Security Guidelines for Product Categories

- Automotive On-board Devices -

Ver. 1.01

CCDS Security Guidelines WG
Automotive On-board Devices SWG

Revision History

Version	Date	Description
Ver.1.0	June 8, 2016	Created a new edition
Ver.1.01	June 15, 2016	Maintained Partial Format

■Trademarks

・All company and product names mentioned in this book are company trademarks or trademarks registered.

■Further notices

・All information provided in this book is stated at the time of publication and may change without notice.

・Any copying or reprinting of the contents of this document without obtaining permission from CCDS is prohibited.

CONTENTS

1 Introduction

To date, every product industry has formulated its own safety standards. Security standards relating to organizational administration (ISO27001) and product design security assessment and authentication (ISO15408) have already been formulated, while recent years have witnessed the formulation of standards targeting control systems for critical infrastructure (plants and facilities essential to social infrastructure) (IEC62443).

With the popularity of IoT, devices in widespread use are supporting a variety of networking features, increasing security concerns. That said, it is undeniable that security standards relevant to IoT products and services are not yet sufficiently in place.

In the U.S. and European nations, moves are underway to determine security standards by using industry-specific safety standards. However, while in Japan there are tangible security concerns that may lead to the establishment of security standards, there are few areas where practical discussions have yet led to action.

The Connected Consumer Device Security Council (CCDS) was established in response to this situation. The Council is committed to formulating security standards for common devices and launching an authentication program to confirm and verify compliance with these standards in order to reassure users of IoT products.

On August 5, 2015, the Information-technology Promotion Agency, Japan (IPA) launched the IoT Safety/Security Development Guidelines Review WG to initiate discussions on security at the national level. The CCDS has come together with the IPA-WG to establish a number of proposals concerning the results of the reviews of guidelines within the CCDS.

On March 24, 2017, the results of the reviews at the IPA-WG were compiled and released as “IoT Safety/Security Development Guidelines - Important Points to be understood by Software Developers toward the Smart-society [1]”. While the IPA's development guidelines focus on the common subjects by comprehensive approach, the CCDS field-specific guidelines is developed for locating individual industry specific safety and security promotion of design or development process.

1.1 The Present Status of, and Security Issues Relating to, Automotive On-board Devices

Rapidly developing car technologies, such as self-driving and connected cars, have greatly increased user convenience. Unfortunately, the incidence of cyber-attacks that threaten safety and security are also increasing, meaning that cars connected to networks or devices taken into the car is vulnerable to such attacks. At Black Hat 2015, a U.S. security-related conference, there was a reported case of a jeep being successfully hacked into by exploiting the vulnerabilities of the Chrysler connected car system: “Uconnect. ” Clearly, there is a real threat of the steering, brakes or other systems being controlled by a malicious false signal to ECU via on-board LAN or other devices.

The possible damage caused by the hacking of an automobile could endanger human life. Security is therefore essential, and so supervisors, managers, and developers, are all endeavoring to improve security within their respective fields.

As products previously thought unlikely to be under threat are now being exposed to attacks as they become connected to networks, allowance should be made for security education for users, as well as the planning and development of security-conscious products.

1.2 Objectives and Reader of This Document

This document has been written mainly for corporate developers working on the development of automotive on-board devices and systems. The document summarizes the guidelines relating to the design and development processes that developers should take into consideration; right through from the design to the release of automotive on-board devices, to ensure that relevant security countermeasures are performed in the devices. More specifically, this document is targeted at the following groups:

1) The designers and developers of on-board devices and systems,
2) Development supervisors in charge of the implementation of on-board devices and systems design projects,
3) Supervisors responsible for the budget and the staff allocated to on-board devices and systems design projects.

Issues that cannot be dealt with by developers alone, but that need overview by management or company-wide support, have been included for reference by company

executives. This document is designed for use in the review of the development of on-board devices and systems, and the guidelines provided should be supplemented by the “IoT Safety/Security Development Guidelines [1]”.

1.3 Abbreviations

The full names of the abbreviations used throughout this manual are as follows.

Table 2-1 List of Abbreviations

Abbreviation	Full Name
A2DP	Advanced Audio Distribution Profile
CAN	Controller Area Network
CCDS	Connected Consumer Devices Security council
CSIRT	Computer Security Incident Response Team
CVSS	Common Vulnerability Scoring System
D-Bus	Desktop Bus
DoS	Denial of Service
DSRC	Dedicated Short Range Communications
ECU	Engine Control Unit
ETC	Electronic Toll Collection system
GPS	Global Positioning System
GSM	Global System for Mobile communications
IEC	International Electrotechnical Commission
IoT	Internet of Things
IPA	Information-technology Promotion Agency, japan
ISO	International Organization for Standardization

SWG	Sub Working Group
WG	Working Group

2 A System Model for Automotive On-board Devices Guidelines

2.1 Target Model

Figure 2-1 should be referred to in the following discussion on the scope of interface connections within target automotive on-board systems. The scope of discussion focuses on connections to the head unit. The target model is discussed with references to currently available literature. In the discussion of SWG, we refer to Figure 2-2 for the automotive on-board systems.

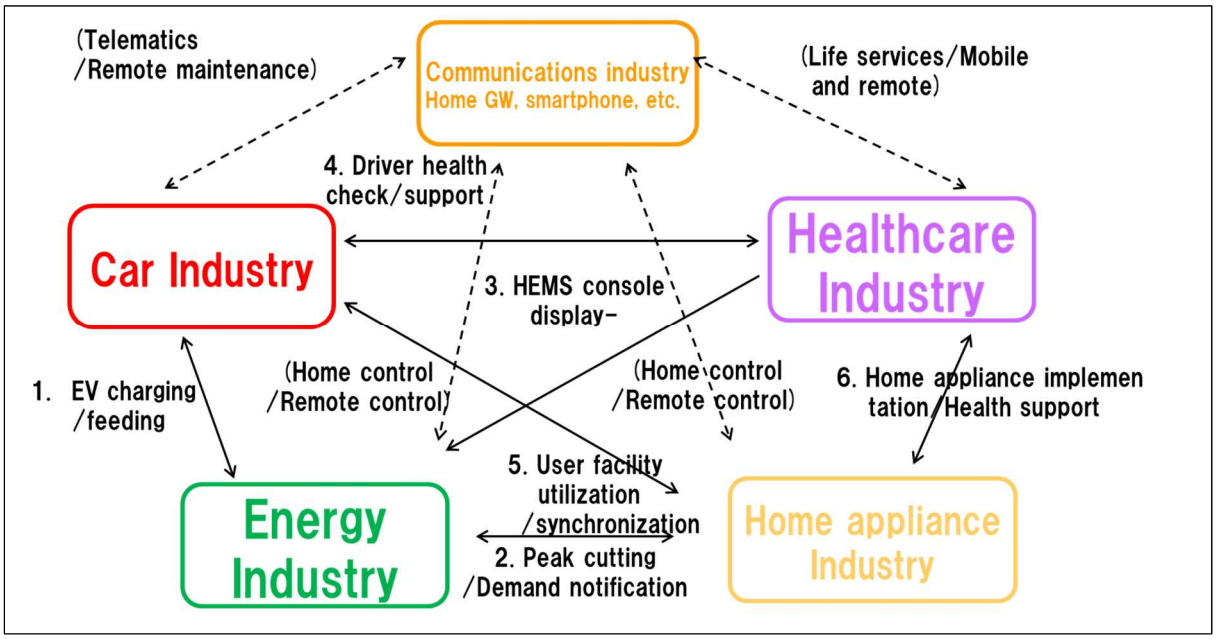


Figure 2-1 Scope of Connectivity[1]

[1] The Connected Consumer Device Security Council "現状のセキュリティ対応記入説明書"(3)

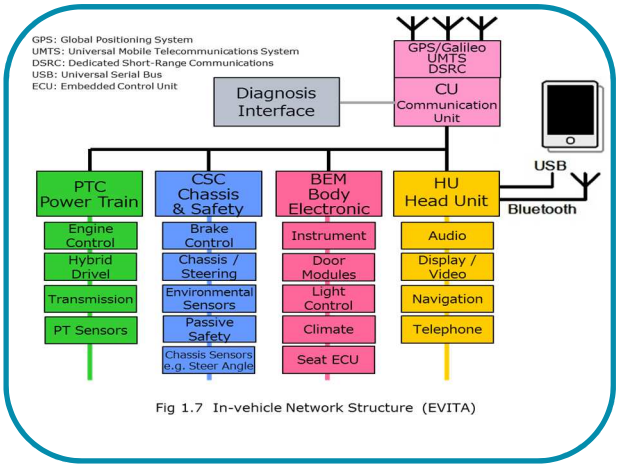
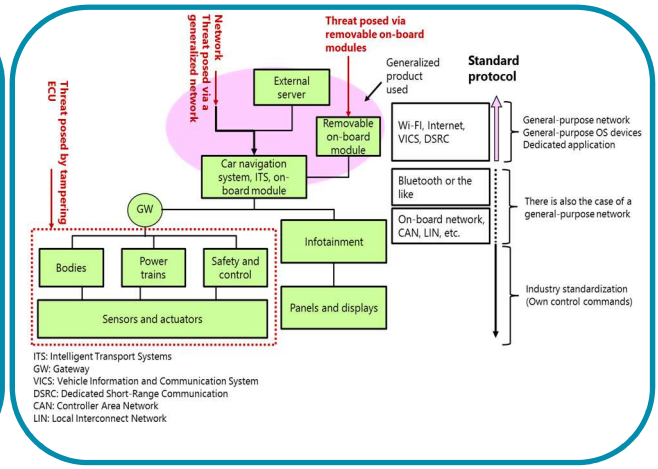


Fig 1.7 In-vehicle Network Structure (EVITA)

Source: Security Trends and Awareness Enhancement Measures Survey Report (IPA)



Source: Security Trends and Awareness Enhancement Measures Survey Report (IPA)

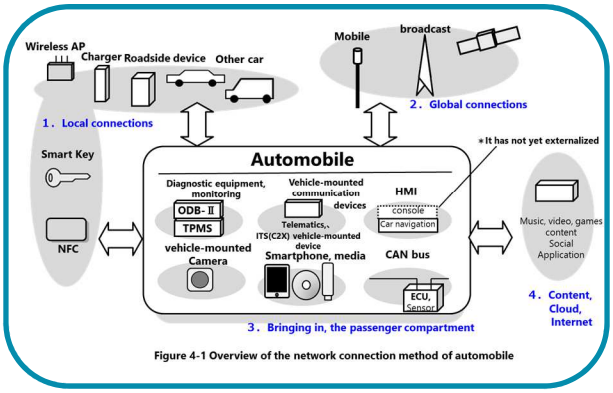


Figure 4-1 Overview of the network connection method of automobile

Source: 2011 Survey on Information Security Trends of car

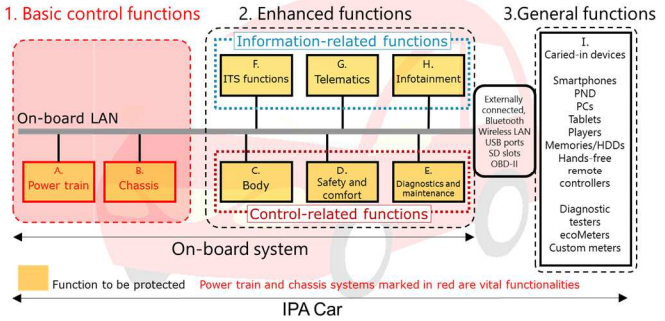
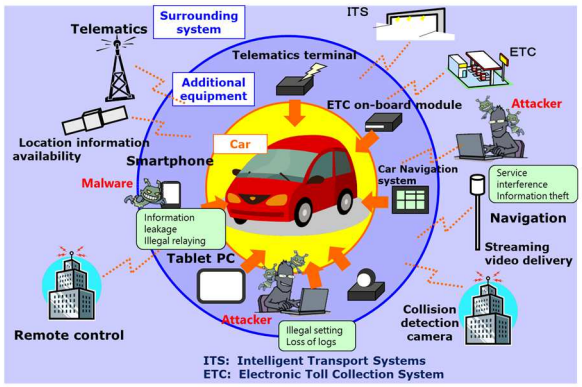
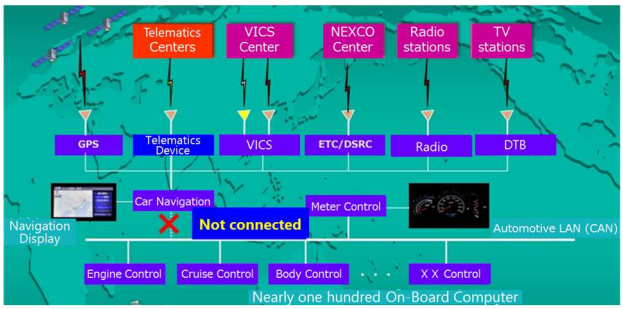


Figure : 2-2 System model of the IPA car

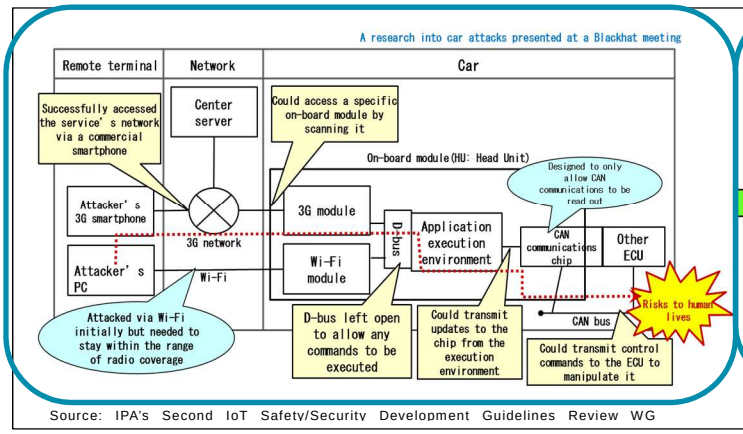
Source: Action guide to the information security of the car



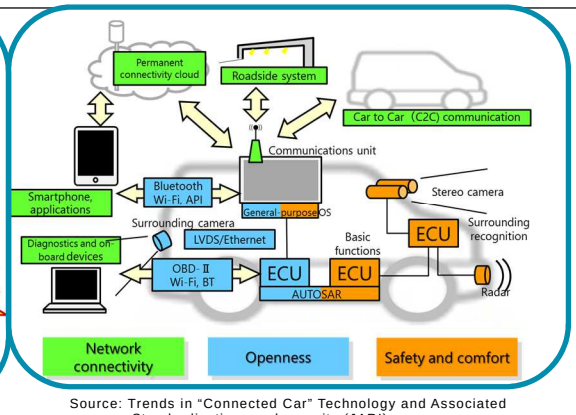
Source: Threats to Connected Built-in Systems and Countermeasures (IPA)



Source: 2020 Car Society and Security (Internet ITS Consortium)



Source: IPA's Second IoT Safety/Security Development Guidelines Review WG



Source: Trends in "Connected Car" Technology and Associated Standardizations and security (JARI)

Figure 2-2 Reference Models for Automotive On-board Systems

2.2 The System Model under Discussion

A system model is used in the discussion to aid in the task of classifying automotive functions and gaining a preliminary insight into the connection interfaces that could be utilized in attacks. The model is also useful for identifying the locations that have properties that put them under threat from attackers. Hence, devices that are either installed in the automobile or ones carried on-board that are connected through the interface to outside vehicle, as well as the on-board head unit, have been listed on the basis of the earlier discussion to work out a rough plan for the model.

Based on prior drafts, the SWG reviewed and revised them at following proper points by members:

- Adding a diagnostic port (OBD-II, On-Board Diagnostics II),
- Adding a smart key connection route,
- Adding a connection route to outside servers,
- Describing each gateway as a CAN-gateway (controller area network gateway) which does not contain security functions,
- Revising to the appropriate categorizations in the car industry that the body system, the power train chassis system and the safety system,
- Removing electrical charge system, out of our scope.

The final model is shown in Figure 2-3.

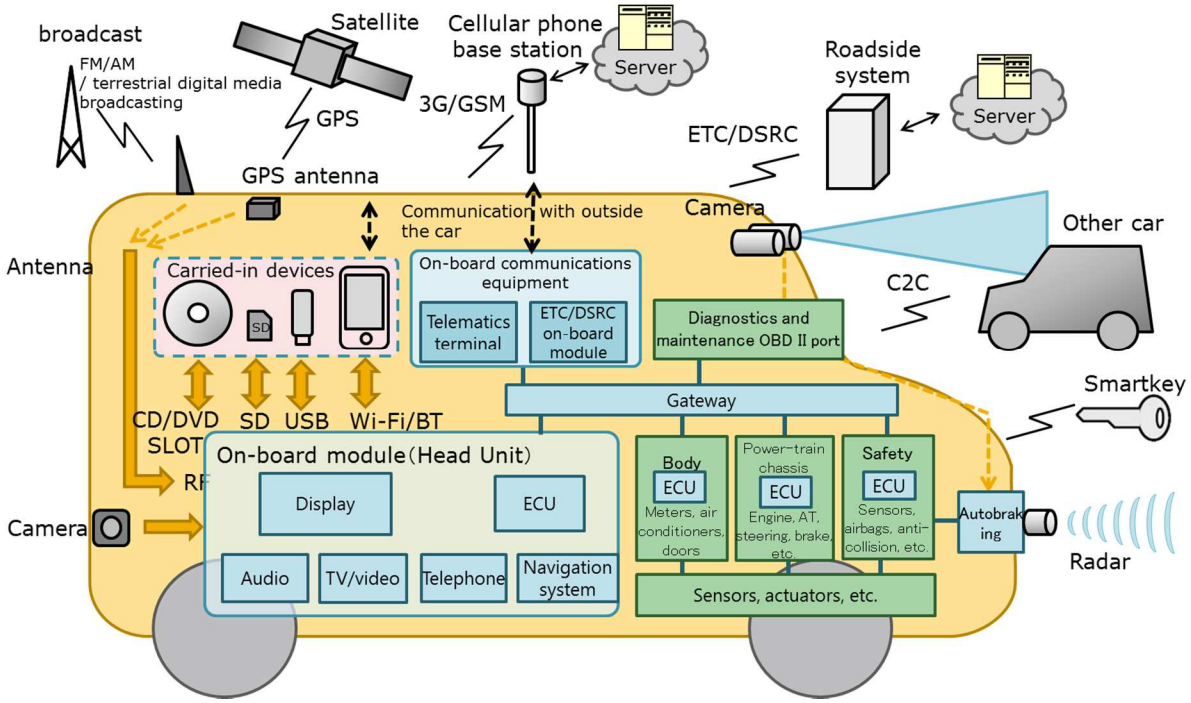


Figure 2-3 A System Model under Discussion in the Guidelines

Table 2-1 Explanations of System Component Elements

Name	Explanation
Automotive on-board device	A device that communicates with the external world by means of a gateway, such as a car navigation system, audio gear or carphone.
On-board communication device	A wireless unit installed to exchange relevant information with either a roadside system for toll payment, an ITS service, telematics communication, or vehicle-to-vehicle communication.
OBD-II port	On-Board Diagnostics, Second Generation. Onboard systems diagnostics interface.
Gateway	Enables reciprocal communication between two networks that utilize different means of communication or diverse operation policies on an automotive on-board system.
ECU	Electronic Control Unit. A unit that electronically controls a number of car mounted on-board systems.
ETC	Electronic Toll Collection System.
DSRC	Dedicated Short Range Communications. A form of wireless communications technology that enables an ITS (Intelligent Transport System) service to communicate with a roadside system or enable vehicle-to-vehicle communication.
C2C	Car-to-Car Communication.
3G/GSM	A third generation system for mobile communications/ A Global System for Mobile communications.
GPS antenna	The antenna used to receive position information from a satellite.
Carried-in on-board device	A device that carries out data communication with an automotive on-board device via either a wired, wireless or an attachment connection.
Wi-Fi	Wireless LAN standard certified by the Wi-Fi Alliance.

BT	Bluetooth. A near-field wireless communication standard designed for digital devices.
USB	Universal Serial Bus. A serial bus standard for connecting peripheral devices to information processing equipment, such as a computer.
SD	An SD card, or a memory card, that is used with mobile devices or the like.
Smart key	A car key that holds electronic data that is used to verify data with the on-board computer via wireless communication.

3 Possible Security Threats

3.1 Carry-in Devices

Carry-in Devices, such as a smartphone, USB or SD, will have more chance to be exposed to threats, for example viruses, by connecting outside resources. As it is becoming increasingly common for external devices to be connected with cars, taking countermeasures from the development stage for defending threats of any kind is extremely important.

3.2 Attacks Launched from External Networks

The use of external communication, such as smart key, GPS, vehicle-to-vehicle communications and cloud data, could assume that facing to malicious attacks of the data interception or the driving operation hack.

❒ A case of remote intrusion into an on-board LAN

A case of hacking into an automotive on-board LAN from a remote location to control steering or the engine was reported at a meeting of Black Hat 2015. This attack resulted in the recall of 1.4 million affected cars.

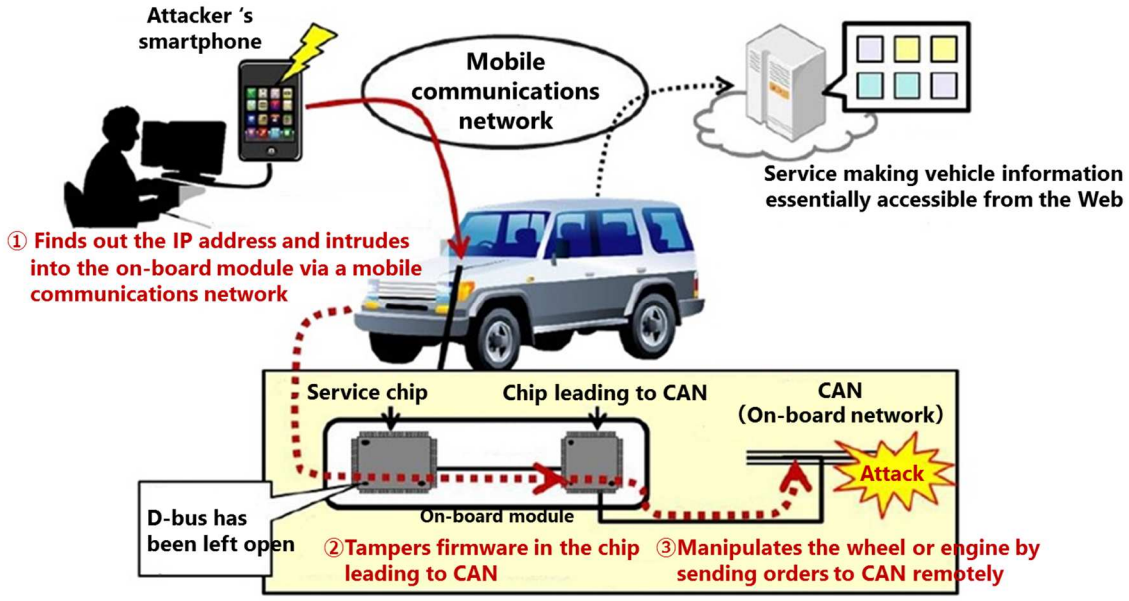


Figure 3-1 Remote Attacks Launched on Cars

3.3 Possible Threats and Damage to Automotive On-board Devices

This section describes possible threats and damages to automotive on-board devices.

Table 3-1 Possible Threats and Damages

No.	Possible threats	Possible damages
1	DoS attacks launched on the automotive on-board networks via an external network.	Shutting the all services down with communication functions.
2	Fake message transmission by server spoofing.	User confusion and more.
3	System freeze of streaming contents due to the exploiting browser bugs.	Shutdown of infotainment services.
4	Messages eavesdrop by the third party receivers.	Use of services not intended by operation management authorities.
5	Messages delivery containing incorrect locations by the third party GPS generators.	Confusion caused by the delivery of messages with the incorrect locations.
6	Spoofing of a second automotive on-board device through the use of the original automotive on-board device by users or due to the Unauthorized utilization of receivers by third parties.	Confusion caused by the delivery of drive information containing incorrect information.
7	Tracing personal locations through receiving messages by the rthird party receivers or through the user by the exploitable usage of devices.	Personal profiling.
8	Intentional shutdown of the ECU control functions through 3G/LTE by third party during normal operations.	ECU disabled from working correctly, thus crippling vehicle functions.
9	Manipulating the vehicle status through Bluetooth devices, smartphone etc., by dealer personnel during maintenance.	Tampering with settings to make unintended changes to performance.

10	Malfunctioning of the information ECU`s information functions during normal operations intentionally caused by third parties via an SD card interface.	Disabling of information functions.

4 The Lifecycle Phases and Security Efforts

The workflow of any system development activity has a lifecycle, which consists of a sequence of phases beginning with development, moving through operation, and ending in disposal. Consideration of security during each of these phases is important. This chapter provides definitions and approaches of each of these phases.

4.1 Definitions of the Lifecycle Phases

The lifecycle of an automotive system can be divided into four phases: Planning, Development, Operation and Disposal. For ensuring the product security, we need to consider the security measures in each of these phases and to perform the plan with our best efforts; as a result, these efforts affect and enhance the quality of our product security.

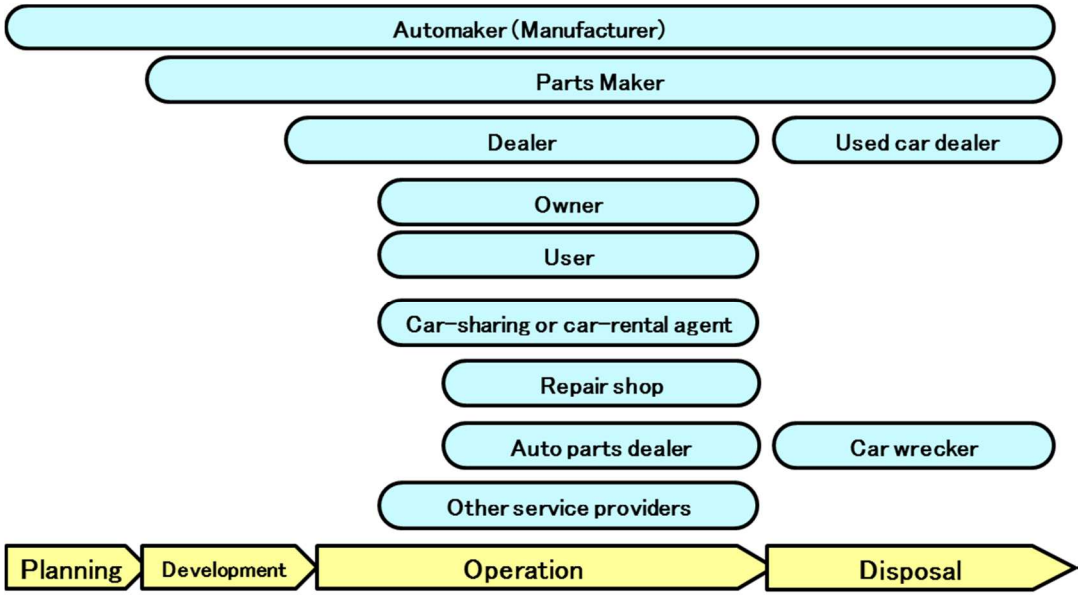


Figure 4-1 Lifecycle of an Automotive System

*See: “Automotive Information Security Efforts Guidelines (2013), IPA [7]”

Table 4-1 Definitions of Phases

Phase	Explanation
Planning	Developing car concepts and the budget required to effort them. Formulating and defining requirements.
Development	Proceeding with the design, efforts and manufacture as per the requirements and definitions formulated in the Planning Phase.
Operation	Responding to incidents that may occur after the car has been sold by the dealer to the customer (user). This includes maintaining and servicing the car, etc.
Disposal	The owner of the car either sells it as a used car or disposes it.

4.2 Security Efforts within the Individual Phases

This document summarizes guidelines for building a framework in the Planning and Development Phase of the lifecycle of an automotive system to defend any threats that may be experienced in the Operation and Disposal Phases. It describes the efforts made to ensure security that are performed in the successive phases of the lifecycle, as outlined in the previous section.

Efforts specific measures is such a costly process that developers often find it difficult to implement them alone, that is, without support from the management or the entire corporate organization. Hence, this document includes a Policy Phase, in addition to the Planning and Development, Operation and Disposal Phases, to help the management develop a key understanding of the whole lifecycle.

A list of the security effort guidelines relevant to each individual phase is provided below.

Table 4-2 List of Security Effort Guidelines Relevant to Individual Phases

Phase	No.	Item	Effort Guideline
Policy Formulation	1	Basic policies	Develop basic corporate policies.
	2	Framework	Build a corporate framework for taking action.
	3	Education	Periodically educate employees.
Planning and Development	1	Model to be assessed	Establish the range of threat analysis.
	2	Threat analysis	Conduct a threat analysis to identify risks.
	3	Measures review	Review measures.

	4	Evidence	Retain evidence.
	5	Parties concerned with design	Beware of assuming the integrity of designers, developers or subcontractors.
	6	Validation and verification	Validate and verify security.
	7	Responses to unknown threats	Prepare for the occurrence of unknown future threats of any kind.
Operation	1	User documentation	Cover all relevant aspects in the user documentation.
	2	Operation-time usage definition	Define the scope of operation-time usage in strict terms.
	3	User alert	Ensure that users identify operational faults as they occur.
	4	Update	Allow measures to also be taken in the future.
	5	Parties concerned with operations	Beware of placing complete trust in the parties concerned.
	6	Sharing incident information	Share incident information in order to use it to maximum effect.
Disposal	1	Obfuscating analyses	The design should allow for the Disposal Phase.
	2	Initialization	Allow settings to be initialized according to their defaults.

4.2.1 Policy Phase

The following is a list of the security efforts that may take place during the Policy Phases.

Table 4-3 Security Efforts Implemented in the Policy Phase

No.	Item	Guideline	Description
1	Basic policies	Establish basic corporate policies.	① Gaining cooperation from management is essential because measures are costly. (Getting the management on board is achieved via raising awareness of the importance of the issues with presentations and publications by public institutions.)
			② Update basic policies to keep up with

			developments in the threats environment.
			③ Establish guidelines to set upper limits on action taken. (This is necessary to prevent action from becoming so costly that the product cannot be launched.)
2	Framework	Maintain a framework for corporate initiatives.	① As cross-organizational approaches are envisioned according to the corporation, a supervisory manager should be appointed to oversee them.
			② Build a framework to ensure that measures run continually and cyclically.
			③It is recommended that the incident response center be set up separately from regular customer support centers.(When a problem is detected with the operation of a product in the market, and it is reported to a regular customer support center, it is usually misclassified as a product fault rather than a security issue. It is therefore recommended that a dedicated incident response center be set up to respond to security problems.)
			④ Decide how incident information received is routed and reported beforehand.
			⑤ It is recommended that a qualification system specifically intended for product security stakeholders be developed in the future.
3	Training	Periodic employee training.	① Ensure periodic retraining of employees to maintain adherence with basic policies.
			② It is recommended that training in information security be conducted in groups depending on the position of the employees. (This is because the kind of training required varies between CSIRT representatives, developers, users, managers and executives.)
			③ Training is also required to maintain employee integrity. => See ② under item 5 in 4.2.2., as well as “Planning and Development Phase”.

4.2.2 Planning and Development Phase

The following is a list of the security initiatives that shall be conducted in the Planning and Development Phase.

Table 4-4 Security Efforts Conducted in the Planning and Development Phase

No.	Item	Guideline	Description
1	Model to be assessed	Establish the scope of the threat analysis.	① Write up the target system.
			② Write up possible connection destinations.
			③ Specify connection ports.
			④ Write up all hidden interfaces.
			⑤ Make an initial listing of all possible threat candidates.
2	Threat analysis	Conduct a threat analysis to determine risks.	① Try to conduct a threat analysis using at least one method of assessment. However, the use of multiple methods is preferred, if possible, in order to compare them. (As different assessment methods have their own strengths and weaknesses, threat analyses that utilize alternative methods shall be attempted.)
			② It is desirable to have attackers` motivations and case history reflected in the risk assessment. (If any past cases are presented, exploitability subscores tend to be lower while attacker`s motivations become elevated.)
			③ Anticipate repeating the threat analyses after having worked out proposed measures in order to verify the effects of the measures. (Doing so will verify the validity and cost effectiveness of the measures.)
			④ Assess corporate risks that may be posed by incidents.
			⑤ Once a measure is put into action, the amount of properties to be protected will increase. The measure should be reimplemented to carry out threat analyses.

3	Action review	Review actions.	① List proposed measures beforehand.
			② Start by assuming that something can always be touched or opened.
			③ Decide where keys are held and who is responsible for their management.
			④ As a rule, consider the server egress as a route of intrusion. (There are cases of on-board devices being used as a springboard to launch external attacks.)
			⑤ Verify the authenticity of the devices connected and application software. (Threat analyses by the Automotive On-board Devices SWG report a high-risk score due to spoofing.)
			⑥ Explore countermeasures to defend risks posed via an informal interface.
			⑦ Consider the cost of development and efforts of countermeasures on the basis of the product value and possible risks before incorporating countermeasures into product designs.
			⑧ It is necessary for the producer of the final product to establish policies on the level of responsibility for security assurance, and letting subcontractors take their respective shares of security.
			⑨ List proposed actions that can be implemented within the individual layers (physical, network, application).
			⑩ If adequate measures cannot be taken due to constraints on the cost or specifications, also consider taking measures with the system as a whole or with upper-level components.

4	Evidence	Retain evidence.	① Discussions on documents related to the risk analysis of threats and measures, along with the effectiveness of the countermeasures taken and the reason for them being chosen. (In the case of any type of event, evidence should be retained of the scope of self-responsibility. The purpose of this is to confirm that the maximum possible effort was made, and further details could not be obtained.)
5	Parties concerned with design	Do not assume that designers, developers or subcontractors are trustworthy.	① Require submission of written pledges.
			② Stress in a training session that breaching security would ruin one`s career. (In addition to seeking compliance with secrecy obligations, training subcontractors is also beneficial.)
			③ Minimize the number of designers who have access to the entire system.
			④ Enforce strict key management. (If costs can be disregarded, use of unique keys will improve protection.)
6	Validation and verification	Validate and verify security.	① Strive to complete testing procedures with a minimum set of fuzzing tools.
			② Even though assessments are conducted in-house, it is desirable that they be subjected to a minimum of third-party checks.
			③ Risk assessment or security verification by third parties is recommended.
7	Responses to unknown threats	Be prepared for the occurrence of unknown threats of any kind.	① Write up all factors for consideration.
			② It is recommended to be constantly prepared to detect incidents of intrusion or suspicious behavior.
			③ It is recommended to be constantly prepared to take appropriate action upon detection of any abnormalities, such as the shutting down of any particular function.
			④ Retain logs to allow analysis at a later time.

4.2.3 Operation Phase

The following is a list of the security efforts that shall be conducted in the Operation Phase.

Table 4-5 Security Efforts Conducted in the Operation Phase

No.	Item	Guideline	Description
1	User documentation	Include all relevant information in the user documentation.	① Specify any disclaimers in the user documentation.
			② Ensure that products, when sold, come with relevant information about their design considerations.
2	Operation-time usage definition	Clearly define the scope of operation-time usage.	① Clearly define the scope of operation-time usage and usage assumptions and impart them to operators.
3	User alert	Ensure that users are made aware of operational faults as they occur.	① It is recommended that there be some means of alerting users to the connection of unknown devices or to the detection of any signs of suspicious behavior.
			② It is recommended that products found to contain configuration errors are not used without those errors first being corrected. (Ensure that security has under no circumstances been disabled due to configuration errors committed by users, dealers or anyone else.)
4	Updates	Allow measures to also be taken at a later time.	① Establish a framework for secure firmware updating. (Firmware should ideally be downloaded from a dependable server with a secure boot key.)
			② Establishing a framework for remote updating is also recommended.
5	Parties concerned with operations	Never place complete trust in the parties concerned.	① Ensure that no harm would be caused by the leakage of maintenance documentation.
			② Be prepared for possible threats from malevolent parties during operations.
6	Sharing of	Share incident	① It is essential to set up a system of

	incident information	information and put it to effective use.	sharing and utilizing available incident information in-house or among stakeholders.

4.2.4 Disposal Phase

The following is a list of the security efforts that shall be conducted in the Disposal Phase.

Table 4-6 Security Efforts Conducted in the Disposal Phase

No.	Item	Guideline	Description
1	Obfuscating analyses	Designs should allow for the Disposal phase.	① It is recommended that boards be designed so they cannot be easily reverse-engineered after being disposed. ② Designs should be resistant to reverse engineering. (One method is to seek authentication every time a request is connected.)
			③ It is also recommended that software be designed to avoid facilitating reverse engineering.
2	Initialization	Allow settings to be initialized according to their defaults.	① Allow settings to be reset to their defaults.

5 Threat Analyses

5.1 Threat Cases

Literature relating to the cases of automotive threats under preliminary discussion at the Automotive On-board Devices SWG was utilized in the compilation of threat analyses. At the Automotive On-board Devices SWG, about 230 cases of known incidents had been classified by risk characteristics, such as “Target Equipment”. “Field-specific and Common”. “Threat Classification” and “Connection Interface (Intrusion Route) ”, to assess risk scores on the basis of predefined assessment items of exploitability, damage and impact subscores. Table 5-1 lists the literature that has been surveyed by the Automotive On-board Devices SWG with regard to the incident cases.

Table 5-1 Surveyed Literature List

No.	Literature surveyed	URL
1	Fiscal 2010 Automotive Information Security Trend Survey Report, IPA	http: //www.ipa.go.jp/files/000014119.pdf
2	Fiscal 2011 Automotive Information Security Trend Survey, IPA	https: //www.ipa.go.jp/files/000024414.pdf
3	Appendix to the Fiscal 2011 Automotive Information Security Trend Survey, IPA	http: //www.ipa.go.jp/files/000014165.pdf
4	Fiscal 2012 Automotive Information Security Trend Survey, IPA	https: //www.ipa.go.jp/files/000027274.pdf
5	Security requirements for automotive on-board networks based on dark-side scenarios, EVITA	http: //evita-project.org/Deliverables/EVITAD2.3.pdf
6	Automotive Information Security Analysis Guide_JASO TP15002, Society of Automotive Engineers of Japan	http: //www.bookpark.ne.jp/cm/jsae/particulars.asp?content_id= JSAE-tp-15002-PDF
7	Driving Support Communication System Security Guidelines, ITS Forum	http: //www.itsforum.gr.jp/Public/J7Database/p41/ITS_FORUM_RC009V1_0.pdf
8	Survey Report Concerning Automotive Security Trends at Home and Abroad and Measures to Enhance Security Awareness, IPA	https: //www.ipa.go.jp/files/000014059.pdf

9	Automotive and Intelligent Home Appliance Built-in Systems Security Survey, IPA	http: //www.ipa.go.jp/files/000013971.pdf
10	Future and Issues of Automotive Networking - Connected Car Security, IPA	http: //home.jeita.or.jp/page_file/20141009110119_FYXUHuv50O.pdf
11	Automotive Information Security Efforts Guidelines, IPA	https: //www.ipa.go.jp/files/000027273.pdf
12	Present Status of Automotive On-board Network Security, FFRI	http: //www.ffri.jp/properties/files/monthly_research/MR201310_Current%20state%20of%20automotive%20network%20security_JPN.pdf
13	Proposals Concerning Tougher Information Security in Built-in Automotive On-board Systems, IPA	https: //www.ipa.go.jp/files/000034668.pdf

5.2 Risk Characteristics

As part of the compilation of threat analyses using the incident cases that had been collected at the Automotive On-board Devices SWG, the items of risk characteristics were reviewed. In addition to the four items of classification such as “target equipment”, “field-specific and common”, “threat classification” and connection Interface (intrusion route)” originally used at the Automotive On-board Devices SWG, three additional items that had been used at the IPA`s IoT Safety/Security Development Guidelines Review WG for classifying risk characteristics – Who : Connected, Whom : Threats Did Harm To, Where : Risks Occurred – have been added. Table 5-2 provides a full list of risk characteristics.

Table 5-2 Risk Characteristics

No.	Item	Description
1	Target Equipment	Equipment exposed to threats.
2	Field-specific and Common	See Table 5-3 Field-specific and Common”.
3	Threat Classification	List cases as per Table 5-4 Threat Classifications”. Classification criteria are as follows. ① Threats resulting from user action.

		=> “Configuration error/Virus infection”. ② Threats launched by attackers with the express intention of attacking. => “Eavesdropping/DoS attack/Fake messaging/Illegal relaying”. ③ The means used by attackers for launching attacks is unknown or does not apply to the above but the following damage has been incurred. => “Illegal setting/information leakage/log loss”. If none of above applies to threats, classify as “Unauthorized utilization”.
4	Connection Interface (Intrusion route)	See Table 5-5 Connection Interface (Intrusion Route) ”.
5	Who : connected	See Table 5-6 Who : Connected”.
6	Whom : threats did harm to	See Table 5-7 Whom : Threats Did Harm To”.
7	Where : risks occurred	See Table 5-8 Where : Risks Occurred”.

■ **Field-specific and common cases**

Those cases that are dedicated to the automobile field relevant to the present development activity have been categorized as being field-specific with a view to generalizing tools. These work not only with automotive on-board devices, but also with the important life apparatuses to be covered by CCDS in the future. Those cases that relate to the automotive field, but that could occur with IoT devices as well, are categorized as being common.

Table 5-3 summarizes criteria for distinguishing between field-specific and common cases, along with criteria to consult when a threat fits to neither a field-specific nor a common case.

Table 5-3 Field-specific and Common Cases

Category	Explanation
Field-specific	Cases in which any equipment or intrusion routes unique to on-board devices appear to be involved are categorized as being field-specific, e.g., the target is a CAN or ECU, or a DSRC or OBD is involved in the intrusion route.

Common	Cases in which the target is an on-board device, but attacks launched on it are considered general (such as phishing or a DoS attack), are categorized as being common.

■ **Threat Classifications**

Table 5-4 lists the cases of classifications of threats caused by user action and threats caused by attackers` intervention.

Table 5-4 Threat Classifications

Threat	Q
Configuration error	A threat that is induced by an invalid action or setting made by the user via the automotive user interface. ・For example, personal information is sent to an unintended service provider by an infotainment function, or transmitted information is eavesdropped as the encryption function for a telematics service has been turned off.
Virus infection	A threat that is induced by the infection of the automotive on-board system by a virus or item of malicious software (malware, etc.) via a device or storage media introduced by the user from the external world. ・For example, a virus penetrating a infotainment device has infected an automotive on-board device via an on-board LAN.
Unauthorized utilization	A threat that enables unauthorized individuals to take advantage of the functions of an automotive system by spoofing or exploiting device vulnerabilities. ・For example, a session of unlocking communication has been spoofed to unlock a car illegally.
Illegal setting	A threat that enables unauthorized individuals to tamper with the settings of an automotive system by spoofing or exploiting device vulnerabilities. ・For example, network settings have been tampered with inhibiting successful communication.
Information leakage	A threat of any information to be protected on an automotive system being made available to unauthorized individuals. ・Stored contents or user information of services are illegally stolen due to intrusion into the equipment or the intercepting of communications.
Eavesdropping	A threat of communication between automotive on-board devices or between a car and a peripheral system being stolen or seized. ・For example, status information (such as the speed of the car and

	information about its position) has been eavesdropped while it is being transferred from the car to a surrounding system as a part of the navigation or the congestion prediction services.
DoS attack	A threat that causes a system to close down or impede a service as a result of invalid or excessive requests for connection. ・For example, excessive communications are directed at a smart key to disable user requests (locking or unlocking).
Fake messaging	A threat that causes an automotive system to perform invalid operations or produce invalid displays by attackers sending spoofing messages to it. ・For example, a TPMS (Tire Pressure Monitoring System) message has been faked to turn on a ca warning lamp when an error does not actually exist.
Log loss	A threat that erases or falsifies an operation log or the like so it cannot be viewed later. ・An example is when an attacker falsifies a log of an attack action committed by the attacker himself or herself in order to destroy evidence of that attack.
Illegal relaying	A threat that manipulates a path of communication or takes over normal communication or uses invalid communication to tamper with it. ・For example, smart key signals are relayed illegally, so that attackers can unlock the car from a remote location.

*See: “Automotive Information Security Efforts Guidelines (2013), IPA [7]”

■ **Connection Interface (Intrusion routes)**

Table 5-1 shows the possible routes of threat intrusion.

Table 5-5 Connection Interface (Intrusion Route)

Connection Interface	Transmission distance	Explanation
3G/GSM	(In network service)	Communications method for digital cellular telephones.
Bluetooth	0 to 10m	A near-range wireless communication standard used by portable information devices for communicating between devices only several meters apart.
CD	0m	One of the optic disc standards for recording digital information.
DSRC	0 to 30m	Wireless communication between a roadside system and

		the automotive on-board devices installed in a driving car. Used by ITS.
eCall service interface	(In network service)	European automatic vehicle emergency notification system.
GPS	Within the range of reception	Global Positioning System. A system that precisely locates where on the Earth you are now with the aid of artificial satellites.
OBD	0m	On-Board Diagnostics implemented by the computer (ECU) mounted aboard an automobile.
RF	0 to 10m	Wireless communication for smart keys or on-board communication.
SD	0m	A kind of memory card.
USB	0m	Universal Serial Bus, or a serial bus standard for connecting peripherals to an information device, such as a car navigation system.
VICS	Within the range of reception	Vehicle Information and Communication System. A system that provides road traffic information, such as congestions and traffic controls, by either FM multiplex broadcasts or radio beacons.
Wi-Fi	0 to 50m	Technology for connecting network-ready devices wirelessly.
Sensor	0m	On-board sensor.
Special tools	0m	An immobilizer cutter, dedicated maintenance tool or the like.

■ **Who : Connected**

Table 5-6 summarizes information about who is connected according to the method of sorting risk characteristics discussed at IPA`s IoT Safety/Security Development Guidelines Review WG.

Table 5-6 Who : Connected

Threat	Explanation
Manufacturer or associated company	A connection envisioned by the manufacturer at the time of design.
Service provider	A connection not envisioned by the manufacturer at the time of design.

User (intentional)	An intentional connection made by the user.
User (wrong connection)	An incorrect connection made by the user.
Attacker	A connection made by exploiting vulnerabilities.
Accidental	An accidental connection that happens to be established when a number of connections are in place.

*See: “IoT Safety/Security Development Guidelines [1]”.

■ **Whom : Threats Did Harm To**

Table 5-7 summarizes information about whom did threats harm according to the method of sorting risk characteristics discussed at IPA`s IoT Safety/Security Development Guidelines Review WG.

Table 5-7 Whom : Threats Did Harm To

Threat	Explanation
IoT functions (communication, linkage, concentration and more)	IoT applications, communication functions, security functions, etc.
Inherent functions (e.g., server, GW, thing)	An inherent function of a device or system, or a function intended for safety assurance.
Information	Personal information, payment information, sensor data, etc.
Bodies and properties	Users` bodies, properties and more.
Others	Commodities kept in a vending machine, cash in an ATM, their bodies components, etc.

*See: “IoT Safety/Security Development Guidelines [1]”

■ **Where : Risks Occurred**

Table 5-8 shows where risk sources are located, according to the method of sorting risk characteristics under discussion by “IoT Safety/Security Development Guidelines [1]” Review WG.

Table 5-8 Where : Risks Occurred

Threat	Explanation
Ordinary-use Interface	A user operation panel, service wired/wires interface, USB terminal or the like.

Maintenance Interface	A management operation panel, remote management communications Interface, software update USB terminal or the like.
Informal Interface	An unused port left open, USB terminal used only during manufacture or the like.
Internally contained risk	Examples include a defect or bug that could be a source of a failure, a vulnerability that could be exploited, a function that could do harm when it fails or is Unauthorized utilizationd etc.
Physical contact	Direct contact with the body.

*See: “IoT Safety/Security Development Guidelines [1]”.

6 Methods of Risk Assessment

Prior to the risk assessment of threat cases, the available methods of on-board disk assessment for automotive on-board devices were explored on the basis of automotive reference literature.

6.1 Modified ETSI Method

According to the ETSI (European Telecommunications Standard Institute), threats are classified by likelihood and impact, and are assessed on a scale of three ranks for each of these two characteristics. Each of these ranks is assigned a score, and the resultant two scores are multiplied together to arrive at a risk score [3]. Table 6-1 lists ETSI definitions of likelihood and impact, while Table 6-2 lists definitions of risk score classifications.

Table 6-1 ETSI Likelihood and Impact Definitions

Item	Score	Rank	Definition
Likelihood	3	Likely	Not fully prepared against threats, with attackers being highly motivated.
	2	Possible	Attackers do not require advanced skills or much effort to launch attacks, only justifiable motivations.
	1	Unlikely	Attacks are difficult to launch even with the latest knowledge, meaning that attackers` motivation is low.
Impact	3	High impact	Business is seriously damaged.
	2	Medium impact	There is a significant impact.
	1	Low impact	The chances of damage occurring are low.

Table 6-2 ETSI Risk Score Calculations

Item	Score (product)	Rank	Definition
Risk score	6,9	Critical	Serious risks could occur that require action of the highest priority.
	4	Major	Major risks could occur, even though they do have a critical impact.
	1,2,3	Minor	Minor risks may occur, but won`t necessitate action.

Since the wisdom of allowing for exploitability (the presence or absence of precedents) and attackers` motivations, as well as likelihood and impact scores, in the risk assessment process was suggested at the Automotive On-board Devices SWG, available literature concerning the methodology of risk assessment relevant to automotive on-board devices was examined. As a result of this examination, the modified assessment method publicized by the European Telecommunications Standard Institute (ETSI) was chosen as a reference [4], [5].

This assessment method analyzes the likelihood in terms of motivation and technical difficulty for assessment purposes. Table 6-3 shows definitions of motivation and technical difficulty. The modified method also works out likelihood ranks in terms of motivation and technical difficulty. Likelihood and impact definitions are given together in Table 6-4.

Table 6-3 Motivation and Technical Difficulty Definitions in the Modified ETSI Method

Item	Rank	Definition
Motivation	High	Highly profitable (in terms of gain) for attacking individuals or organizations.
	Moderate	Service confusion (e.g. offender is motivated by pleasure).
	Low	Not very profitable.
Technical difficulty	None	Attacks technically and economically easy to launch (antecedents available).
	Solvable	Attacks theoretically possible.
	Strong	Attacks extremely difficult to launch theoretically, technically or economically.

Table 6-4 Likelihood and Impact Definitions in the Modified ETSI Method

Item	Rank	Value	Definition
Likelihood	Likely	3	All elements exist.
	Possible	2	Some elements exist.
	Unlikely	1	Essential elements are missing.
Impact	High	3	Users and services are seriously affected.
	Medium	2	Services shut down for a short period of time.
	Low	1	Users and services are affected.

As with ETSI, risk scores are classified on the basis of the multiplication of likelihood and

impact. Table 6-5 shows definitions of risk score classifications.

Table 6-5 Risk Score Classifications in the Modified ETSI Method

Item	Score (product)	Rank	Definition
Risk score	9,6	Critical	Action mandatory.
	4	Major	Caution required.
	3,2,1	Minor	Immediate action not required.

Table 6-6 shows the classifications of risk scores, in a matrix form, based on the relationships between the scores of motivation, technical difficulty and likelihood, as well as the impact scores.

Use of the modified ETSI method is expected to allow risk assessment with attackers` motivations being taken into consideration.

Table 6-6 Risk Score Definitions in the Modified ETSI Method

<table>
<tr><th rowspan="2">Motivation</th><th rowspan="2">Technical Difficulty</th><th rowspan="2">Likelihood</th><th colspan="3">Impact</th></tr>
<tr><th>High (3)</th><th>Medium (2)</th><th>Low (1)</th></tr>
<tr><td rowspan="2">High</td><td>None</td><td rowspan="2">Likely (3)</td><td rowspan="3">Critical (9,6)</td><td rowspan="3"></td><td rowspan="4">Minor (3,2,1)</td></tr>
<tr><td>Solvable</td></tr>
<tr><td rowspan="2">Moderate</td><td>None</td></tr>
<tr><td>Solvable</td><td>Possible (2)</td><td>Major (4)</td></tr>
<tr><td>Low</td><td>Any</td><td rowspan="2">Unlikely (1)</td><td colspan="3" rowspan="2"></td></tr>
<tr><td>Any</td><td>Strong</td></tr>
</table>

6.2 CRSS Method (Applied CVSS Method) [6]

The CVSS-based Risk Scoring System (CRSS) is a scheme of risk scoring that builds on the Common Vulnerability Scoring System (CVSS), which is a scheme of risk scoring with proven success in the assessment of vulnerabilities in information devices and systems.

While CVSS has been formulated by Forum of Incident Response and Security Teams (FIRST) and is in widespread use as a scheme of assessing information system vulnerabilities, it does not consider impacts severe enough to affect human bodies, such as those of threats to an automotive on-board system. CRSS, on the other hand,

addresses the task of risk scoring for automotive on-board systems by classifying those impact parameters that are partial, and therefore minor, as well as those that are full-scale, and therefore severe.

Among the three assessment criteria considered, CVSS uses base scores for risk assessment. Table 6-7 shows the parameters of base metrics used by CRSS. By using these parameters of base metrics, the impact and exploitability subscores are determined by solving the equations given below and then risk scores are classified by the resultant base scores. Table 6-8 shows definitions of the risk score classifications.

- Impact subscore = 10.41×(1-(1-C)×(1-I)×(1-A))
- Exploitability subscore = 20×AV×AC×Au
- f (Impact subscore) = 0 (impact subscore 0), 1.176 (impact subscore other than 0)

Base score = ((0.6 × impact subscore) + (0.4 × exploitability subscore)-1.5) × f (impact subscore)

Table 6-7 Base Metrics

Parameter	Outline	Category	Score
AV: Access Vector	Assesses from where a vulnerable system can be attacked.	Local	0.395
		Adjacent	0.646
		Network	1.0
AC: Access Complexity	Assesses the complexity of the conditions prerequisite to attacking a vulnerable system.	High	0.35
		Medium	0.61
		Low	0.71
Au: Authentication	Assesses the need to seek authentication from the target system to exploit its vulnerabilities.	Multiple	0.45
		Single	0.56
		No need	0.704
C: Confidentiality Impact	Assesses the possibility of any confidential information stored in the target system leaking when its vulnerabilities are exploited.	None	0.0
		Minor	0.275
		Severe	0.660
I: Integrity Impact	Assesses the possibility of any information stored in the target system being falsified when its vulnerabilities are exploited.	None	0.0
		Minor	0.275
		Severe	0.660

A: Availability Impact	Assesses the possibility of any functionalities of the target system being delayed or shut down when its vulnerabilities are exploited.	None	0.0
		Minor	0.275
		Severe	0.660

Table 6-8 Risk Score Classifications

Threat level	Risk score (base score)
Level (serious)	7.0 to 10.0
Level II (warning)	4.0 to 6.9
Level III (caution)	0.0 to 3.9

6.3 RSMA Method [6]

RSMA (Risk Scoring Methodology for Automotive system) is the method whereby risk scores are evaluated from a table of risk level assessments by impact subscore and likelihood. Impact subscores are grouped into one of three damage classifications – safety, personal information/privacy and property/corporate value. Further, the likelihood is assessed at one of three levels, high, medium and low, pursuant to a likelihood assessment table on the basis of the five parameters – duration, specialized knowledge, TOE knowledge, opportunity and devices. These are summarized in Table 6-9 and Table 6-10. Risk scores are evaluated in a matrix of impact subscores and likelihoods. The evaluation table is given in Table 6-11.

Table 6-9 Likelihood Parameters

Parameter	Explanation	Criteria	
Duration	Time needed to identify and then exploit vulnerabilities.	Realistic.	0
		Non-realistic.	19
Specialized knowledge	Technical specialized knowledge required.	Amateurs.	0
		Professionals.	3
TOE knowledge	Knowledge limited to attacked objects (TOE).	Publicized information.	0
		Information available to dealers, developers and manufacturers.	3

		Information available only to limited sets of users.	7
Opportunity	Time and frequency of access to attacked objects (TOE).	Access not required. Access required/unlimited access.	0
		Access required/limited frequencies.	4
		Access required/Inaccessible.	19
Devices	Hardware and software used to launch attacks.	Commercial products (commercial hardware, software and other products).	0
		Special devices (such as dealer-owned products).	4
		Custom devices (such as products dedicated to development work).	8

Table 6-10 Likelihood Level Assessment Table

Likelihood level	Value
High	0 to 14
Medium	15 to 24
Low	25 or more

Table 6-11 Risk Level Assessment Table

Damage classification	Impact subscore	Description	Likelihood		
			Low	Medium	High
Safety	None	No human impact.	0	0	0
	Low	Minor.	L	L	M
	Medium	Serious.	L	M	H
	High	Life threatening.	M	H	H
Personal information/privacy	None	No personal information/privacy.	0	0	0
	Low	Information that does not lead to individual identification alone.	L	L	M
	High	Information that helps identify individuals.	M	M	H
Property/corporate value	None	No impact on properties/corporate values.	0	0	0
	Low	Limited to impact in-house only (low business impact).	L	L	M
	Medium	Impacting customers (medium	L	M	H

		business impact).			
	High	Impacting both customers and business (high business impact).	M	H	H

6.4 CCDS Prototype Method

The Automotive On-board Devices SWG uses a method whereby risk scores are ranked on the basis of attack exploitability and user impact subscores. This method uses exploitability and impact subscores as basic axes with a view to expediting assessment and development in the initial stages with reference to the information found in the “Common Vulnerability Scoring System CVSS Overview”.

Exploitability subscores are broken down into four ranks, S, A, B and C, S being the lowest level of exploitability and C being the highest. Rank C is assigned 10 points. The higher a threat level is, the higher its assigned score. A large score difference of 5 points is allowed between a threat having no security in place and one having at least one security feature in place, with 2 points allowed between all other threats. Consequently, the four ranks are assigned 10, 5, 3 and 1 points, respectively.

Impact subscores are broken down into four levels – minor, medium, serious and destructive. The destructive level is assigned 10 points and other levels are evaluated accordingly. Attack exploitability and impact subscore definitions and scores are listed in Table 6-12 below.

Table 6-12 Scores of Attack Exploitability and Impact Subscores

Item	Item definition	Rank	Rank definition	Value
Exploitability subscore	Are there any conditions necessary to launch attacks (such as authentication or special privileges)?	S	Multiple conditions (authentication, special privileges and so forth) are required, and only local connections (attacks) are possible.	1
		A	A single condition (authentication, special privilege or the like) is required, and only connections (attacks) are possible.	3
		B	One or more conditions (authentication, special privilege and so forth) are required, or only local connections (attacks) are	5

			possible.	
		C	No need for conditions for launching attacks, and connectable (attacks possible) from a wireless network.	10
Impact sub score	What are the impact subscores and ranges of attacks and secondary damage?	Minor	Attacks launched will leave no impact on users or only produce a minor display error. Furthermore, there is no leak of information that will help identify individuals.	1
		Medium	Attacks launched will put users at a disadvantage or allow an individual to be identified from leaked information.	3
		Serious	Attacks launched will not only put users at a disadvantage, but also produce secondary damage or allow multiple individuals to be identified from leaked information.	5
		Destructive	Attacks launched will produce damage with either fatal consequence or secondary damage.	10

The Automotive On-board Devices SWG decided to take attackers` motivations into account when conducting risk assessments, because higher attackers` motivations tended to give higher threat risk levels. Attackers` motivations were assessed at one of three levels, low, medium, and high, on the basis of the CCDS method. The medium level was set to give a 1.25 times higher risk score, and the high level, a 1.5 times higher risk score. Risk scores are calculated by the following equation.

Risk score= (Exploitability subscore + Impact subscore) × Attackers` motivation

Table 6-13 summarizes attackers` motivations, with definitions of the risk scores listed in Table 6-14.

Table 6-13 Definitions of Attackers` Motivations

Item	Rank	Definition	Value
Attackers` motivation	Low	Threats occur accidentally, with attackers having no particular intention at all.	1
	Medium	Attackers seek experimentation, amusement, exhibitionism or other objectives.	1.25
	High	Attackers have stronger incentives, such as gaining monetary profits or impacting security.	1.5

Table 6-14 Risk Score Classifications

Risk score	Criterion
Low	Less than 8
Middle	8 or more but less than 12
^	12 or more but less than 17
Essential	17 or more

7 Results of Risk Assessment

7.1 Modified ETSI Method

As the modified ETSI method calculates risk scores on the basis of the product of multiplication of likelihood and impact, the risk scores are discrete. Furthermore, since only a score of 4 will produce a “major” result, the modified ETSI method is more liable to produce results in the “critical” (red) and “minor” (yellow) bands than the other methods. Table 7-1 summarizes some examples of risk assessments produced by the modified ETSI method.

Table 7-1 Examples of Risk Assessments Produced by the Modified ETSI Method

No	Possible threats	Possible damages	Target devices	Field-specific or common	Threat classification	Connection Interface	Who: Connected	Whom: Threats Did Harm To	Where: Risks Occurred	Modified ETSI method				
										Motivation	Technical difficulty	Likelihood	Impact	Risk score
1	DoS attacks launched on an automotive on-board network via an external network	Shutdown of all services that require communication functions	Automotive on-board devices	Common	DoS Attack	3G/ GSM	Attacker	IoT functions	Ordinary-use Interface	Moderate	Solvable	2	3	6
2	Transmission of fake messages by server spoofing	User confusion and more	Automotive on-board devices	Common	Fake messaging	3G/ GSM	User (wrong connection)	IoT functions	Ordinary-use Interface	Moderate	Solvable	2	2	4
3	Freezing of systems due to streaming content exploiting browser bugs	Shutdown of infotainment services	Automotive on-board devices	Common	Fake messaging	3G/ GSM	User (intentional)	IoT functions	Ordinary-use Interface	Moderate	Solvable	2	2	4
4	Eavesdropping of communication messages by taking advantage of third parties` receivers	Use of services not intended by the operation management authorities	Automotive on-board devices	Common	Eavesdropping	Wi-Fi	Attacker	Information	Ordinary-use Interface	High	Solvable	3	1	3
5	Delivery of messages containing incorrect locations through the Unauthorized utilization of GPS generators by third parties	Confusion caused by the delivery of messages containing incorrect locations	Automotive on-board devices	Common	Illegal relaying	GPS	Attacker	Inherent functions	Ordinary-use Interface	Moderate	Solvable	2	2	4
6	Spoofing of a second automotive on-board device through the use of the original automotive on-board device by users or the Unauthorized utilization of receivers by third parties	Confusion caused by the delivery of drive information containing incorrect information	Automotive on-board devices	Common	Unauthorized utilization	3G/ GSM	User (intentional)	Information	Ordinary-use Interface	Moderate	Solvable	2	2	4
7	Tracing to personal locations from received messages through the use of receivers by third parties or the Unauthorized utilization of an	Personal profiling	Automotive on-board devices	Field-specific	Information Leakage	Wi-Fi	Attacker	Information	Ordinary-use Interface	High	Solvable	3	1	3

	automotive on-board device by users													
8	Intentional shutdown of the control ECU`s control functions from 3G/LTE lines by third parties during normal operations	ECU disabled from working correctly, crippling the vehicle functions	ECU	Field-specific	Unauthorized utilization	3G/ GSM	Attacker	Inherent functions	Ordinary-use Interface	Moderate	Solvable	2	3	6
9	Dealers' personnel falsify vehicle status information from Bluetooth devices, such as a smartphone, during maintenance.	Tampering with settings to make unintended changes to performance	Automotive on-board devices	Field-specific	Illegal setting	Bluetooth	Service provider	Information	Ordinary-use Interface	Moderate	Solvable	2	2	4
10	Malfunctioning of the information in the ECU`s information functions intentionally induced by third parties from an SD card interface during normal operations	Information functions prevented from working correctly	ECU	Field-specific	Unauthorized utilization	SD	Attacker	Inherent functions	Ordinary-use Interface	Moderate	None	3	1	3

Critical (6,9)
Major (4)
Minor (3, 2, 1)

7.2 CRSS Method (Applied CVSS Method)

The CRSS method changes the impact subscore parameter categories from “partial” to “total” and from “total” to “severe”. which better reflects risk assessment solutions for automotive on-board systems than the original CVSS method. For this reason, the impacts on information processing and vehicle control are categorized as being “minor” and “severe” respectively, so that impact subscores tend to appear lower than those produced by other method. Consequently, there are fewer serious risk score levels (red). Furthermore, when assessed by the CRS method, the same threat case could characteristically deliver different risk scores depending on the attack route taken (3G/GSM, Wi-Fi and so forth). Table 7-2 summarizes examples of risk assessments produced by the CRSS method.

Table 7-2 Examples of Risk Assessments Produced by the CRSS Method

No	Possible threats	Possible damages	Target devices	Field-specific and common	Threat classification	Connection Interface	Who : Connected	Whom : Threats Did Harm To	Where : Risks Occurred	CRSS (CVSS-based)								
										AV Access Vector	AC Access Complexity	Au Authentication	Exploitability subscore	C Confidentiality Impact	I Integrity Impact	A Availability Impact	Impact subscore	Risk score
1	DoS attacks launched on an automotive on-board network via an external	Shutdown of all services that require communication functions	Automotive on-board devices	Common	DoS Attack	3G/ GSM	Attacker	IoT functions	Ordinary-use Interface	Network	Low	Single	7.95	None	Minor	Minor	4.94	5.46

	network																	
2	Transmission of fake messages by server spoofing	User confusion and more	Automotive on-board devices	Common	Fake messaging	3G/GSM	User (wrong connection)	IoT functions	Ordinary-use Interface	Network	Low	Single	7.95	None	Minor	Minor	4.94	5.46
3	Freezing of systems due to streaming content exploiting browser bugs	Shutdown of infotainment services	Automotive on-board devices	Common	Fake messaging	3G/GSM	User (intentional)	IoT functions	Ordinary-use Interface	Network	Low	Single	7.95	None	Minor	Minor	4.94	5.46
4	Eavesdropping of communication messages by taking advantage of third parties` receivers	Use of services not intended by the operation management authorities	Automotive on-board devices	Common	Eavesdropping	Wi-Fi	Attacker	Information	Ordinary-use Interface	Adjacent	Medium	Multiple	3.55	Minor	None	None	2.86	1.92
5	Delivery of messages containing incorrect locations through the Unauthorized utilization of GPS generators by third parties	Confusion caused by the delivery of messages containing incorrect locations	Automotive on-board devices	Common	Illegal relaying	GPS	Attacker	Inherent functions	Ordinary-use Interface	Network	Low	None	10.00	None	Minor	Minor	4.94	6.42
6	Spoofing of a second automotive on-board device through the use of the original automotive on-board device by users or the Unauthorized utilization of receivers by third parties	Confusion caused by the delivery of drive information containing incorrect information	Automotive on-board devices	Common	Unauthorized utilization	3G/GSM	User (intentional)	Information	Ordinary-use Interface	Network	Low	Single	7.95	None	Minor	Minor	4.94	5.46
7	Tracing to personal locations from received messages, through the use of receivers by third parties or the Unauthorized utilization of an automotive on-board device by users	Personal profiling	Automotive on-board devices	Field-specific	Information Leakage	Wi-Fi	Attacker	Information	Ordinary-use Interface	Adjacent	Medium	Multiple	3.55	Minor	Minor	None	4.84	3.39
8	Intentional shutdown of the control ECU`s control functions from 3G/LTE lines by third parties during normal operations	ECU disabled from working correctly, crippling the vehicle functions	ECU	Field-specific	Unauthorized utilization	3G/GSM	Attacker	Inherent functions	Ordinary-use Interface	Network	Medium	Single	6.83	None	Severe	Severe	9.21	7.95
9	Dealers' personnel falsify vehicle status information from Bluetooth devices, such as a smartphone, during maintenance.	Tampering with settings to make unintended changes to performance	Automotive on-board devices	Field-specific	Illegal setting	Bluetooth	Service provider	Information	Ordinary-use Interface	Adjacent	Low	Single	5.14	Minor	Minor	None	4.94	4.14
10	Malfunctioning of the information in the ECU`s information functions intentionally induced by third parties from an SD card interface during normal operations	Information functions prevented from working correctly	ECU	Field-specific	Unauthorized utilization	SD	Attacker	Inherent functions	Ordinary-use Interface	Local	Low	None	3.95	None	Minor	None	2.86	2.11

Level □ (Serious)
Level II (Warning)
Level □ (Caution)

7.3 RSMA Method

While impact subscores are categorized based on damage classifications for assessment, the impact subscore level is directly reflected in the risk score as an axis of assessment, as defined in the risk level assessment table. The likelihood level is another axis of assessment in the risk level assessment table, and is determined by the sum total of the scores of the five parameters: duration, specialized knowledge, TOE knowledge, opportunity and devices. The RSMA method involves more assessment parameters than other methods, so that the number of impact subscore parameters and likelihood subscore parameters to be assessed are out of balance. Table 7-3 summarizes examples of risk assessments produced by the RSMA method.

Table 7-3 Examples of Risk Assessments Produced by the RSMA Method

No	Possible threats	Possible damages	Target devices	Field-specific and common	Threat classification	Connection Interface	Who: Connected	Whom: Threats Did Harm To	Where: Risks Occurred	RSMA Method								
										Damage classification	Impact subscore	Duration	Specialized knowledge	TOE knowledge	Opportunity	Devices	Likelihood	Risk score
1	DoS attacks launched on an automotive on-board network via an external network	Shutdown of all services that require communication functions	Automotive on-board device	Common	DoS attack	3G/ GSM	Attacker	IoT functions	Ordinary-use Interface	Property and corporate value	Medium	Realistic	Professionals	Limited sets of users	Access not required and unlimited	Commercial products	High	H
2	Transmission of fake messages by server spoofing	User confusion and more	Automotive on-board device	Common	Fake messaging	3G/ GSM	User (wrong connection)	IoT functions	Ordinary-use Interface	Property and corporate value	Medium	Realistic	Professionals	Limited sets of users	Access not required and unlimited	Custom products	Medium	M
3	Freezing of systems due to streaming content exploiting browser bugs	Shutdown of infotainment services	Automotive on-board device	Common	Fake messaging	3G/ GSM	User (intentional)	IoT functions	Ordinary-use Interface	Property and corporate value	Medium	Realistic	Professionals	Limited sets of users	Access not required and unlimited	Custom products	Medium	M
4	Eavesdropping of communication messages by taking advantage of third parties` receivers	Use of services not intended by the operation management authorities	Automotive on-board device	Common	Eavesdropping	Wi-Fi	Attacker	Information	Ordinary-use Interface	Personal information and privacy	Low	Realistic	Professionals	Dealers, developers, manufacturers	Limited access count	Custom products	Medium	L
5	Delivery of messages containing incorrect locations through the Unauthorized utilization of GPS generators by third parties	Confusion caused by the delivery of messages containing incorrect locations	Automotive on-board device	Common	Illegal relaying	GPS	Attacker	Inherent functions	Ordinary-use Interface	Property and corporate value	Medium	Realistic	Professionals	Publicized information	Limited access count	Commercial products	High	H
6	Spoofing of a second automotive on-board device through the use of the original automotive on-board device by users or the Unauthorized utilization of receivers by third parties	Confusion caused by the delivery of drive information containing incorrect information	Automotive on-board device	Common	Unauthorized utilization	3G/ GSM	User (intentional)	Information	Ordinary-use Interface	Property and corporate value	Medium	Realistic	Professionals	Limited sets of users	Limited access count	Custom products	Medium	M

7	Tracing to personal locations from received messages, through the use of receivers by third parties or the Unauthorized utilization of an automotive on-board device by users	Personal profiling	Automotive on-board device	Field-specific	Information leakage	Wi-Fi	Attacker	Information	Ordinary-use Interface	Personal information and privacy	Low	Realistic	Professionals	Limited sets of users	Limited access count	Custom products	Medium	L
8	Intentional shutdown of the control ECU`s control functions from 3G/LTE lines by third parties during normal operations	ECU prevented from working correctly, crippling the vehicle functions	ECU	Field-specific	Unauthorized utilization	3G/ GSM	Attacker	Inherent functions	Ordinary-use Interface	Safety	High	Realistic	Professionals	Dealers, developers, manufacturers	Access not required and unlimited	Special devices	High	H
9	Dealers' personnel falsify vehicle status information from Bluetooth devices, such as a smartphone, during maintenance.	Tampering with settings to make unintended changes to performance	Automotive on-board device	Field-specific	Illegal setting	Bluetooth	Service provider	Information	Ordinary-use Interface	Property and corporate value	Low	Realistic	Professionals	Dealers, developers, manufacturers	Limited access count	Special devices	High	M
10	Malfunctioning of the information in the ECU`s information functions intentionally induced by third parties from an SD card interface during normal operations	Information functions prevented from working correctly	ECU	Field-specific	Unauthorized utilization	SD	Attacker	Inherent functions	Ordinary-use Interface	Property and corporate value	Low	Realistic	Professionals	Dealers, developers, manufacturers	Inaccessible	Special devices	Low	L

7.4 CCDS Prototype Method

The modified CCS method offers a simpler solution to calculating risk assessment than the other methods because it uses only the exploitability subscore and impact subscore as the basic items of assessment. Moreover, it has four risk score ranks defined to reduce significant variations in scoring and the tendency of risk scores to favor the center. An effort to reflect attackers` motivations in the risk scores has also been incorporated. This method was so radical that concerns were raised over the validity of its risk assessments. But following risk assessments conducted with the other three methods using the same set of threat cases, it was found to demonstrate similar trends despite slight method-specific differences. Table 7-4 summarizes examples of risk assessments produced by the CCDS Prototype Method.

Table 7-4 Examples of Risk Assessments Produced by the CCDS Prototype Method

No	Possible threats	Possible damages	Target devices	Field-specific and common	Threat Classification	Connection Interface	Who : Connected	Whom : Threats Did Harm To	Where : Risks Occurred	CCDS Prototype Method			
										Exploitability subscore	Impact subscore	Attackers` motivation	Risk score
1	DoS attacks launched on an automotive on-board network via an external network	Shutdown of all services that require communication functions	Automotive on-board devices	Common	DoS attack	3G/ GSM	Attacker	IoT functions	Ordinary-use Interface	C	Serious	Medium	Essential

2	Transmission of fake messages by server spoofing	User confusion and more	Automotive on-board devices	Common	Fake messaging	3G/GSM	User (wrong connection)	IoT functions	Ordinary-use Interface	C	Medium	Medium	High
3	Freezing of systems due to streaming content exploiting browser bugs	Shutdown of infotainment services	Automotive on-board devices	Common	Fake messaging	3G/GSM	User (intentional)	IoT functions	Ordinary-use Interface	C	Medium	Medium	High
4	Eavesdropping of communication messages by taking advantage of third parties` receivers	Use of services not intended by the operation management authorities	Automotive on-board devices	Common	Eavesdropping	Wi-Fi	Attacker	Information	Ordinary-use Interface	B	Minor	Medium	Low
5	Delivery of messages containing incorrect locations through the Unauthorized utilization of GPS generators by third parties	Confusion caused by the delivery of messages containing incorrect locations	Automotive on-board devices	Common	Illegal relaying	GPS	Attacker	Inherent functions	Ordinary-use Interface	B	Medium	Medium	Middle
6	Spoofing of a second automotive on-board device through the use of the original automotive on-board device by users or the Unauthorized utilization of receivers by third parties	Confusion caused by the delivery of drive information containing incorrect information	Automotive on-board devices	Common	Unauthorized utilization	3G/GSM	User (intentional)	Information	Ordinary-use Interface	B	Medium	Medium	Middle
7	Tracing to personal locations from received messages, through the use of receivers by third parties or the Unauthorized utilization of an automotive on-board device by users	Personal profiling	Automotive on-board devices	Field-specific	Information Leakage	Wi-Fi	Attacker	Information	Ordinary-use Interface	B	Minor	Medium	Low
8	Intentional shutdown of the control ECU`s control functions from 3G/LTE lines by third parties during normal operations.	ECU prevented from working correctly, crippling the vehicle functions	ECU	Field-specific	Unauthorized utilization	3G/GSM	Attacker	Inherent functions	Ordinary-use Interface	B	Destructive	大	Essential
9	Dealers' personnel falsify vehicle status information from Bluetooth devices, such as a smartphone, during maintenance.	Tampering with settings to make unintended changes to performance	Automotive on-board devices	Field-specific	Illegal setting	Bluetooth	Service provider	Information	Ordinary-use Interface	C	Medium	Medium	High
10	Malfunctioning of the information in the ECU`s information functions intentionally induced by third parties from an SD card interface during normal operations.	Information functions prevented from working correctly	ECU	Field-specific	Unauthorized utilization	SD	Attacker	Inherent functions	Ordinary-use Interface	B	Medium	Medium	Middle

Essential
High
Middle
Low

8 Trend Analyses Of Risk Assessment

Using the results of the risk assessments of the listed threat cases, trend analyses by item were conducted with regard to the six risk characteristics: field-specific and common threats, threat classification, connection Interface (intrusion route), who : connected, whom : threats did harm to and where : risks occurred.

Since risk analyses of the around 230 known incidents listed had already been completed, the risk assessment trend analyses were carried out using results of risk assessment with the CCDS Prototype Method. “Essential”, “High”, “Medium” and “Low” occurrences of the six risk characteristics by category item were counted, and the ratio of the number of “Essential” and “High” occurrences by category was calculated as an M&H ratio, along with the risk score average. Risk trends by category item were then analyzed on the basis of these values.

8.1 Field-specific and Common Threat

Table 8-1 summarizes the field-specific and common threat trend analyses conducted. No significant difference in the M&H ratio is seen between field-specific and common threats, but in terms of the “Essential” ratio, the field-specific threat cases score 46.0% when compared with 24.6% for common threats. Field-specific threat cases that specialize in the automotive field, including impacts on vehicle control, have a much higher “Essential” ratio than common threat cases concerned with information processing, which could also occur with other IoT devices. Field-specific threat cases are thus found to present more severe impacts than common threat cases.

Formulating field-common security guidelines or developing a field-common security verification infrastructure is clearly important, but responding to threats that could deliver tougher impacts should call for the formulation of field-specific guidelines or the development of field-common verification infrastructures.

Table 8-1 Field-specific and Common Threat Trend Analyses

Category	Essential	High	Middle	Low	Total occurrences	Risk score average	M&H ratio	Essential ratio
Field-specific	80	44	38	12	174	17.0	71.3%	46.0%

Common	14	26	13	4	57	14.5	70.2%	24.6%

8.2 Threat Classification

Table 8-2 summarizes threat classification trend analyses. Among the 10 items in the threat classifications, Unauthorized utilization and fake messaging are found to have a high M&H ratio. As outlined in Table 5-4, Unauthorized utilization is defined as unauthorized individuals taking advantage of the functions of an automotive system by spoofing or exploiting device vulnerabilities. Fake messaging is a threat posed by an attacker sending a spoofing message to an automotive system causing it to malfunction or display incorrect information. Considering the fact that both kinds of attacks are based on spoofing, the need to take countermeasures against spoofing in the operation phase of an automotive system should be factored into the guidelines for consideration.

Furthermore, configuration errors have a low M&YH ratio but users sometimes keep their automotive systems running without security being enabled because of configuration errors, which might pose a major threat to security.

Table 8-2 Threat Classification Trend Analyses

Category	Essential	High	Middle	Low	Total occurrences	Risk score average	M&H ratio
Configuration errors	2	0	2	0	4	14.8	50.0%
Virus infection	14	7	8	0	29	17.3	72.4%
Unauthorized utilization	33	18	10	2	63	18.1	81.0%
Illegal setting	3	8	2	2	15	14.4	73.3%
Information leakage	0	1	1	6	8	7.2	12.5%
Eavesdropping	3	3	2	2	10	13.2	60.0%
DoS attack	21	12	18	3	54	15.1	61.1%
Fake messaging	17	16	3	0	36	19.7	91.7%
Log loss	0	0	0	1	1	7.5	0.0%

Illegal relaying	1	5	5	0	11	12.5	54.5%

8.3 Connection Interface (Intrusion Route)

Table 8-3 summarizes connection Interface (intrusion route) trend analyses. OBD is generally considered to be an intrusion route vulnerable to attacks, but registered lower M&H ratio than other routes. This is probably because the risk assessment in the CCDS Prototype Method, used for the trend analyses, assessed exploitability subscores on the basis of the CVSS method. It therefore tended to give a higher exploitability subscores to local attacks than attacks originating from wireless networks, resulting in lower risk scoring.

3G/GSM and Wi-Fi, both of which were open to remote manipulation, had been predicted to result in high risk scores generally, but turned out to deliver lower M&H ratios than other intrusion routes. This is probably because many threat cases relating to information processing were involved, with impact subscores moving from medium to minor, giving rise to lower risk scoring.

Table 8-3 Connection Interface (Intrusion Route) Trend Analyses

Category	Essential	High	Middle	Low	Total occurrences	Risk score average	M&H ratio
3G/GSM	17	15	12	3	47	16.4	68.1%
Bluetooth	7	3	2	0	12	18.4	83.3%
CD	1	2	0	0	3	20.8	100.0 %
DSRC	0	3	0	0	3	15.4	100.0 %
E-call service interface	1	2	0	0	3	16.3	100.0 %
GPS	4	4	1	0	9	17.4	88.9%
OBD	25	8	11	4	48	16.4	68.8%
RF	13	11	2	2	28	18.3	85.7%
SD	2	0	3	0	5	16.0	40.0%

USB	2	3	4	0	9	14.3	55.6%
VICS	0	3	0	0	3	15.4	100.0 %
Wi-Fi	12	11	12	2	37	15.5	62.2%
Sensor	2	0	0	0	2	18.8	100.0 %
Special equipment	6	5	4	5	20	12.9	55.0%

8.4 Who : Connected

Table 8-4 summarizes who-connected trend analyses. Service providers had a somewhat higher M&H score than the others. This may be attributable to the fact that no threat use cases were essentially considered for service providers, i.e. a connection not envisioned by manufacturers at the time of design, hence no risks were expected.

Table 8-4 Who : Connected

Category	Essential	High	Middle	Low	Total occurrences	Risk score average	M&H ratio
Manufacturers and related firms	0	0	0	0	0	-	-
Service provider	0	5	0	1	6	11.5	83.3%
User (intentional)	0	10	12	0	22	12.5	45.5%
User (wrong connection)	2	2	2	0	6	15.3	66.7%
Attacker	92	53	37	15	197	17.0	73.6%
Accidental	0	0	0	0	0	-	-

8.5 Whom : Threats Did Harm To

Table 8-5 shows whom-did-threats-harm trend analyses. The IoT functions delivered an M&H ratio somewhat higher than others, but these attacks are mostly those launched from

wireless networks and tend to deliver a lower exploitability subscore, resulting in higher risk scores. Attackers might launch attacks on an automotive system from a wireless system to Unauthorized utilization or take over its IoT functions via remote control. This poses a greater threat by exploiting the IoT functions as a starting point, rather than simply harming certain kinds of information, such as personal and payment information. In the present context of a growing number of automotive systems linking and syncing with other IoT devices, responses to such threats should be mandatory.

Table 8-5 Whom : Threats Did Harm To

Category	Essential	High	Middle	Low	Total occurrences	Risk score average	M&H ratio
IoT functions (communication, linkage, concentration and more)	5	23	2	2	32	15.4	87.5%
Inherent functions (e.g., server, GW, thing)	74	25	31	4	134	17.8	73.9%
Information	14	19	19	10	65	13.7	55.4%
Bodies and properties	0	0	0	0	0	-	-
Others	1	3	0	0	1	19.5	100.0%

8.6 Where : Risks Occurred

Table 8-6 summarizes Where-risks-occurred trend analyses. There is not a significant difference between ordinary-use Interface and maintenance Interface in their M&H ratio, but in terms of the “Essential” ratio, the uppermost risk level, ordinary-use Interface and maintenance Interface are 37.2% and 55.8% respectively. If it is assumed that the maintenance Interface or informal Interface, as used by managers in running or updating software, will not be used for launching attacks because they are hidden and not publicized, professionals could navigate through such Interface to launch attacks.

Table 8-6 Where : Risks Occurred

Category	Essential	High	Middle	Low	Total occurr	Risk score	M&H ratio	Essen

					ences	averag e		tial ratio
Ordinary-use Interface	58	55	36	7	156	16.7	72.4%	37.2%
Maintenance Interface	29	8	11	4	52	16.6	71.2%	55.8%
Informal Interface	5	7	3	4	19	13.0	63.2%	26.3%
Internally contained risk	0	0	0	0	0	-	-	-
Physical contact	1	0	1	1	3	13.8	33.3%	33.3%

9 Conclusion

While this document is designed to present security guidelines related to automotive on-board devices, the discussions of possible threats, security procedures to beperformed in the lifecycle of a product, and other topics presented could also apply to other fields. Stringent use of these guidelines is recommended to allow for the efforts of security countermeasures in the processes of the development of a range of products.

As the growing popularity of the Internet of Things (IoT) means that previously standalone domestic appliances continue to provide a variety of connections to increase their functionality, the frequency of attacks that target these devices are only expected to increase. The number of cases of attacks launched on automotive on-board systems has noticeably been growing in recent years, and often makes headlines in the media, which is motivating interest in car security. The following measures are required to pursue security-conscious design and development activity in response to these and other evolving cases and threats:

① Update threat cases and have such updates reflected in the review of threat analyses and countermeasures.

② Conduct a threat analysis by assuming a system responsive to cases of evolving use to explore requirement specifications and countermeasures.

It has also been found from the threat case risk assessments and trend analyses by risk characteristics that attackers are able to breach systems through a carried-in device or via an external interface to attempt takeover by spoofing or launching more risky threats. In parallel with the formulation of field-specific security guidelines, the CCDS is working to develop security validation and verification tools compatible with IoT devices as part of its security verification infrastructure formation initiative. Two kinds of validation and verification tools have also been developed in the automotive on-board devices field. The reader is strongly advised to utilize tests starting with possible interface with an automotive on-board devices the most likely trapdoor.

Finally, thanks are due to the members of the Automotive On-board Devices SWG for their extensive support in compiling this document.

10 Association With “IoT Safety/Security Development Guidelines”

“IoT Safety/Security Development Guidelines” was released by the Information-technology Promotion Agency, japan (IPA) in March 2016. These Guidelines have been formulated to encourage the manufacturers of IoT devices and systems to carry out certain basic tasks to ensure compliance with security-conscious development practice such as security guidelines, as well as existing safety standards.

Four committee members joined from the CCDS to work on the compilation. The formulation of this document and the IoT Safety/Security Development Guidelines have been achieved through mutual sharing of the status of discussions. The IoT Safety/Security Development Guidelines may be thought of as a collection of industry-wide interdisciplinary guidelines, when compared with this document that covers compatible guidelines focusing on the specific field of automotive on-board systems. A comparison between IoT Safety/Security Development Guidelines and this document is summarized in Table 10-1 and Table 10-2 for use in cross-referencing.

Table 10-1 A Comparison between IoT Safety/Security Development Guidelines and This Document 1

IoT Safety/Security Development Guidelines			Corresponding part of this book	
Major item		Guidelines	Chapter No.	Overview
Policy	Making corporate efforts for the Safety/Security of the Smart-society	Guideline 1 Formulating the basic policies for Safety/Security	4.2.1	Describe the efforts contents ① ~ ③ to the basic policy of the company in Section 1.Lists issues 1 to 3 relating to the efforts to be made by a corporation to approach its basic policies under Item 1.
		Guideline 2 Reviewing systems and human resources for Safety/Security	4.2.1	Lists issues 1 to 5 relating to the corporate framework required under Item 2. Lists issues 1 to 3 relating to the scheme of human resources development activity required under Item 3.
		Guideline 3 Preparing for internal frauds and mistakes	4.2.1	Lists issue 3 relating to education aimed at preventing internal fraudulence under Item 3.
			4.2.2	Lists issues 1 to 4 relating to the actions to be taken to prevent fraudulence by stakeholders under Item 5.
			4.2.3	Lists cautions to prevent setup errors and the outflow of documentation in (2) under Item 3 and in (1) under Item 5.
			8.2	Inserts an alert to prevent setup errors in the implementation of trend analyses of threat classifications.
Analysis	Understanding the risks of the Smart-society	Guideline 4 Identifying the objects to be protected	5.2	Defines what needs to be observed on the “Whom threats did harm to” principle in accordance with the IPA’s scheme of classifying risk characteristics in the implementation of threat analyses.
			7.1～7.4	Implement risk assessments of the threat cases after defining what needs to be observed.
			8.5	Summarizes the results of trend analyses carried out with regard to the risk characteristics of whom threats have done harm to.
		Guideline 5 Assuming the risks caused by connections	2.2	Presents the system model under discussion in Figure 2.3, defining the points of connectivity with an on-board system.
			4.2.2	Lists issues 1 to 5 for presuming the risks of connectivity under Item 1. Singles out (3) key management and (6) informal interface as topics of discussion in an action review under Item 3.
			5.2	Defines who connected and where risks occurred as a result of connections on the “Who connected” and “Where risks occurred” principle in accordance with the IPA’s scheme of classifying risk characteristics in the implementation of threat analyses.
			7.1～7.4	Implement a risk assessment of threat cases after identifying who connected and where risk occurred.
			8.4、8.6	Present the results trend analyses carried out with regard to the risk characteristics of who connected and where risks occurred.
		Guideline 6 Assuming the risks spread through connections	5.2	Presents risk classifications as part of the risk characteristics of a threat analysis, including “virus infection,” “abuse” and “DoS attacks,” which are possible risks that may result from connections.
			7.1～7.4	Implement a risk assessment of the threat cases after defining threat classifications.
			8.2	Summarizes the results of trend analyses carried out with regard to the risk characteristics of threat classifications.
		Guideline 7 Understanding physical security risks	3.2	Figure 3-1 illustrates the case of a remote attack launched on a car.
			4.2.4	Items 1 and 2 describe efforts to be made in the scrapping phase.
			8.5、8.6	Present alerts to attacks launched in a remote operation or over a maintenance or informal interface.

Table 10-2 A Comparison between IoT Safety/Security Development Guidelines and This Document 2

IoT Safety/Security Development Guidelines			Corresponding part of this book	
Major item		Guidelines	Chapter No.	Overview
Design	Considering the designs to protect the objects to be protected	Guideline 8 Designing to enable both	4.2.2	Covered in (9) and (10) in the action review under Item 3.
			5.2	Describes risks raised via an external interface, intrinsic risks and risks raised upon physical contact in the context of "Where threats occurred."
			7.1～7.4	Implement a risk assessment of threat cases after identifying where risks occurred.
			8.2	Describes the need to take countermeasures against the risks of spoofing, in a trend analysis of threat classifications.
			8.6	Presents alerts to attacks launched over a maintenance or informal interface, in a trend analysis of where threats occurred.
		Guideline 9 Designing so as not to cause trouble in other connected entities	4.2.2	Lists issues 1 to 4 relating to responses to unknown threats under Item 7.
		Guideline 10 Ensuring consistency between the designs of safety and security	4.2.2	Covers issues relevant to the threat analysis under Item 2 and the evidence under Item 4.
			Chapters 5 to 7	Presents case studies conducted using four methods with regard to how to carry out threat analyses and risk assessments, to recommend the implementation of analyses using multiple assessment methods in (1) under Item 2, 2.2.2 and to aid in the reassessment of threats after the implementation of measures in (3) under Item 2.
		Guideline 11 Designing to ensure Safety/Security even when it is connected with the unspecified partner.	4.2.2	Covered in (5) in the action review under Item 3 only to mention the action validation, without going as far as to mention how to make connections depending on whom to connect with and where.
		Guideline 12 Verifying/validating the designs of safety and security	4.2.2	Lists issues 1 to 3 relating to the assessment and verification process under Item 6.
			Chapters 5 to 7	Assess risks by defining what needs to be protected, how to make connections, where risks occurred and so on, in addition to who connected, whom risks did harm to and where risks occurred, in accordance with the IPA's scheme of classifying risk characteristics in the implementation of threat analyses, and suggest the need to explore measures according to the risk degree.
Maintenance	Considering the designs to ensure protection even after market	Guideline 13 Implementing the functions to identify and record own status	4.2.2	Describes an issue relating to logs in (4) under Item 7.
		Guideline 14 Implementing the functions to maintain Safety/Security even after the passage of time	4.2.3	Describes issues 1 and 2 as updates under Item 4.
Operation	Protecting with relevant parties	Guideline 15 Identifying IoT risks and providing information after market release	4.2.3	Describes what is shared as incident information under Item 6.
			Chapter 9	Suggests the need to update threat cases and carry on threat analyses to respond to new use cases, as future tasks.
		Guideline 16 Informing relevant business operators of the procedures to be followed after market release	4.2.3	Presents a definition of usage during operations under Item 2.2.
		Guideline 17 Making the risks caused by connections known to general users	4.2.3	Describes issues 1 and 2 relating to what needs to be observed by users as user instructions under Item 1. Describes issues 1 to 2 to alert users under Item 3.

11 Association With “Automotive Information Security Efforts Guidelines” [7]

In formulating these Guidelines, the “Automotive Information Security Efforts Guidelines”. published by the Information-technology Promotion Agency, japan (IPA) in March 2013, was consulted. A comparison between the “Automotive Information Security Efforts Guidelines” and this document is summarized in Table 11-1 for cross-referencing with the comparison between the IoT Safety/Security Development Guidelines and the document listed in the previous chapter.

Table 11-1 Table of Comparison between the “Automotive Information Security Efforts Guidelines” and This Document

Action Guide to Information Security of Automobiles				Corresponding part of this book	
Chapter	Title	Chapter No.	Title	Chapter No.	Summary
1	Introduction	1.1.	Current status and Issues of car security	1.1	Presents the present status and issues of security of automotive on-board modules.
		1.2.	The aim of this book	1 and 1.2	Defines the objective of this document in Chapter 1, "Introduction," and its audiences in Section 1.2.
2	Automotive Systems and Security	2.1.	Model of automobile systems	2.1 and 1.2	Defines the target model in Section 2.1 and the system model under discussion in Section 2.2.
		2.2.	Threat on the security assumed in a car system		Describes possible threats to security.
		2.3.	Security measures against threats	–	A detailed description of the measures is beyond the scope of this document.
		2.4.	Mapping functions, threats and countermeasures technology	–	A detailed description of the measures is beyond the scope of this document.
3	Efforts to security in the automotive system	3.1.	Life cycle of the automotive system	4,1	Cites and defines the life style of an automotive system.
		3.2.	Security efforts level and policy of each phase	–	A description of phase-specific efforts to be made is beyond the scope of this document.
4	Details of the efforts to security	4.1.	Efforts in the management	4.2.1	Describes efforts to be made in the policy formulation phase.
		4.2.	Efforts in the planning phase	4.2.2	Describes efforts to be made in the planning and development phase.
		4.3.	Efforts in the development phase	4.2.2	Describes efforts to be made in the planning and development phase.
		4.4.	Efforts in the operational phase	4.2.3	Describes efforts to be made in the operation phase.
		4.5.	Efforts in the disposal phase	4.2.4	Describes efforts to be made in the scrapping phase.

References

[1] H. Takada, A. Goto and et al., “IoT Safety/Security Development Guidelines,” Information-technology Promotion Agency, Japan (IPA), First Edition, 2016, http://www.ipa.go.jp/files/000053920.pdf.

[2] 高田 広章, 後藤 厚宏ら, “つながる世界の開発指針,” 独立行政法人情報処理推進機構 (IPA) 技術本部 ソフトウェア高信頼化センター(SEC), 第 1 版, 2016, http://www.ipa.go.jp/files/000054906.pdf.

[3] ETSI, “Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis,” Europian Telecommunications Standards Institute, ETSI TS 102 165-1 v4.1.1 (2003-02), Technical pecification, 2003, http://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.01.01_60/ts_10216501v040101p.pdf.

[4] C. Laurendeau and M. Barbeau, “Threats to Security in DSRC/WAVE,” ADHOC-NOW 2006 Proceedings, Lecture Notes in Computer Science Vol. 4104, pp. 266—279, 2006, http://people.scs.carleton.ca/~claurend/Pubs/adhocnow2006.pdf.

[5] 萱島 信ら, “運転支援通信システムに関するセキュリティガイドライン,” ITS 情報通信システム推進会議, ITS FORUM RC-009 1.0 版, 2011, http://www.itsforum.gr.jp/Public/J7Database/p41/ITS_FORUM_RC009V1_0.pdf.

[6] JASO, “自動車ー情報セキュリティ分析ガイド,” 公益社団法人自動車技術会 規格会議審議, JASO TP15002, 2015.

[7] IPA, “自動車の情報セキュリティへの取組みガイド,” 独立行政法人情報処理推進機構 (IPA), 第 1 版, 2013, https://www.ipa.go.jp/files/000027273.pdf.