JASO

Technical Paper

Guideline for Automotive Information Security Analysis

JASO TP-15002

Enacted March 15, 2016

Society of Automotive Engineers of Japan

Standards Board Deliberation

Documents
Document Sharing Hub

Full document details: JASO TP-15002 2016

Contents

Page

Foreword

1. Introduction 1

1.1 Background **1**

1.2 Purpose **1**

1.3 Terminology and definitions **2**

2. How to use this document **3**

3. Definition of security problems **4**

3.1 Phase 1: TOE definition **4**

3.2 Phase 2: threat analysis **5**

3.3 Phase 3: risk assessment **7**

4. Security Objectives **8**

4.1 Phase 4: define Security Objectives **8**

5. Security requirement **9**

5.1 Phase 5: security requirement selection **9**

Appendix A System model example **11**

Appendix B TOE Definition **12**

Appendix C Threat analysis **15**

Appendix D Risk Assessment **20**

Appendix E Security Objectives **28**

Appendix F Security Requirements **31**

References **43**

Notes **44**

Documents
Document Sharing Hub

Full document details: JASO TP-15002 2016

Foreword

This technical paper was established by the Standards Board, through deliberations at the Standards Committee in accordance with the Standards Board organization rules based on the bylaws of the Society of Automotive Engineers of Japan.

This technical paper is protected under copyright law.

Attention is drawn to the possibility that some of the elements of this technical paper may conflict with patent rights, applications for patents after opening to the public, or utility model rights. The Standards Committee of the Society of Automotive Engineers of Japan is not responsible for identifying such patent rights, applications for patents after opening to the public and utility model rights.

Documents
Document Sharing Hub

Full document details: JASO TP-15002 2016

Documents
Document Sharing Hub

Full document details: JASO TP-15002 2016

TECHNICAL PAPER

Guideline for Automotive Information Security Analysis

1. Introduction

1.1 Background

Information security problem are gaining prominent attention in the automotive field as automotive electronic control technology develops and connections with external networks expand. It is necessary to use an appropriate security function in the total in-vehicle network and in the development of the various ECUs that are connected to this network.

In the information system field, Common Criteria (CC) (ISO/IEC 15408) and the like are used to check and evaluate the security function of IT products and systems. In the automotive industry, there is emerging recognition of the need to develop a framework in which security functions are used in reference to the information system field. As a result, The Society of Automotive Engineers of Japan, Inc. began to develop a standard procedure for security design via the Information Security Subcommittee of the Electronics and Electrical Committee.

1.2 Purpose

When considering Cybersecurity design, it is necessary to analyze the threats and to assess the risks. However, current standards used as a reference have not clearly defined these procedures. For this reason, this document was developed to describe standard procedures that define the security function by analyzing the threats for the developers of the system, including the in-vehicle network [(*)]. The appendices of this document describes the following procedures while showing a simple in-vehicle network as an example:

- Modeling the system (TOE)
- Extracting the Threat analysis
- Evaluating the Risk assessment
- Security objectives
- Extracting the security requirements

Details about extracting security requirements can be found in the CC and other related documents.

* Although the phase structure of this document can also be applied to threat analysis for each ECU, the examples described herein use the in-vehicle system including the network.

Documents
Document Sharing Hub

Full document details: JASO TP-15002 2016

1.3 Terminology and definitions

Common Criteria (CC)	An international standard to evaluate information technology security.
Common Vulnerability Scoring System (CVSS)	A project of The National Infrastructure Advisory Council. The draft was created in October 2004. This is an open and generalized method to evaluate vulnerabilities of information system.
Evaluation Assurance Level (EAL)	The evaluation assurance level defined by CC.
Fault tree (FT)	A method to represent the event used to analyze failures and accidents. The FTA is a top-down analysis method often used for reliability evaluation and safety analysis.
Protection Profile (PP)	Security requirement specifications defined by CC.
Security Function Policy (SFP)	Security function policy defined by CC.
Security Functional Requirement (SFR)	Security functional requirements defined by CC.
Security Target (ST)	Security design specifications defined by CC.
Target of Evaluation (TOE)	Any items that are evaluated for security. A whole product or partial function can be evaluated as a target.
TOE Security Functionality (TSF)	Security functionality of the TOE as defined by CC.
Security problem	This is a statement defined by a format, describing the characteristics or security scope to which the TOE should respond. This statement consists of the following items: - Threat that are to be countered by the TOE - Organizational Security Policies(OSPs) that are to be enforced by the TOE - Assumptions maintained for the TOE and its operation environment.
Threat	A potential cause of a security incident that harms the information system.
Vulnerability	A weak point in the system that may be used to cause a security incident.
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes (SOURCE: ISO/IEC2700)
Integrity	Property of accuracy and completeness (SOURCE:ISO/IEC2700)
Availability	Property of being accessible and usable upon demand by an authorized entity (SOURCE: ISO/IEC2700)
Threat agent	Person or object that causes a threat.
Protected asset	Any item that must be protected from a security threat.

Documents
Document Sharing Hub

Full document details: JASO TP-15002 2016

2. How to use this document

This document describe the in-vehicle network system. It can be used as a “how-to” to extract the threats and establish the countermeasures. The procedures defined by this document consist of the phases and steps described in **Figure 2.1**. Detailed examples of the procedures in each step are described in the appendices.

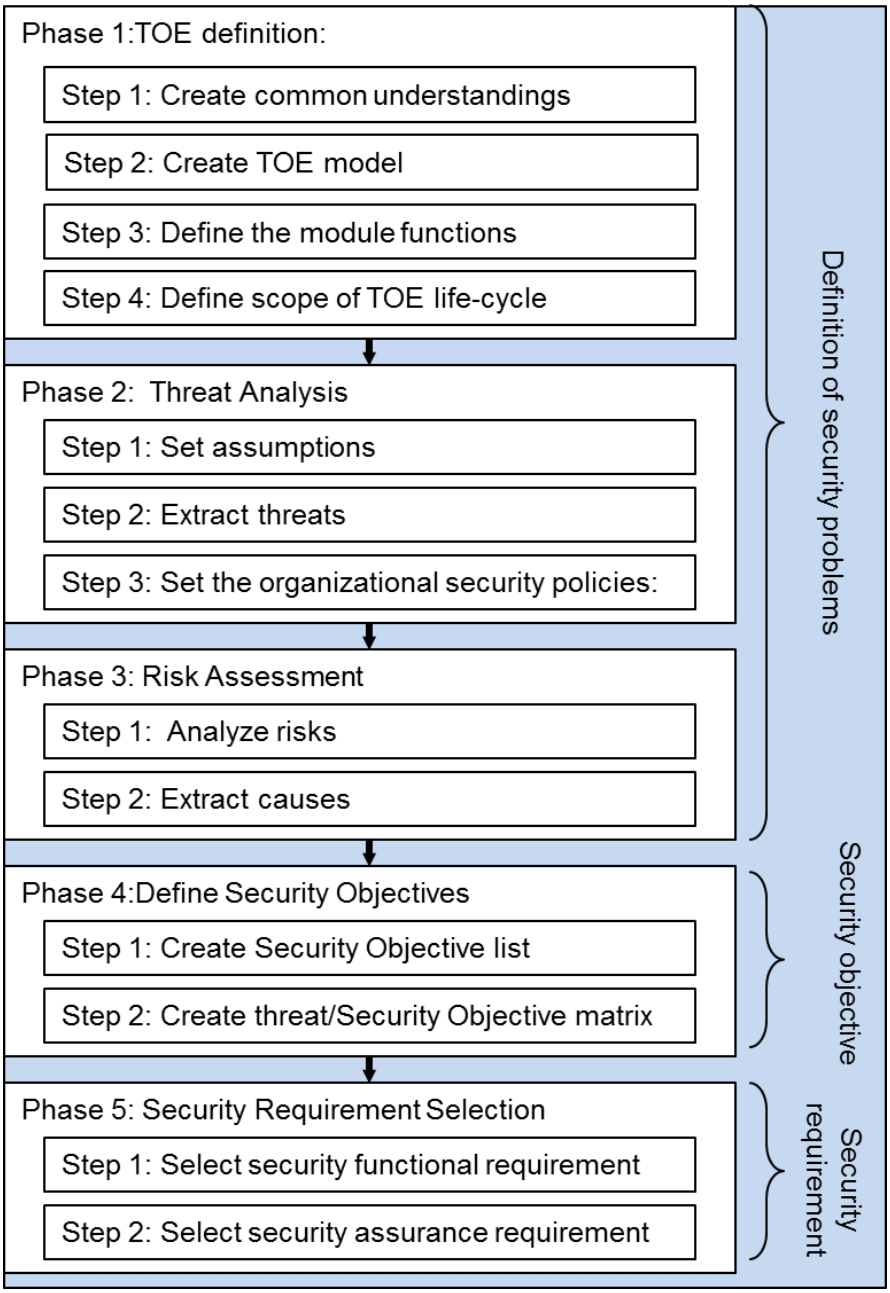

Figure 2.1 Procedures to be performed as defined this document

Documents
Document Sharing Hub
Full document details: JASO TP-15002 2016

3. Definition of security problems

This section describes the procedures to analyze the threats and to evaluate the risks for the TOE.

3.1 Phase 1: TOE definition

3.1.1 Purpose and contents

To clarify the TOE for Threat analysis in the next step.

3.1.2 Inputs

a) System outline

1) System configuration

2) System function

3) Information/data that the system handles

3.1.3 Outputs

b) TOE system outline

1) TOE Model

2) Module Function List

3) Life-cycle List

3.1.4 Activity

Figure 3.1 shows the procedure to perform this phase.

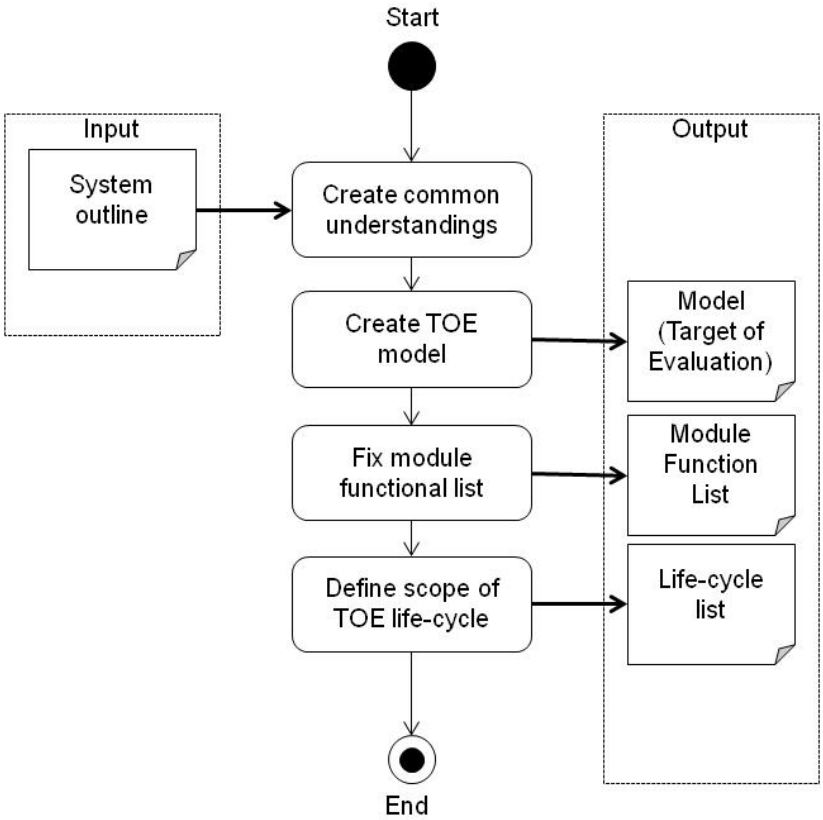

Figure 3.1 Procedure in TOE Definition phase

Documents
Document Sharing Hub
Full document details: JASO TP-15002 2016

3.1.4.1 Step 1: create common understandings

To generate a common recognition of all project members for the life-cycle and system architecture of the target system based on the system concept, the data to be input as defined in **Section 3.1.2** can be prepared. For details, see **Section B.2** of **Appendix B**.

3.1.4.2 Step 2: create TOE model

A TOE model can be created to identify the components of the TOE system and the information flow between the components. For details, see **Section B.3** of **Appendix B**.

3.1.4.3 Step 3: define the module functions

The Module Function List that describes the functions provided for each component module (described in the TOE model) and the protected assets included in the functionality can be created. For details see **Section B.4** of **Appendix B**.

3.1.4.4 Step 4: define scope of TOE life-cycle

The Life-cycle List that clarifies the whole TOE system life-cycle can be created. For details, see **Section B.5** of **Appendix B**.

3.2 Phase 2: threat analysis

3.2.1 Purpose and contents

The information security problem of the TOE system defined in Phase 1 can be identified.

3.2.2 Inputs

a) Information related to the TOE system

1) System preliminary condition (including rules and regulations that need to be in compliance)

2) System outline

b) Work products in the TOE Definition phase

1) TOE Model

2) Module Function List

3) Lifecycle List

3.2.3 Outputs

a) Assumptions List

b) Threats List

c) Organizational security policies List

3.2.4 Activity

Figure 3.2 shows the procedures executed in this phase.

Documents
Document Sharing Hub

Full document details: JASO TP-15002 2016

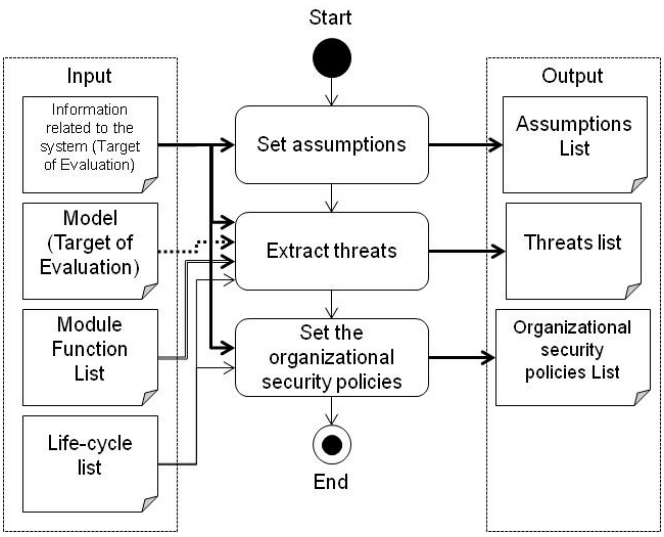

Figure 3.2 Procedure in Threat Analysis phase

3.2.4.1 Step 1: set Assumptions

The assumptions for TOE environment can be defined based on the TOE model, Module Function List, and Life-Cycle List in order to clarify the scope of the threat analysis and to limit the scope of threat extraction for Step 2 (e.g., “the developer of the TOE must be confidence” or “the Internet service communicating with the TOE must be properly operated”) . An Assumptions List can be created by assigning an identification name with an “A” prefix for each Assumption. For details, see **Section C.2** of **Appendix C**.

3.2.4.2 Step 2: extract threats

The threats to the protected asset of the system component, which include “where”, “who”, “when”, “why”, and “what”, can be invoked by setting up an FT, based on the TOE model, Module Function List and Life-cycle List. An Assumptions List can be created by assigning an identification name with a “T” prefix for each extracted threat. For details, see **Section C.3** of **Appendix C**.

3.2.4.3 Step 3: set the Organizational security policies

The Organizational security policies define the requirements for the security countermeasures to be implemented for reasons except the threats. The policy can be regulations and industry guidelines with which compliance is necessary when developing or operating the TOE. Also information related to the TOE system, which are defined as security problem can be extracted from the regulations and internal standard related to the system development. An Organizational security policies List can be created by assigning an identification name with a “P” prefix for each security policy. For details, see **Section C.4** of **Appendix C**.

* If there are no regulations or guidelines requiring compliance, there cannot be any items listed in the Organizational security policies list.

Documents
Document Sharing Hub
Full document details: JASO TP-15002 2016

3.3 Phase 3: risk assessment

3.3.1 Purpose and contents

To determine the Security Objectives, the risk level for all identified threats in the Threat Analysis phase can be identified and the goal for the countermeasures can be established.

3.3.2 Inputs

a) Work products in the TOE Definition phase

1) TOE Model

2) Module Function list

b) Work products in the Threat Analysis phase

1) Threats List

3.3.3 Outputs

a) Threats List (version in which the risk assessment have been added)

b) FT

3.3.4 Activity

Figure 3.3 shows the procedures executed in this phase.

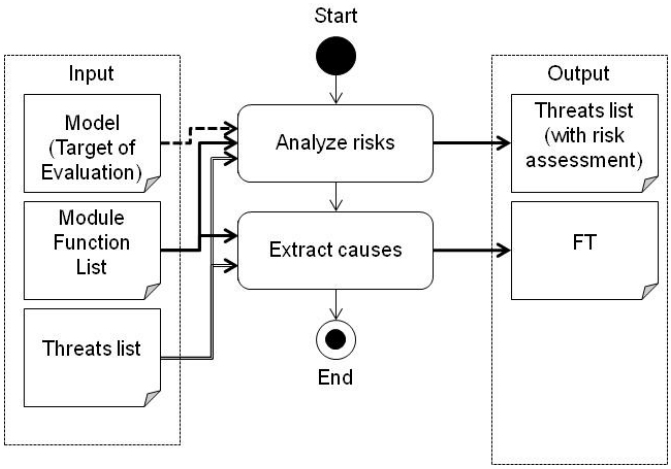

Figure 3.3 Procedure in Risk Assessment phase

3.3.4.1 Step 1: analyze risks

The threat occurrence possibility and the impact for each threat event in the Threat List resulting from Phase 2 can be identified, and the risk values can be calculated. The risk values can be calculated by referencing the Module Function List and Threat List defined in the previous phase. For details, see **Section D.2** of **Appendix D**.

3.3.4.2 Step 2: extract causes

An FT can be created for threat events of certain level (or higher) of risk value, and how those threats are

Documents
Document Sharing Hub
Full document details: JASO TP-15002 2016

invoked can be analyzed logically. For details, see **Section D.3** of **Appendix D**.

4. Security Objectives

This section describes the procedure to establish the security objectives for the TOE.

4.1 Phase 4: define Security Objectives

4.1.1 Purpose and contents

The security objectives for the threat events (for which the countermeasures should be applied), Assumptions, and the Organizational security policies shall be identified, and, at the same time, the definition of the necessary security objectives shall be confirmed.

4.1.2 Inputs

a) Deliverables from the Threat Analysis phase

1) Assumptions List

2) Organizational security policies List

b) Deliverables from the Risk Assessment phase

1) Threat List (version in which the risk assessment have been added)

2) Fault Tree

4.1.3 Outputs

a)Security Objectives

b)Threat/Security Objective Matrix

4.1.4 Activity

Figure 4.1 shows the procedures executed in this activity

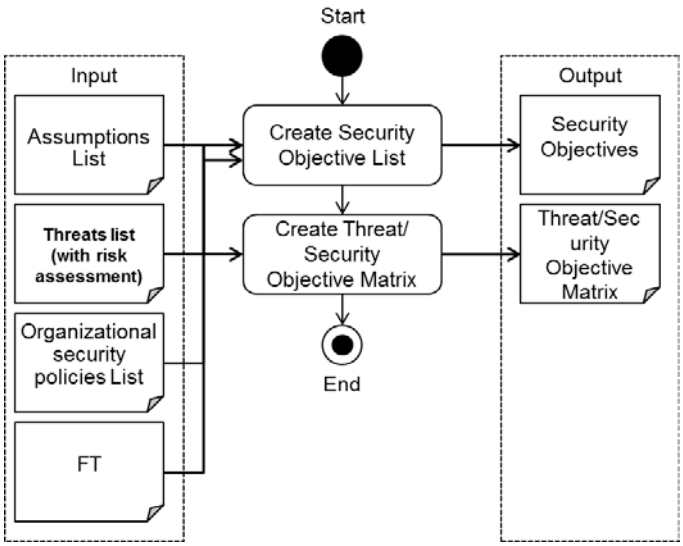

Figure 4.1 Procedures executed in security objective Definition phase

Documents
Document Sharing Hub
Full document details: JASO TP-15002 2016

4.1.4.1 Step 1: create security objective list

Select threats to develop its security objectives according to its risk score. And develop security objectives for each end-point of fault tree of the selected threats. For details, see **Section E.2** of **Appendix E**.

4.1.4.2 Step 2: Create threat/security objective matrix

To make sure that every threat to be dealt with is linked with appropriate security objectives, create threat/security objective matrix and check it. For details, see **Section E.3** of **Appendix E**.

5. Security requirement

This section describes the procedures to develop the security requirements for the TOE.

5.1 Phase 5: security requirement selection

5.1.1 Purpose and contents

The security functionality requirements for the security objectives and the security assurance requirements required by the TOE shall be selected.

5.1.2 Inputs

a) Catalog of security requirement [(1)]

1)Catalog of security functional requirement

2)Catalog of security assurance requirement

b) Deliverable from Security Objectives Formulation phase

3) Security Objectives

Note: [(1)]

Details of the Catalog of security requirement are shown in parts 2 and 3 of the Common Criteria for Information Technology Security Evaluation.

5.1.3 Outputs

a) Security Functional Requirement List

b) Security Policy/Security Functional Requirement Matrix

c) Security Assurance Requirement List

5.1.4 Activity

Figure 5.1 shows the procedures executed in this phase.

Documents
Document Sharing Hub

Full document details: JASO TP-15002 2016

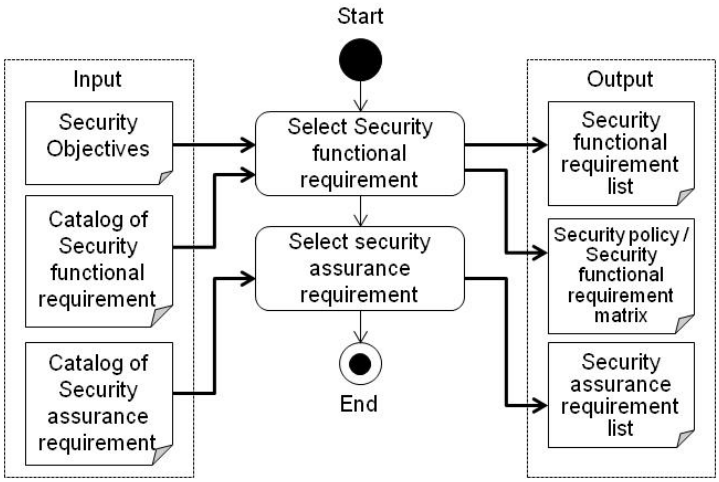

Figure 5.1 Procedure in Security Requirement Selection phase

5.1.4.1 Step 1: select security functional requirement

The security functional requirement list shall be derived by choosing its items from the catalog of security functional requirements according to the security objectives of TOE.

To make sure that each objective is linked with one or more security functional component, the security objective / functional component matrix should be derived from security objectives and the catalog of security functional components. For details, see Section F.2 of Appendix F.

5.1.4.2 Step 2: select security assurance requirement

To define security assurance requirement for TOE, select EAL (Evaluation Assurance Level) according to the catalog of security assurance requirements and security functional requirements for TOE, see Section F.3 of Appendix F.

Documents
Document Sharing Hub
Full document details: JASO TP-15002 2016

Appendix A

System model example

*To provide a clear understanding of how to use this document, the following appendices explain the procedures to define the security problem using the example in-vehicle system shown in **Figure A.1**.*

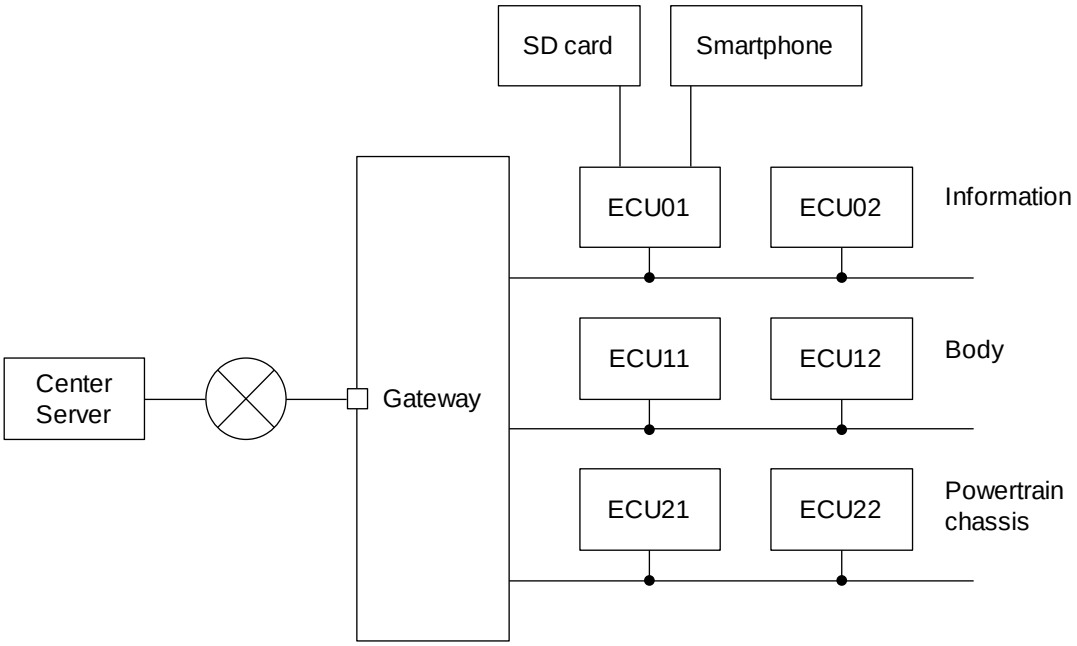

Figure A.1 In-vehicle system configuration (example)

The following functionalities are assumed in this in-vehicle system example:

a) A function to transmit the information to the Center Server from the Information domain ECUs

b) A function to transmit the information to the Control ECU (i.e. Body domain ECUs and Powertrain chassis domain ECUs) from the Center Server

c) A function to overwrite the data by the SD card interface in the Information ECUs

d) A function to communicate with a smartphone using a Bluetooth interface in the Information ECUs

The following appendices describe how to use this document by the examples in which the Security Analysis procedures are applied for the above system.

Documents
Document Sharing Hub
Full document details: JASO TP-15002 2016