle, and thus to ensure secure processing [32].
Secure imple-mentation	Secure coding			This involves a programming technique to prevent known vulnerabilities, such as buffer overflow and cross-site scripting. In other words, preventing the creation of vulnerability within a program. It is effective to ban the use of functions that may become the source of security holes as well as code notation that may elicit misunderstanding, as part of programing conventions.
Security assessmen t	Security test			This involves making sure that a completed program has no vulnerability. Examples include visual check of source code by humans, static verification by a tool, and dynamic verification in which the tester actually runs the program and verifies its behavior. For static verification, there is a tool that evaluates the compliance to coding conventions and a tool that analyzes source code and outputs statistical information. For dynamic verification, there is a tool that checks for known vulnerabilities and a tool that inputs abnormal data and confirms how the system works (i.e., fuzzing) (See Section 4.3.3)
Other counter-measures	Smart use			This involves devising a way of using that can prevent the emergence of security problems. For example, DoS attack may be carried out against wireless connection for a smart key and the vehicle's lock operation impeded. In such cases, vehicles should be able to let the user know through blink etc. so that they can properly lock it
	User training			This involves educating users not to perform any operations that may cause security problems and teaching them about risks as well as secure way of using
	Defined value security			This involves ensuring security with factory default settings. Examples include enabling security feature at the time of shipment, letting users choose to leave it or disable it at their discretion.

Appendix II: A Table for "Security Efforts" Levels in the Lifecycle

	Items to address	A	B	C	D	E	F	G	H	I	J	K	Level 1	Level 2	Level 3	Level 4
Management	Drawing up Security Rules (P21)	●											No security rules are established.	Security rules are established voluntarily by the on-the-spot personnel.	Security rules are established as an organization and documented.	Security rules are established as an organization and documented. An audit to evaluate the compliance to the rules is also in place.
	Providing Security Education (P23)	●											No security education is done.	A voluntary working session is held. The on-the-spot manager and personnel acquire the knowledge or organize study sessions as needed.	Security education is provided as part of daily work. Attending security seminars and taking security training are encouraged.	Security education is provided as part of daily work. Taking security training with an expert is required.
	Collecting and disseminating security information (P25)	●											No security information is collected.	Security information is collected by the on-the-spot manager and personnel as needed.	There exists a system where security information is collected as an organization and disseminated to those involved	Security information is actively collected and accumulated and then utilized.
Planning	Formulating Requirement Definition Considering Security (P26)	●											No security is taken into account when defining requirements.	Security requirement definition is done by the department in charge or the person in charge.	Security requirement definition is done in accordance with the organizational criteria.	Security requirement definition is done in accordance with international standards such as CC.
	Securing Security-Related Budget (P27)	●											No budget for security issues is ensured.	Budget is considered when the on-site manager or personnel require and ensured if approved.	There exists a system where a certain amount of budget is allocated to ensure security at each phase of the lifecycle as part of the development process.	Budget is allocated to set up a specialized security team and put it on work.
	Security Consideration When Outsourcing System Development (P28)	●											No security measure is taken into account when outsourcing. Even if the project has security features, the same outsourcing policy is applied.	Security measure in the case of outsourcing is up to the voluntary effort by system developers or some project members. No uniformed effort is done even in the same department. Since it is done based on the knowledge and experiences of the project manager and system developers, there are no clear criteria.	A contract for software development outsourcing requires an organizational security effort within the outsourced party to ensure security. An audit of the compliance with the contract conditions within or across the departments is included in the development process.	In addition to the efforts in the level 3, there is a security team in the organization and it gives advice to the outsourced entity.
	Responding to Threats Posed by the Adoption of New Technologies (P29)	●											With regard to what security influence may be brought about by the adoption of new technology, no consideration is done in the planning phase. Security requirement definition is not considered either.	Consideration in the planning phase is up to the person in charge of planning.	Items to consider in the planning phase are established.	Items to consider in the planning phase are established. There is an audit process to review the contents
Development	Designing (P30)	●	●							▲			No security is taken into account in the design phase and it is not included in the specification documents	Consideration on security in the design phase is up to the on-the-spot manager and personnel.	An organizational security review policy that should be followed in the design phase is established. The design process is preceded following the policy.	An organizational security review policy that should be followed in the design phase is established. The design process is preceded following the policy. There is an audit process for the security team to review the implementation process and defined security requirements.
	Security Measures Phase (P35)	●	●							▲			No security measure is taken into account when implementing.	Security measures in the implementation phase are based on the knowledge and experiences of the project manager and system developers, so there are no clear criteria.	There is an organizational policy and rules about coding and reviews that should be followed in software implementation to ensure security. System developers write source code following the rules.	In addition to the efforts in the level 3, there is a specialized security team in the organization and it gives supports for secure cording and reviews. The security team is also involved with the rule making.
	Security Assessment and Debugging (P36)	●	●							▲			Security assessment test is not done. There are no security-related test items, either.	Security assessment test is planned based on the knowledge and experience of the project manager and system developers. The quality of the security testing depends on system developers' knowledge.	There are organization-established security assessment procedure, items and criteria, and evaluation is done based on them.	There are organization-established security assessment procedure, items and criteria, and evaluation is done based on them. The internal security team reviews the result.
	Preparing for Web Contents to Provide Information to Users (P37)	●	●							▲			No security-related statements are included in the contents for the provision of information.	Security-related statements are included in the contents for the provision of information. Security precautions and troubleshooting procedure are posted. What to state is up to the project manager and system developers	Security-related statements are included in the contents for the provision of information. Security precautions and troubleshooting procedure are posted. Selection of security-related matters to be posted and decision on what to state is done based the organizational criteria.	Security-related statements are included in the contents for the provision of information. Security precautions and troubleshooting procedure are posted. Selection of security-related matters to be posted and decision on what to state is done based the organizational criteria. Their contents are updated on a regular basis and reviewed by the security team.
Operation	Handling Security Issues (P38)	●	●	○				○		▲			No effort is made to respond to security issues (vulnerabilities) arising or discovered in the operation phase.	Security issues arising or discovered in the operation phase are dealt with based on the judgment of the Customer Relations department and there are no unified rules/criteria within the organization.	Security issues arising or discovered in the operation phase are dealt with based on the organization's handling policy and criteria, and information is disseminated to those involved.	Security issues arising or discovered in the operation phase are dealt with based on the organization's handling policy and criteria, and information is released to and shared with industry groups and users.
	Providing Information to Users and Those Involved in Vehicles (P39)	●	●		○	○			○	▲			Provision of security-related information to users and those involved in the vehicle is not done at all or on an ongoing basis. No mechanism for security update is provided.	Security-related information for users and information on coping strategies such as security update as well as vulnerability information for those involved in the vehicle can be obtained actively by users and those involved via the developer's Website. With regard to security update, users can ask their dealer to take care of it.	Provision of security-related information to users and those involved in the vehicle is done on a regular basis, through an automatic user notification. With regard to security update, users can ask their dealer to take care of it. Precautions regarding sell-out and delivery are communicated to those involved in the vehicle.	Provision of security-related information to users and those involved in the vehicle is done on a regular basis, through an automatic user notification. Security update is provided through a mechanism such as automatic update. Whether or not such information has properly been disseminated to those involved is regularly checked.
	Leveraging Vulnerability Information (P40)	●	●							▲			With regard to information on vulnerabilities arising or discovered in the operation phase, no effort is made to leverage it.	Vulnerability information is leveraged by the department in charge of the operation.	A workflow management system to leverage vulnerability information as an organization is established.	A workflow management system to leverage vulnerability information and countermeasures as an organization is established and such information is available to those involved at each phase of the lifecycle.
Disposal	Drawing up and Disseminating Disposal Policy (P41)	●	●		○	○	(○)			▲	▲	▲	No consideration on security in the disposal phase is done	Information about disposal and data removal is proved to the users through the user guide and the Website.	Information about disposal and data removal is defined as an organization and proved to the users through the user guide and the Website.	Information about disposal and data removal is defined as an organization and proved to the users through the user guide and the Website. The products are being tracked and there is a framework to work as an organization when disposing them

Explanatory note: A stands for vehicles, B for parts manufacturers, C for dealers, D for owners, E for users, F for car-sharing/rental agents, G for maintenance factories, H for vehicle equipment outlets, I for provider s of other services, J for used car dealership, K for automotive dismantlers

Meaning of the symbols: ●Read this guide and act on their own initiative, ○Take the action, encouraged by the actor (it is recommended to read this guide and act proactively), ▲Use this guide as reference * Car-sharing/rental agents implement the recommended approach for the disposal phase in this guide in their operation. phase.

Glossary

Term	Description
IPA Car	An automotive system model crated by IPA. In order to facilitate the examination of automotive system security, functional classification and prioritization are done for this model.
Add-on in-vehicle equipment	In-vehicle equipments added to in-vehicle LAN after the shipment. Examples include collision-prevention system and driving control system.
Incident handling	Handling security problems arising in the operation phase.
Operation	A phase in which the vehicle is sold to the user (owner) by a dealer. In this phase, the vehicle's manufacturer performs tasks such as incident handling, maintenance and customer support.
Development	A phase in which the product is designed, implemented and manufactured based on the requirement definition established in the planning phase.
Planning	A phase in which the concept of the product is established, budgeting is done and requirements are defined.
On-the-spot personnel	Personnel in charge of planning, development and operation within that organization. In this document, it refers to the "management layer".
Service provider	An entity that provides services to vehicles from their outside via network, through the combination with terminal equipments (e.g., ITS, telematics) and add-on in-vehicle equipments Throughout this document, car-sharing/car rental-agents are collectively referred to as "providers of other services".
In-vehicle system	An information system that is mounted on the vehicle shipped by its manufacturer. It does not include add-on in-vehicle equipments or devices that are brought into and used by the car users, such as Tablet PC and smartphone.
Automotive system	It refers to a system consisting of a vehicle shipped by its manufacturer and the information systems related to the vehicle. It includes the "vehicle" (in-vehicle system) shipped by its manufacturers, tablet PC and smartphone, add-on in-vehicle equipment or other "peripheral equipment" (brought-in devices), and "peripheral system" that provides services via network such as ITSand telematics.
Vehicle manufacturer	The vehicle's manufacturer (OEM).
Peripheral system	A system that enables service providers to provide a variety of service to vehicles from their outside.
Control-relevant function	A function that is related to the mechanical control of the vehicle, It includes door lock, opening and closing of windows, and control of air conditioners.
Information-relevant function	A function that is not directly related to the control of the vehicle. Examples include car navigation.
Vulnerability	Security flaw in systems that could be exploited by unauthorized access or computer viruses and allow the degradation in functionality and capability of the system.
Security	Protecting the vehicle, its passengers and information from malicious attackers. As a new utilization form of vehicles emerged in which software and networks and devices such as smartphone are used with a vehicle, security is becoming more and more important. Traditionally, vehicles have been protected by "safety", but from now on, countermeasures that entails security element would be necessary. This document covers only security aspect. See <Safety>.
Safety	Protecting the vehicle and its passengers from rough road and accidents. In the field of vehicles, safety has traditionally been of great importance, and it is assumed that, vehicles shipped are protected with advanced safety technology. Safety and security are complementary to each other, and vehicles are protected with both or either of them, depending on the characteristics of the functions and assets that should be protected.
Security architecture	Security architecture shows what security measures should be implemented where within the system. It should be based on the results of risk assessment for potential threats.
Security rule	Organizational security policy (basic policy and measure criteria concerning security efforts) and managerial rule (specific steps) that are established by management personnel. It concretely defines what must be done and what must not be done.
Organization	A unit for which security rules are established. "Organization" may be a business entity engaging in system development, or an enterprise group having affiliate companies and engaging in system development as a unit. Each department within an enterprise is not regarded as "organization".
Disposal (of vehicle)	Relinquishment of a vehicle by its owner. The vehicle may be sold out as previously-owned one or scrapped.
Cancellation of vehicles	An option of disposal. Instead of selling the vehicle as a used car, the owner performs the deletion registration procedure and discontinues its use. Unlike being sold as a used car, there is no next user.
Malicious program	A program that is covertly installed on the automotive system without the legitimate user's intent and cause adverse effects on the system.
Parts manufacturer	A manufacturer (supplier) that supplies parts etc. to vehicle manufacturers. In this document, upper-class parts manufacturer are referred to as "major parts manufacturer".
User	The own who drives the vehicle. This may not be identical to the vehicle's owner.
User's guide	A guide for users that comes with the shipped product (vehicle). It covers usage and precaution statement etc. This guide is created in the development phase.
Requirements	Matters that are required of the product. Requirements are defined in the planning phase.
Requirement definition	Clearly defining and documenting "requirements". It does not include implementation. Requirements are defined and documented in the planning phase. The documented requirements serve as input to the development phase.

This page intentionally left blank.

This page intentionally left blank.

For more information:

IT Security Center, Information-technology Promotion Agency of Japan
Bunkyo Green Court Center Office, 16th Floor,
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, 113-6591, Japan
TEL: +81-3-5678-7527　FAX: +81-3-5978-7518
E-mail：vuln-inq@ipa.go.jp　URL：http://www.ipa.go.jp/security/english/

This guide is available for download at:
URL：　http://www.ipa.go.jp/security/fy24/reports/emb_car/index.html

2013/3/25　First Edition (In Japanese)
2013/8/20　First Edition (in English)