関係各部署　御中

To departments concerned

Confidentiality classification	PROTECTED 関係者外秘	原紙保管 Storage of original	M/Y /
		コピー保管 Storage of copy	M/Y /

侵入検知　エントリーポイント向け Host IDS　要求仕様書 Requirements Specification of Host-based IDS for Entry Point

制御電子プラットフォーム開発部
制御ネットワーク・アーキ開発室 4G
System Network & Architecture Development Dept. 4G
E/E Architecture Development Div.

No. SEC-ePF-IDS-HIE-REQ-SPEC-a00-04-c

承認 Approved by	調査 Checked by	作成 Created by	2022/06/09
河井	松井	竹山	Omission of signature (approved electronically)

適用先 Target	エントリーポイント ECU/VM のうち、別文書にて定義される特定の ECU/VM に適用される Allocated to entry-point ECUs / VMs specified by another document.
変更概要 Change	SEC-ePF-IDS-HIE-REQ-SPEC-a00-04-b ⇒ SEC-ePF-IDS-HIE-REQ-SPEC-a00-04-c ・要求事項の表現修正 Requirement editorially corrected
特記 Special note	【展開規則　Distribution rule】 必要に応じて、関係会社・関係部署（海外事業体、ボデーメーカ、ECU サプライヤ）への展開をお願いします。 Please distribute this document to affiliated companies, or departments (e.g. overseas business entities, car body manufacturers, or ECU suppliers) if necessary. 【問合せ先　Contact information】 制御電子プラットフォーム開発部　制御ネットワーク・アーキ開発室 セキュリティ仕様問合せ窓口 System Network & Architecture Development Dept. E/E Architecture Development Div. Contact for Security Inquiries email: epf-sec-sp@mega.tec.toyota.co.jp

変更履歴

Version	変更内容	日付	変更者
a00-00-a	新規作成	2021/04/05	46F 4G 稲垣
a00-00-b	英訳追加	2021/05/14	46F 4G 稲垣
a00-01-a	要求具体化、可読性向上	2021/08/06	46F 4G 竹山
a00-02-a	死活監視の SEv 生成に関わる要求を削除 バージョン読み出し機能に関わる要求を削除	2021/12/03	46F 4G 竹山
a00-03-a	参照文書を追加 T.B.D.の記載を削除 QSEv 保管の要求を修正 IDSHER_07208 追加 IDSHER_02101 の検知技術例修正 IDSHER_04101 修正 IDSHER_02301 修正 IDSHER_07102 修正 IDSHER_07108 修正	2022/02/03	46F 4G 竹山
a00-04-a	・要求一覧にハードウェア関連要件の列を追加 ・IDSHER_02301 文言の修正 ・IDSHER_04101 文言の修正 ・IDSHER_07102 Context Data の項目の明確化 ・IDSHER_07108 文言の修正 ・IDSHER_07109 QSEv 保管の要求を変更 ・IDSHER_07111 UserDefineDTC, DID の要求追加 ・IDSHER_07110 QSEv 読み出しの SID を明確化 ・IDSHER_07202 削除 ・IDSHER_07204 QSEv 消去の SID を明確化	2022/04/29	46F 4G 竹山
a00-04-b	・IDSHER_07111 UserDefMemoryDTC の値修正 ・IDSHER_07110 ダイアグ仕様参照を追記 ・IDSHER_07204 ダイアグ仕様参照を追記	2022/05/20	46F 4G 竹山
a00-04-c	・表 2-2 誤記修正 ・IDSHER_12201 誤記修正 ・IDSHER_07109 補足の一部を要求として記載	2022/06/09	46F 4G 竹山

目次

1. はじめに

1.1. 本書の目的

エントリーポイント向けホスト型侵入検知システム（以下、本システム）の目的は、エントリーポイントへの侵入またはその試みを検知し、記録することである。本システムによって記録されるログは、米国国立標準研究所（NIST）が作成したサイバーセキュリティ対策に関するフレームワークにおける「検知」機能（参照文書[1]）の実現に用いられる。この本システムの要求を定義することが、本書の目的である。

1.2. 適用範囲

本書は、エントリーポイント ECU/VM のうち、別文書にて定義される特定の ECU/VM に適用される。

1.3. 前提条件

無し

1.4. 要求事項の記載

【要求事項：**】と記載されている部分が要求事項である。なお、<補足>と記載されている部分は、単なる補足事項であり、要求事項に含まれない。

1.5. 関連文書

上位文書および参照文書を本節にて示す。なお、関連文書のバージョンは ECU の要求仕様書に従うこと。

1.5.1. 上位文書

表 1-1：上位文書

No.	文書名	Ver.
1	車両サイバーセキュリティコンセプト定義書	-

1.5.2. 参照文書

表 1-2：参照文書

No.	文書名	Ver.

1	Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11	1.1
2	QSEv 生成要求仕様書	-
3	AUTOSAR_PRS_IntrusionDetectionSystem	R20-11
4	AUTOSAR_SWS_IntrusionDetectionSystemManager	R20-11
5	AUTOSAR_SWS_AdaptiveIntrusionDetectionSystemManager	R20-11
6	車両サイバーセキュリティ及びプライバシー用語定義書	-
7	欠番	-
8	タイムスタンプ要求仕様書	-
9	TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	-
10	侵入検知 多層分離機能向け Host IDS 要求仕様書	-
11	侵入検知 検知マスタ要求仕様書	-

1.6. 用語定義

本書で用いる用語を以下に示す。なお、本システムの一部は AUTOSAR にしたがい実装されることを想定しているため、本書では AUTOSAR で定義されている用語を利用する。それらの意味については参照文書[3]、[4]、[5]を参照されたい。その他用語については、参照文書[6]を参照されたい。

表 1-3：用語一覧

用語	解説
-	-

2. 要求概要

2.1. システムコンテキスト

本システムのシステムコンテキストをデータフローダイアグラムで示す（図 2-1）。円は本システムを、四角は本システムと情報やサービスのやり取りを行う主体を表す。

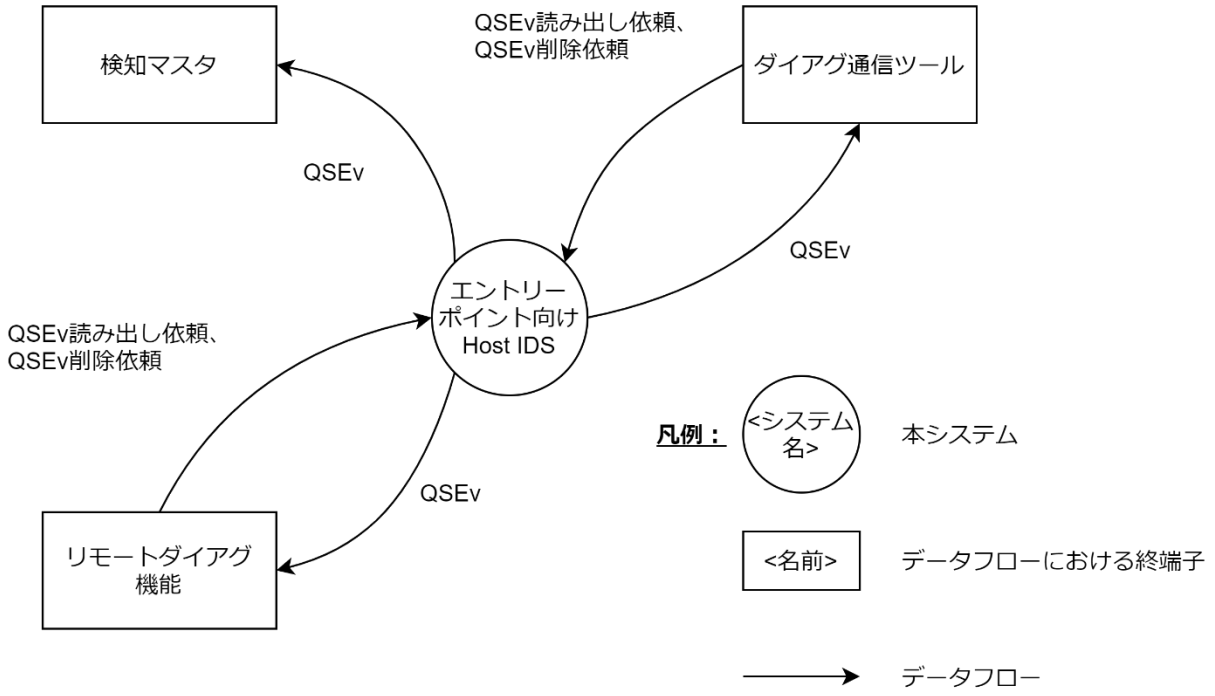

図 2-1：システムコンテキスト

2.2. システム動作概要

本システムは、表 2-1 に示す事象のいずれかが生じたとき、アクティビティ図（図 2-2）で示すとおりの動作をする。

表 2-1：本システムの動作始点となる事象

事象番号	本システムの動作始点となる事象
①	本システム搭載先 ECU・VM への侵入発生
②	本システムに保管されている QSEv の読み出し依頼
③	本システムに保管されている QSEv の削除依頼

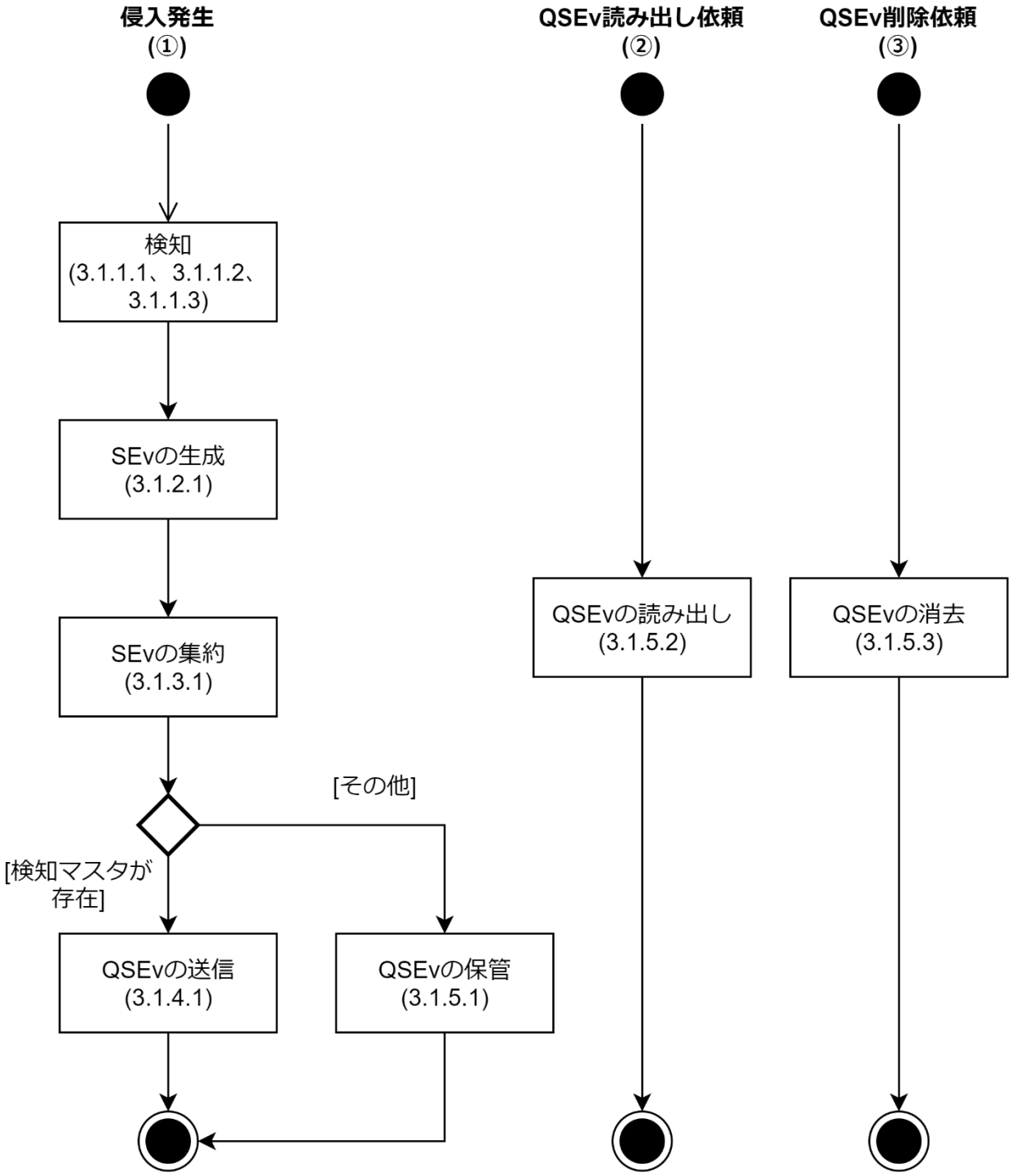
侵入発生
(①)
検知
(3.1.1.1、3.1.1.2、
3.1.1.3)
SEvの生成
(3.1.2.1)
SEvの集約
(3.1.3.1)
[その他]
[検知マスタが
存在]
QSEvの送信
(3.1.4.1)
QSEvの保管
(3.1.5.1)
QSEv読み出し依頼
(②)
QSEvの読み出し
(3.1.5.2)
QSEv削除依頼
(③)
QSEvの消去
(3.1.5.3)

図 2-2：本システム動作

2.3. 要求一覧

本書が定義する要求事項の一覧を表 2-2 に示す。

表 2-2：要求一覧

分類			要求 ID	ハードウェア関連要件
機能要求	検知機能	車外からの通信を終端する機能が持つセキュリティ機能の停止の検知	IDSHER_04101	No
		車外からの通信を終端する機能の不正動作の検知	IDSHER_01601	No
			IDSHER_01101	No
			IDSHER_01102	No
			IDSHER_01201	No
			IDSHER_01202	No
			IDSHER_01501	No
			IDSHER_01502	No
			IDSHER_01401	No
		エントリーポイント領域の CSP/PSP・ソフトウェアの改ざんの検知	IDSHER_02101	No
			IDSHER_02301	No
	SEv 生成機能	SEv の生成	IDSHER_07102	No
	QSEv 生成機能	SEv の集約	IDSHER_07103	No
	QSEv 送信機能	QSEv の送信	IDSHER_07108	No
			IDSHER_07208	No
	QSEv 保管機能	QSEv の保管	IDSHER_07109	No
			IDSHER_07111	No
		QSEv の読み出し	IDSHER_07110	No
		QSEv の消去	IDSHER_07204	No
品質要求			IDSHER_12201	No
設計値			IDSHER_03401	No
			IDSHER_03402	No

3. システム要求

本章では本システムのシステム要求を定義する。

3.1. 機能要求

本節では機能要求を定義する。

3.1.1. 検知機能

検知は大きく分けて三つの観点で行う。一つ目は、「車外からの通信を終端する機能が持つセキュリティ機能の停止の検知」（図 3-1 の No.1）である。二つ目は、「車外からの通信を終端する機能の不正動作の検知」（図 3-1 の No.2）の検知である。三つ目は、「エントリーポイント領域の CSP/PSP・ソフトウェアの改ざんの検知」（図 3-1 の No.3）である。

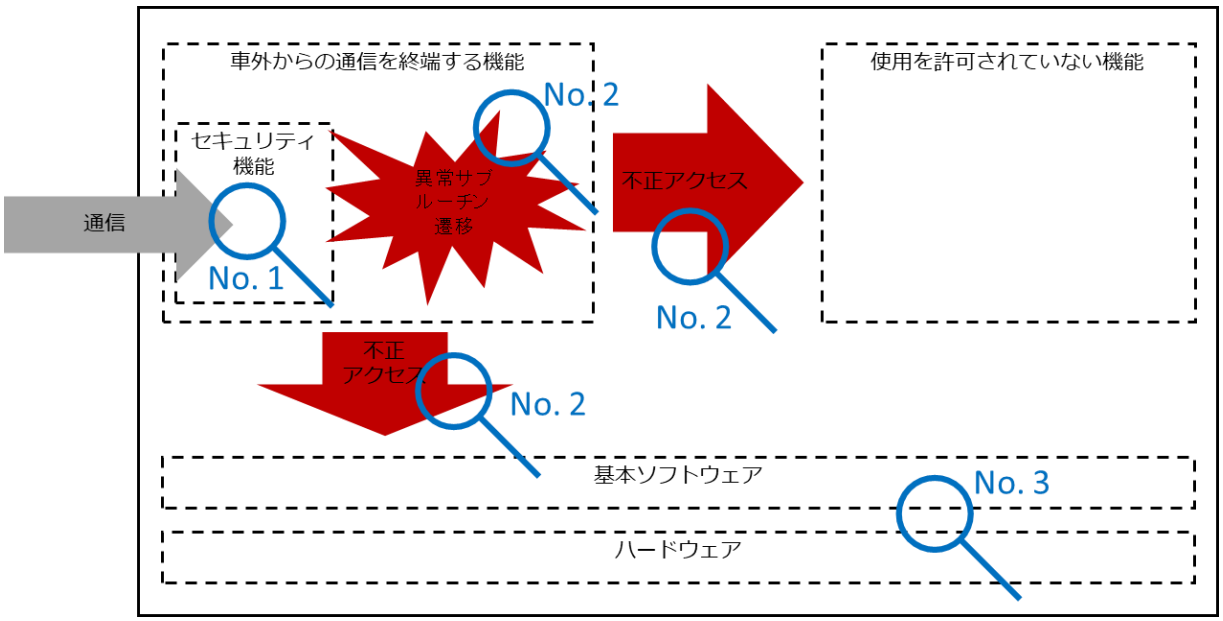

図 3-1：エントリーポイント ECU/VM のモデル

3.1.1.1. 車外からの通信を終端する機能が持つセキュリティ機能の停止の検知

3.1.1.1.1. 一層目防御機能の停止の検知

【要求事項：IDSHER_04101】

一層目防御機能を構成するソフトウェアが何らかの事象の発生を契機として動作するよう設計される場合に、本要求事項は適用される。当該事象が発生したにもかかわらず当該ソフトウェアが動作しなかったとき、検知機能は SEv 生成機能に異常を通知する必要がある。ただし、参照文書[10]の IDSHMR_04101 が適用される場合、各一層目防御機能を構成するソフトウェアの停止は本システムと多層分離機能向けホスト型侵入検知システムのどちらか一方で検知するだけでもよい。

※ここで何らかの事象の発生とは、データの送信/受信/利用、および、時間の経過、を含む。
<補足>
検知技術例：一層目防御機能の死活監視

3.1.1.2. 車外からの通信を終端する機能の不正動作の検知

3.1.1.2.1. 制御フローの異常検知

【要求事項：IDSHER_01601】
車外からの通信を終端する機能を構成するソフトウェアが複数のサブルーチンより構成される場合に、本要求事項は適用される。当該ソフトウェアの実行中に正規の制御フローとして起こりえないサブルーチン間での実行箇所の移動が行われたまたは試みられたとき、検知機能は SEv 生成機能に異常を通知する必要がある。
※ここで正規の制御フローとして起こりえないサブルーチン間での実行箇所の移動とは、実行箇所を指し示すデータの改ざんに起因して発生する事象を指し、コードの改ざんに起因して発生する事象を含まない。
<補足>
検知技術例：ソフトウェアの制御フロー監視

3.1.1.2.2. 不揮発性メモリへの不正アクセス検知

【要求事項：IDSHER_01101】
車外からの通信を終端する機能を構成するソフトウェアがファイルシステムを利用しパスによって ECU 内の不揮発性メモリにアクセスできる仕組みを持つ場合に、本要求事項は適用される。当該ソフトウェアが、パスによって、下記の操作のいずれかをその操作が許可されていないエントリーポイント領域の不揮発性メモリに対して行ったまたは試みたとき、検知機能は SEv 生成機能に異常を通知する必要がある。

- 読み出しアクセス
- 書き込みアクセス
- 実行アクセス
- 属性の変更

※ここで不揮発性メモリとは、MCU/SoC 内蔵やディスクリート型などの実装形態に依らず、不揮発性を持ってデータを保持することができる物理的または論理的なデバイスを指す。なお、HSM は IO(ペリフェラル)の一種であり、不揮発性メモリに該当しない。
※ここで属性とは、読み出しアクセス・書き込みアクセス・実行アクセスの可否を指す。
<補足>
検知技術例：ファイルアクセスの監視

【要求事項：IDSHER_01102】
車外からの通信を終端する機能を構成するソフトウェアがアドレスによって ECU 内の不揮発性メモリ

にアクセスできる仕組みを持つ場合に、本要求事項は適用される。当該ソフトウェアが、アドレスによって、下記の操作のいずれかをその操作が許可されていないエントリーポイント領域の不揮発性メモリに対して行ったまたは試みたとき、検知機能は SEv 生成機能に異常を通知する必要がある。

- 読み出しアクセス
- 書き込みアクセス
- 実行アクセス
- 属性の変更

※ここで不揮発性メモリとは、MCU/SoC 内蔵やディスクリート型などの実装形態に依らず、不揮発性を持ってデータを保持することができる物理的または論理的なデバイスを指す。なお、HSM は IO(ペリフェラル)の一種であり、不揮発性メモリに該当しない。

※ここで属性とは、読み出しアクセス・書き込みアクセス・実行アクセスの可否を指す。

<補足>

検知技術例：メモリアクセスの監視

3.1.1.2.3. 揮発性メモリへの不正アクセス検知

【要求事項：IDSHER_01201】

車外からの通信を終端する機能を構成するソフトウェアがファイルシステムを利用しパスによって ECU 内の揮発性メモリにアクセスできる仕組みを持つ場合に、本要求事項は適用される。当該ソフトウェアが、パスによって、下記の操作のいずれかをその操作が許可されていないエントリーポイント領域の揮発性メモリに対して行ったまたは試みたとき、検知機能は SEv 生成機能に異常を通知する必要がある。

- 読み出しアクセス
- 書き込みアクセス
- 実行アクセス
- 属性の変更

※ここで揮発性メモリとは、実装形態に依らず、揮発性を持ってデータを保持することができる物理的または論理的なデバイスを指す。

※ここで属性とは、読み出しアクセス・書き込みアクセス・実行アクセスの可否を指す。

<補足>

検知技術例：ファイルアクセスの監視

【要求事項：IDSHER_01202】

車外からの通信を終端する機能を構成するソフトウェアがアドレスによって ECU 内の揮発性メモリにアクセスできる仕組みを持つ場合に、本要求事項は適用される。当該ソフトウェアが、アドレスによって、下記の操作のいずれかをその操作が許可されていないエントリーポイント領域の揮発性メモリに対して行ったまたは試みたとき、検知機能は SEv 生成機能に異常を通知する必要がある。

- 読み出しアクセス

- 書き込みアクセス
- 実行アクセス
- 属性の変更

※ここで揮発性メモリとは、実装形態に依らず、揮発性を持ってデータを保持することができる物理的または論理的なデバイスを指す。
※ここで属性とは、読み出しアクセス・書き込みアクセス・実行アクセスの可否を指す。
<補足>
検知技術例：メモリアクセスの監視

3.1.1.2.4. IO(ペリフェラル)への不正アクセス検知

【要求事項：IDSHER_01501】
車外からの通信を終端する機能を構成するソフトウェアがファイルシステムを利用しパスによって ECU 内の IO(ペリフェラル)にアクセスできる仕組みを持つ場合に、本要求事項は適用される。当該ソフトウェアが、パスによって、下記の操作のいずれかをその操作が許可されていないエントリーポイント領域の IO(ペリフェラル)に対して行ったまたは試みたとき、検知機能は SEv 生成機能に異常を通知する必要がある。

- 読み出しアクセス
- 書き込みアクセス
- 属性の変更

※ここで IO(ペリフェラル)とは、実装形態に依らず、データの入出力ができる物理的または論理的なデバイスを指す。
※ここで属性とは、読み出しアクセス・書き込みアクセスの可否を指す。
<補足>
検知技術例：ファイルアクセスの監視

【要求事項：IDSHER_01502】
車外からの通信を終端する機能を構成するソフトウェアがアドレスによって ECU 内の IO(ペリフェラル)にアクセスできる仕組みを持つ場合に、本要求事項は適用される。当該ソフトウェアが、アドレスによって、下記の操作のいずれかをその操作が許可されていないエントリーポイント領域の IO(ペリフェラル)に対して行ったまたは試みたとき、検知機能は SEv 生成機能に異常を通知する必要がある。

- 読み出しアクセス
- 書き込みアクセス
- 属性の変更

※ここで IO(ペリフェラル)とは、実装形態に依らず、データの入出力ができる物理的または論理的なデバイスを指す。
※ここで属性とは、読み出しアクセス・書き込みアクセスの可否を指す。
<補足>

検知技術例：メモリアクセスの監視

3.1.1.2.5. 機能の不正使用検知

【要求事項：IDSHER_01401】

車外からの通信を終端する機能を構成するソフトウェアが、使用を許可されていないエントリーポイント領域の機能を使用したまたは試みたとき、検知機能は SEv 生成機能に異常を通知する必要がある。

<補足>

検知技術例：システムコールの使用監視、Identity and Access Management

3.1.1.3. エントリーポイント領域の CSP/PSP・ソフトウェアの改ざんの検知

3.1.1.3.1. CSP/PSP の改ざん検知

【要求事項：IDSHER_02101】

エントリーポイント領域が CSP/PSP に該当するデータを不揮発性メモリに持つ場合に、本要求事項は適用される。当該データの使用時に当該データが改ざんされているとき、検知機能は SEv 生成機能に異常を通知する必要がある。

※ここで不揮発性メモリとは、MCU/SoC 内蔵やディスクリート型などの実装形態に依らず、不揮発性を持ってデータを保持することができる物理的または論理的なデバイスを指す。なお、HSM は IO(ペリフェラル)の一種であり、不揮発性メモリに該当しない。

※ここで使用時とは、不揮発性メモリに格納されている CSP/PSP を揮発性メモリまたは HSM に展開するとき、を含む。

<補足>

検知技術例：CSP/PSP 使用前の完全性/真正性検証

3.1.1.3.2. ソフトウェアの改ざん検知

【要求事項：IDSHER_02301】

エントリーポイント領域に配置される機能を構成するソフトウェアの起動時に下記のいずれかが改ざんされているとき、検知機能は SEv 生成機能に異常を通知する必要がある。ここで、改ざん検知は完全性が保証された領域から行われる必要がある。ただし、参照文書[10]の IDSHMR_01601 が適用される場合、本システムと多層分離機能向けホスト型侵入検知システムのどちらか一方がソフトウェアの改ざんを検知するだけでもよい。

- 当該ソフトウェアのコード
- 当該ソフトウェアの振舞いを制御するデータ

<補足>

検知技術例：セキュアブート、未許可ソフトウェアの起動検知

3.1.2. SEv 生成機能

3.1.2.1. SEv の生成

【要求事項：IDSHER_07102】

SEv 生成機能は、検知機能から異常が通知されるたびに、SEv（表 3-1）を生成し QSEv 生成機能に通知する必要がある。ここで、Event Definition ID と Context Data は、表 3-2 に従う必要がある。また、Context Data は、ビッグエンディアンにて内容が設定される必要がある。

表 3-1：異常通知により生成される SEv

Field Name	Length	Description
Security Event ID	16 bit	QSEv 生成機能が QSEv に設定する Event Definition ID と Sensor Instance ID の組み合わせを一意に識別するための情報を設定する。 - Event Definition ID は、異常を検知した検知機能の要求 ID に基づいて設定される（表 3-2）。 - Sensor Instance ID は、固定値 0 である。 <補足> 本フィールドは、AUTOSAR CP では IdsMInternalEventId 型の引数として実現される。
Context Data Size	8 bit or 32 bit	Context Data のバイト長。ソフトウェアの設計者等が Event Definition ID 毎にその Context Data の長さに応じてどちらか一方を選択する。
Context Data	Variable length	検知された異常についての情報を格納するバイト列であり、異常を通知した検知機能の要求 ID に基づいて設定する。また、その異常が発生した時点でのダイアグタイムスタンプ等も設定する。

表 3-2：要求 ID ごとの Event Definition ID と Context Data

Corresponding Requirement ID	Event Definition ID	Context Data		
		Field Name	Length [Byte]	Description
IDSHER_04101	0x8110	Format Version	1	Fixed value: 0x01
		Diagnostic timestamp (※1)	7	ダイアグタイムスタンプのトリップカウンタと時間カウンタ
		Diagnostic clock Information (※1)	6	ダイアグタイムスタンプの時刻情報
		Diagnostic vehicle odometer information (※1)	4	ダイアグタイムスタンプの累積走行距離情報
		Software ID Size	1	Software ID のバイト長(0~16)

		Software ID	Variable length	技術制約により取得困難な場合(※2)を除き、停止したソフトウェアを一意に識別するための情報(※3)を記録すること。 （例）当該ソフトウェアの実行ファイル名、当該ソフトウェアに紐づいた識別番号など
IDSHER_01601	0x8120	Format Version	1	Fixed value: 0x01
		Diagnostic timestamp (※1)	7	ダイアグタイムスタンプのトリップカウンタと時間カウンタ
		Diagnostic clock information (※1)	6	ダイアグタイムスタンプの時刻情報
		Diagnostic vehicle odometer information (※1)	4	ダイアグタイムスタンプの累積走行距離情報
		Software ID Size	1	Software ID のバイト長(0~16)
		Software ID	Variable length	技術制約により取得困難な場合(※2)を除き、制御フローの異常が発生したソフトウェアを一意に識別するための情報(※3)を記録すること。 （例）当該ソフトウェアの実行ファイル名、当該ソフトウェアに紐づいた識別番号など
		Subroutine ID Size	1	Subroutine ID のバイト長(0~16)
		Subroutine ID	Variable length	技術制約により取得困難な場合(※2)を除き、正規ではない実行箇所の移動が行われたサブルーチンを一意に識別するための情報(※3)を記録すること。 （例）当該サブルーチン名、当該サブルーチンに紐づいた識別番号など
IDSHER_01101 IDSHER_01102 IDSHER_01201 IDSHER_01202 IDSHER_01501 IDSHER_01502	0x8130	Format Version	1	Fixed value: 0x01
		Diagnostic timestamp (※1)	7	ダイアグタイムスタンプのトリップカウンタと時間カウンタ
		Diagnostic clock information (※1)	6	ダイアグタイムスタンプの時刻情報
		Diagnostic vehicle odometer information (※1)	4	ダイアグタイムスタンプの累積走行距離情報
		Software ID Size	1	Software ID のバイト長(0~16)

		Software ID	Variable length	技術制約により取得困難な場合(※2)を除き、不正アクセスを行ったソフトウェアを一意に識別するための情報(※3)を記録すること。 （例）当該ソフトウェアの実行ファイル名、当該ソフトウェアに紐づいた識別番号など
		Memory or IO ID Size	1	Memory or IO ID のバイト長(0~16)
		Memory or IO ID	Variable length	技術制約により取得困難な場合(※2)を除き、不正アクセスが行われたメモリまたは IO(ペリフェラル)一意に識別するための情報(※3)を記録すること。 （例）当該メモリのアドレス、当該 IO のデバイス名、当該 IO に紐づいた識別番号など
IDSHER_01401	0x8140	Format Version	1	Fixed value: 0x01
		Diagnostic timestamp (※1)	7	ダイアグタイムスタンプのトリップカウンタと時間カウンタ
		Diagnostic clock information (※1)	6	ダイアグタイムスタンプの時刻情報
		Diagnostic vehicle odometer information (※1)	4	ダイアグタイムスタンプの累積走行距離情報
		Software ID Size	1	Software ID のバイト長(0~16)
		Software ID	Variable length	技術制約により取得困難な場合(※2)を除き、機能の不正使用を行ったソフトウェアを一意に識別するための情報(※3)を記録すること。 （例）当該ソフトウェアの実行ファイル名、当該ソフトウェアに紐づいた識別番号など
		Function ID Size	1	Function ID のバイト長(0~16)
		Function ID	Variable length	技術制約により取得困難な場合(※2)を除き、不正使用された機能を一意に識別するための情報(※3)を記録すること。 （例）当該機能名、当該機能に紐づいた識別番号など
IDSHER_02101 IDSHER_02301	0x8150	Format Version	1	Fixed value: 0x01
		Diagnostic timestamp (※1)	7	ダイアグタイムスタンプのトリップカウンタと時間カウンタ

		Diagnostic clock information (※1)	6	ダイアグタイムスタンプの時刻情報
		Diagnostic vehicle odometer information (※1)	4	ダイアグタイムスタンプの累積走行距離情報
		CSP/PSP or Software ID Size	1	CSP/PSP or Software ID のバイト長(0~16)
		CSP/PSP or Software ID	Variable length	技術制約により取得困難な場合(※2)を除き、改ざんされた CSP/PSP またはソフトウェアを一意に識別するための情報(※3)を記録すること。 （例）当該 CSP/PSP 名、当該ソフトウェアの実行ファイル名、当該ソフトウェアに紐づいた識別番号など

(※1) 情報の詳細は参照文書[8]を参照

(※2) 取得するために、OS や BSW の改修が必要となる場合等を想定

(※3) 開発元(ECU 設計部署やサプライヤ等)が発生原因や発生箇所を特定するために有効な情報を定義する

3.1.3. QSEv 生成機能

3.1.3.1. SEv の集約

【要求事項：IDSHER_07103】

QSEv 生成機能は、参照文書[2]に従って、通知される SEv を Security Event ID ごとに集約し QSEv を生成する必要がある。Security Event ID ごとの集約の設定は【要求事項：IDSHER_03402】で定義する。

3.1.4. QSEv 送信機能

3.1.4.1. QSEv の送信

【要求事項：IDSHER_07108】

検知マスタ(参照文書[11])がいずれかの ECU に存在する場合に、本要求事項は適用される。QSEv 生成機能が QSEv を生成する度に、QSEv 送信機能は、図 3-2 に示す構造のデータを、下記に示す領域へ設定して通信フレームを生成し、それを検知マスタへ送信する必要がある。

・自 ECU が、CAN 通信または CAN FD 通信を用いて、QSEv を送信する場合：
　Data Label が QSEV_DATA_[ECU ノード名(※1)]で定義された領域
・自 ECU が、Ethernet 通信を用いて、QSEv を送信する場合：
　Property が[ECU ノード名(※1)]QsevData で定義された領域

Protocol Version	Protocol Header	IdsM Instance ID	Sensor Instance ID	Event Definition ID	Count	Reserved	Context Data (※2)
msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb

図 3-2：データ構造

（※1）[ECU ノード名]は、通信仕様中の自 ECU を示すノード名に置換すること。該当する Data Label 又は Property が存在しない場合は、本書の発行元部署に相談すること。
（※2）CAN FD 通信及び Ethernet 通信に適用される。CAN 通信は適用対象外。

【要求事項：IDSHER_07208】
QSEv 送信機能が、QSEv を検知マスタへ送信する場合に本要求は適用される。QSEv 送信機能による QSEv 送信がネットワークの WakeUp 要因もしくは Sleep 阻害要因となる場合、QSEv 送信機能は QSEv を送信してはならない。
<補足>
QSEv の送信が、バッテリ上がりの原因となることを避けるため。

3.1.5. QSEv 保管機能

3.1.5.1. QSEv の保管

【要求事項：IDSHER_07109】
検知マスタがいずれの ECU にも存在しない場合に、本要求事項は適用される。QSEv 保管機能は、QSEv 生成機能が生成する最新[NumberOfQSEvs]個の QSEv を、Event Definition ID 毎に不揮発性メモリに保管する必要がある。ただし、QSEv 保管機能は、不意のリセット（バッテリ瞬断、低電圧等）時に QSEv を保管しなくてもよい。なお、QSEv 保管機能は、不揮発性メモリの書き込み回数上限を考慮し設計される必要がある。

<補足>
検知マスタがいずれかの ECU に存在する場合には、QSEv を保管するかは任意である。
不揮発性メモリの書き込み回数上限を考慮した設計の例として、IG-ON 中は RAM 領域に QSEv をバッファリングし、IG-OFF 時に不揮発性メモリに書き込む設計が挙げられる。

【要求事項：IDSHER_07111】
QSEv 保管に関する UserDefMemoryDTC および DID は表 3-3、表 3-4、表 3-5 に従う必要がある。
UserDefMemoryDTC および DID は以下の方針で定義している。
・UserDefMemoryDTC：Event Definition ID ごとに定義

・DID：QSEv 全体で一つ定義、かつ、全 Event Definition ID に対して共通で一つ定義

表 3-3：UserDefMemoryDTC 関連情報

UserDefMemoryDTC	FTB	対応 Event Definition ID	Memory Selection
U2B21	0x00	0x8110	0x14
U2B22	0x00	0x8120	0x14
U2B23	0x00	0x8130	0x14
U2B24	0x00	0x8140	0x14
U2B25	0x00	0x8150	0x14

表 3-4：QSEv 保管に関する DID

DID	Data	Length [Bit]
0xA910	Protocol Version	4
	Protocol Header	4
	IdsM Instance ID	10
	Sensor Instance ID	6
	Event Definition ID	16
	Count	16
	Reserved	8
	Context Data (※1)	Variable Length

(※1) CAN FD 通信及び Ethernet 通信に適用される。CAN 通信は適用対象外。

表 3-5：QSEv 保管データ例(Event Definition ID:0x8110 の QSEv を 5 件保管)

UserDefMemoryDTC	FTB	UserDefDTC SnapshotRecordNumber	Description
U2B21	0x00	0x01	最新[NumberOfQSEvs]個の QSEv のうち、最も古い QSEv (DID: 0xA910)
		0x02	最新[NumberOfQSEvs]個の QSEv のうち、2 番目に古い QSEv (DID: 0xA910)
		0x03	最新[NumberOfQSEvs]個の QSEv のうち、3 番目に古い QSEv (DID: 0xA910)
		0x04	最新[NumberOfQSEvs]個の QSEv のうち、4 番目に古い QSEv (DID: 0xA910)
		0x05	最新[NumberOfQSEvs]個の QSEv のうち、最も新しい QSEv (DID: 0xA910)

3.1.5.2. QSEv の読み出し

【要求事項：IDSHER_07110】

QSEv が不揮発性メモリに保管される場合に、本要求事項は適用される。不揮発性メモリに保管される QSEv は、オフボードクライアントおよびオンボードクライアントからダイアグ通信 SID 0x19 (Sub Function 0x17/0x18)で読み出しできる必要がある。ただし、前述の QSEv が一時的に揮発性メモリ上に置かれている場合、揮発性メモリ上のそれら QSEv が読み出される必要がある。

ダイアグ通信の詳細は、参照文書[9]を参照。

3.1.5.3. QSEv の消去

【要求事項：IDSHER_07204】

QSEv が不揮発性メモリに保管される場合に、本要求事項は適用される。不揮発性メモリに保管される QSEv は、オフボードクライアントからダイアグ通信 SID 0x14 (QSEv 出力用 MemorySelection 0x14)で消去できる必要がある。

ダイアグ通信の詳細は、参照文書[9]を参照。

3.2. 品質要求

本節では品質要求を定義する。

【要求事項：IDSHER_12201】

検知機能を除く本システムの機能及びそれが生成する QSEv は車外からの通信を終端する機能から改ざんされないように設計する必要がある。

<補足>

例えば、以下の全 4 項目をもって本要求を満たすことができる。

1) 検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）がレジスタを利用する場合、検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）が使用するレジスタは、車外からの通信を終端する機能から書き換えアクセス禁止とすること。

2) 検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）がメモリを利用する場合、メモリについて、検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）が使用する領域は、下記の例外に該当しない限り、車外からの通信を終端する機能から書き換えアクセス禁止とすること。
※例外
仮想的な CAN 通信インターフェース、または、仮想的な Ethernet 通信インターフェースにおいて、検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）と検知機能（3.1.1）との間で授受されるデータのみを格納する領域
※例外に該当するメモリ領域の例
仮想的な CAN 通信インターフェースにおいて、検知機能（3.1.1）から検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）へのデータを格納する領域

3) 検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）が HSM を利用する場合に本要求事項は適用される。検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）が使用する HSM インターフェースからの出力情報(暗号結果、MAC 値など)は、車外からの通信を終端する機能から書き換えアクセス禁止とすること。

HSM インターフェースの物理的な分離は必ずしも要求されない。例えば、1)や 2)を満たすことによって、車外からの通信を終端する機能から HSM インターフェースが出力する情報への書き換えアクセスを禁止できるのであれば、それをもって車外からの通信を終端する機能からの書き換えアクセス禁止を実現してもよい。

4) 検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）が車載通信インターフェースを利用する場合に本要求事項は適用される。検知機能（3.1.1）以外の機能（3.1.2、3.1.3、3.1.4、3.1.5）が使用する車載通信インターフェース情報は、車外からの通信を終端する機能から書き換えアクセス禁止とすること。

車載通信インターフェースの物理的な分離は必ずしも要求されない。例えば、1)や 2)を満たすことによって、車外からの通信を終端する機能から車載通信インターフェース情報への書き換えアクセスを禁止できるのであれば、それをもって車外からの通信を終端する機能からの書き換えアクセス禁止を実現してもよい。

3.3. 制約

無し

3.4. 設計値

本節では設計値を定義する。

【要求事項：IDSHER_03401】
本節で定義する設計値は各要求で定められる条件下で設定変更可能である必要がある。

【要求事項：IDSHER_03402】
QSEv 生成・保管は表 3-6 の設計値を用いて行われる必要がある。なお、単位などの設計値に関する条件は　　表 3-7 と表 3-8 に従う必要がある。

表 3-6：QSEv 生成・保管の設計値

名称	Event Definition ID	Sensor Instance ID	設定値（※1）
IdsMEventAggregationTimeInterval	0x8110	0x0	0.3
	0x8120	0x0	0.3
	0x8130	0x0	0.3
	0x8140	0x0	0.3
	0x8150	0x0	0.3
IdsMContextDataSourceSelector	0x8110	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8120	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8130	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8140	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8150	0x0	IDSM_FILTERS_CTX_USE_FIRST
NumberOfQSEvs	0x8110	0x0	5
	0x8120	0x0	5
	0x8130	0x0	5
	0x8140	0x0	5
	0x8150	0x0	5

表 3-7：QSEv 生成設計値メタ情報

名称	単位	型	下限値	上限値
IdsMEventAggregationTimeInterval (※2)	sec	EcucFloatParam Def	0.05	10.00

IdsMContextDataSourceSelector	-	EcucEnumerationParamDef	IDSM_FILTERS_CTX_USE_FIRST	IDSM_FILTERS_CTX_USE_LAST

※１：IdsMEventAggregationTimeInterval および IdsMContextDataSourceSelector の設定値がハイフン「-」であるのは集約を行わないことを意味する。

※２：設定値列に記載の値と同じ値を設定できない場合、記載の設定値より小さく、かつ、設定可能な設計値のうち、最大の値が設定される必要がある。

表 3-8：QSEv 保管設計値メタ情報

名称	説明	単位	下限値	上限値
NumberOfQSEvs	QSEv の保管件数	-	0	10

Revision history

Version	Change	Date	Reviser
a00-00-a	First version issued	2021/04/05	46F 4G Inagaki
a00-00-b	Translation into English added	2021/05/14	46F 4G Inagaki
a00-01-a	Requirements fleshed, readability improved	2021/08/06	46F 4G Takeyama
a00-02-a	Heartbeat SEv creation deleted	2021/12/03	46F 4G Takeyama
a00-03-a	- References added - T.B.D. deleted - Requirements about QSEv storing modified - IDSHER_07208 added - Detection method example of IDSHER_02101 modified - IDSHER_04101 modified - IDSHER_02301 modified - IDSHER_07102 modified - IDSHER_07108 modified	2022/02/03	46F 4G Takeyama
a00-04-a	- Hardware-related requirement added in List of requirements - IDSHER_02301 requirement modified - IDSHER_04101 requirement modified - IDSHER_07102 description of Context Data clarified - IDSHER_07108 requirement modified - IDSHER_07109 QSEv storing requirement modified - IDSHER_07111 UserDefineDTC and DID requirement added - IDSHER_07110 SID for QSEv read clarified - IDSHER_07202 deleted - - IDSHER_07204 SID for QSEv deletion clarified	2022/04/29	46F 4G Takeyama
a00-04-b	- IDSHER_07111 UserDefMemoryDTC value modified - IDSHER_07110 diagnostic specification reference added - IDSHER_07204 diagnostic specification reference added	2022/05/20	46F 4G Takeyama
a00-04-c	- Table 2-2 Editorial errors corrected - IDSHER_12201 Editorial errors corrected - IDSHER_07109 The part of the note moved to requirement	2022/06/09	46F 4G Takeyama

Table of contents

1. Introduction

1.1. Purpose of this document

The goal of Host-based IDS for Entry Point (hereinafter referred to as *this system*) is to detect and log intrusion into an entry point and the attempt. Log recorded by this system is used to realize the *detection* function in the framework for cybersecurity (Reference [1]) defined by National Institute of Standards and Technology (hereinafter referred to as *NIST*). The purpose of this document is to define the requirements of this system.

1.2. Target

This document is allocated to entry-point ECUs/VMs specified by another document.

1.3. Prerequisites

None

1.4. Description of requirements

We describe requirements as [Requirement: **] in this document where <Note> means just a supplementary note.

1.5. Input documents

Inputs documents, and references are shown in this section. If the specification of the ECU specifies the version of the reference, follow it.

1.5.1. Input documents

Table 1-1: Input documents

No.	Document name	Ver.
1	Vehicle Cyber Security Concept Definition Document	Latest

1.5.2. References

Table 1-2: References

No.	Document name	Ver.

1	Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, National Institute of Standards and Technology, April 16, 2018, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11	1.1
2	Requirements specification of QSEv creation	-
3	AUTOSAR_PRS_IntrusionDetectionSystem	R20-11
4	AUTOSAR_SWS_IntrusionDetectionSystemManager	R20-11
5	AUTOSAR_SWS_AdaptiveIntrusionDetectionSystemManager	R20-11
6	Terms and Definitions related to Vehicle Cybersecurity and Privacy	-
7	Deleted	-
8	Time Stamp requirement specification	-
9	TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	-
10	Requirements Specification of Host-based IDS for Multi-layered Separation Function	-
11	Requirements Specification of Intrusion Detection Master	-

1.6. Glossary

We define terms used in this document. Since some parts of this system are expected to be implemented in accordance with AUTOSAR requirements, we use terms defined by AUTOSAR. See [3], [4] and [5] for the terms. See [6] for the other terms.

Table 1-3: Glossary

Term	Meaning
-	-

2. Requirement overview

2.1. System context

We show the system context with DFD (Figure 2-1). The circle means this system, and the rectangles mean subjects transmitting information or services.

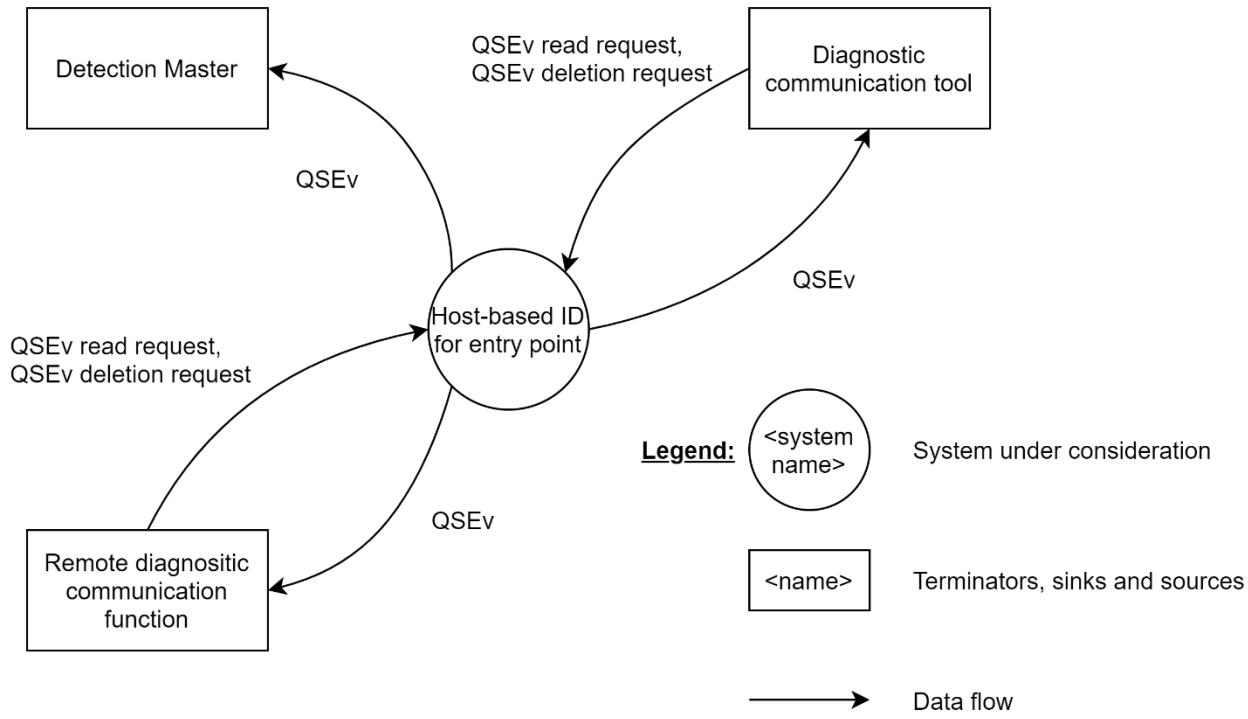

Figure 2-1: System context

2.2. System operation overview

This system operates as the UML activity diagram (Figure 2-1) when one of these events shown in (Table 2-1) happens.

Table 2-1: Events to start the operation

Event No.	Event that can be the starting point of the operation
①	Occurrence of intrusion on ECUs/VMs where this system is implemented.
②	Request to read QSEvs stored by this system
③	Request to delete QSEvs stored by this system

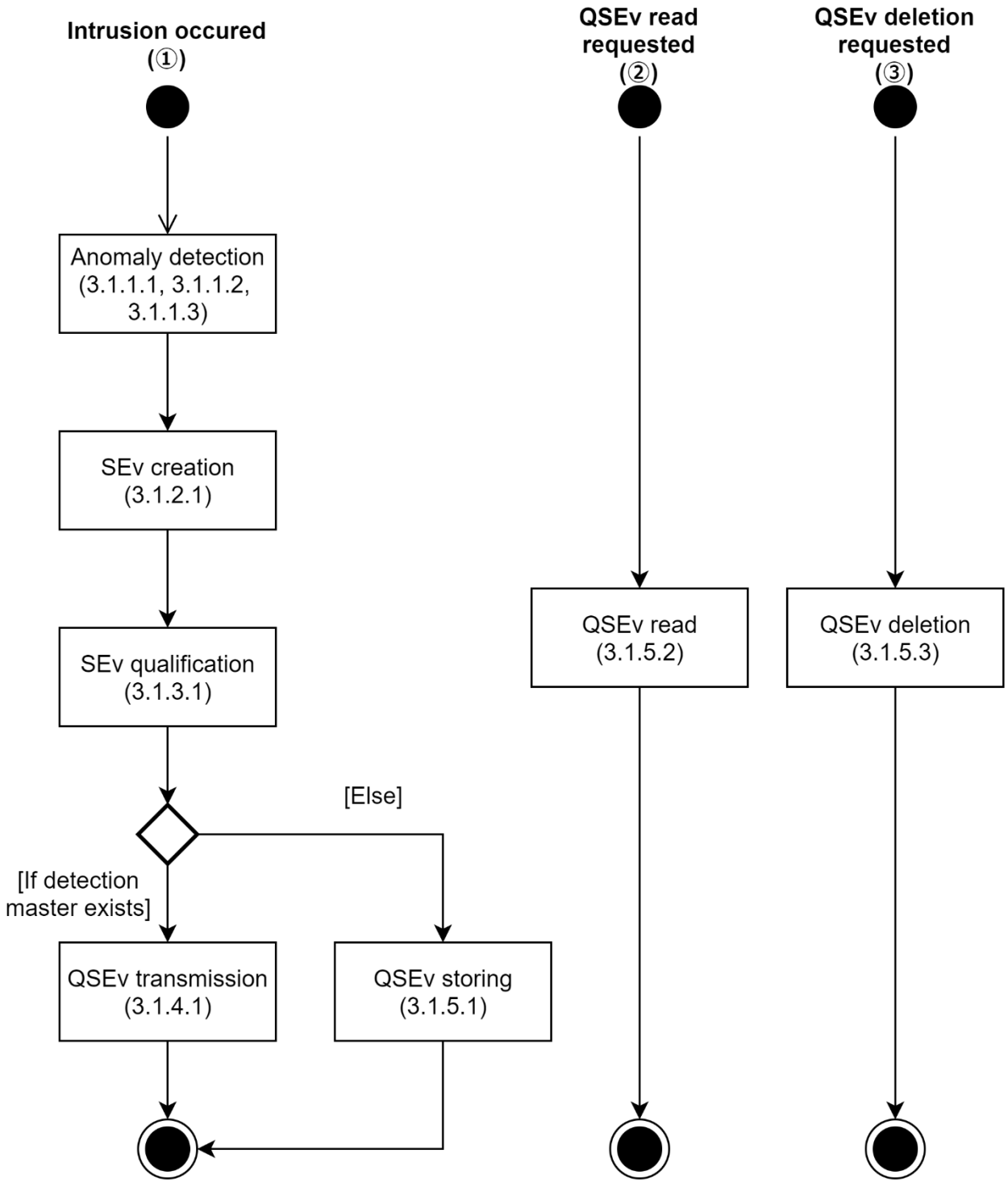

Figure 2-2: System operation

2.3. List of requirements

We show the list of all requirements defined in this document (Table 2-2).

Table 2-2: List of requirements

Category			Requirement ID	Hardware-related requirement
Functional requirements	Detection function	Detection of abort of a security function of a function to terminate communication from Out-Car	IDSHER_04101	No
		Detection of illegal operation of a function to terminate communication from Out-Car	IDSHER_01601	No
			IDSHER_01101	No
			IDSHER_01102	No
			IDSHER_01201	No
			IDSHER_01202	No
			IDSHER_01501	No
			IDSHER_01502	No
			IDSHER_01401	No
		Detection of manipulation of CSP/PSP or software in an entry point region	IDSHER_02101	No
			IDSHER_02301	No
	SEv creation function	SEv creation	IDSHER_07102	No
	QSEv creation function	SEv qualification	IDSHER_07103	No
	QSEv transmission function	QSEv transmission	IDSHER_07108	No
			IDSHER_07208	No
	QSEv storing function	QSEv storing	IDSHER_07109	No
			IDSHER_07111	No
		QSEv read	IDSHER_07110	No
		QSEv deletion	IDSHER_07204	No
Quality requirements			IDSHER_12201	No
Parameters			IDSHER_03401	No
			IDSHER_03402	No

3. System requirements

We define system requirements in this chapter.

3.1. Functional requirements

We define functional requirements in this section.

3.1.1. Detection function

There are mainly three kinds of detection. The first one is *detection of abort of security function of function to terminate communication from Out-Car* (No. 1 of Figure 3-1). The second one is *detection of illegal operation of function to terminate communication from Out-Car* (No. 2 of Figure 3-1). The third one is *detection of manipulation of CSP/PSP or Software in an entry point region* (No. 3 of Figure 3-1).

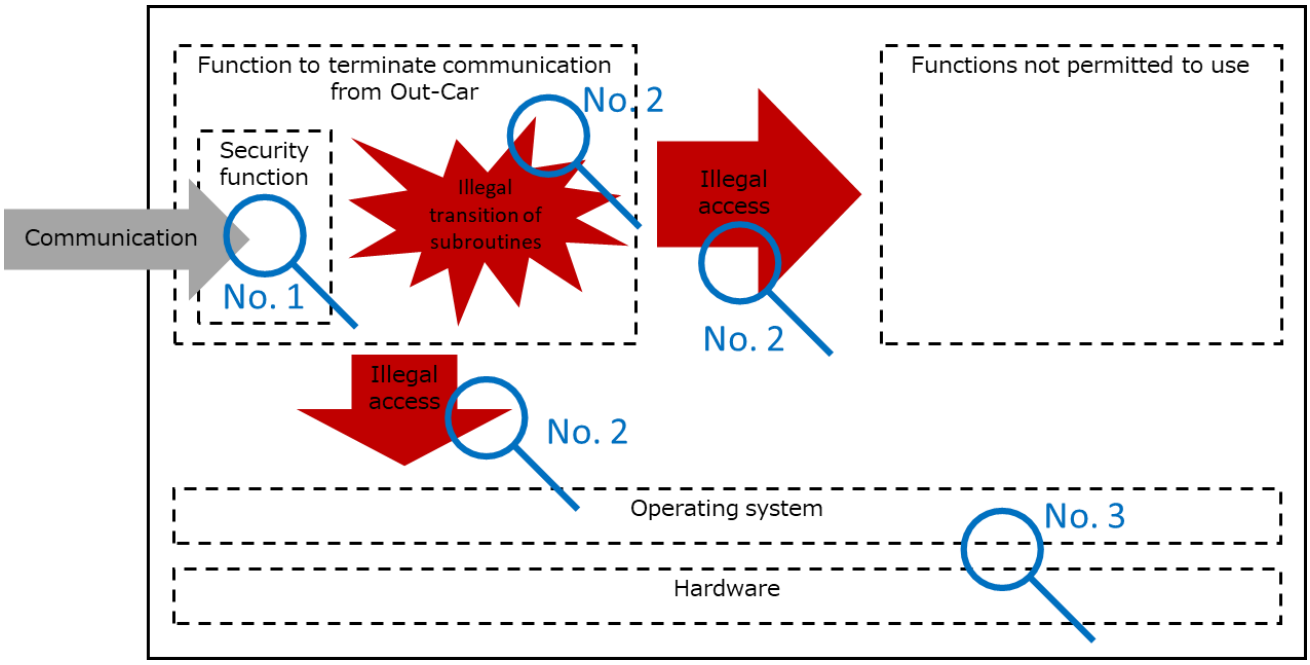

Figure 3-1: Entry-point ECU/VM model

3.1.1.1. Detection of abort of security function in function to terminate communication from Out-Car

3.1.1.1.1. Detection of abort of the first layer defense function

[Requirement: IDSHER_04101]

If software composing the first layer defense function is designed to operate when an *event* (*1) occurs, this requirement shall be allocated. If such software does not operate although the event occurs, a detection function shall notify a SEv creation function of the anomaly. However, if

IDSHMR_04101 in [10] is allocated, both this system and Host-based IDS for Multi-layered Separation Function does not have to detect abort of software comprising the first layer defense function.

*1: *event*s include transmission/reception/use of data, and elapse.

<Note>

Detection method example: monitoring whether the first layer defense function is working or not

3.1.1.2. Detection of illegal operation of function to terminate communication from Out-Car

3.1.1.2.1. Detection of abnormal control flow

[Requirement: IDSHER_01601]

If software composing a function to terminate communication from Out-Car consists of subroutines, this requirement shall be allocated. If a *transition between subroutines that shall not occur in an authenticate flow* (*1) occurs, or is attempted, a detection function shall notify a SEv creation function the anomaly.

*1: *transition*s *between subroutines that shall not occur in an authenticate flow* do not include events caused by manipulation of code but include events caused by manipulation of data indicating point of execution.

<Note>

Detection method example: monitoring flow of software

3.1.1.2.2. Detection of illegal access to non-volatile memory

[Requirement: IDSHER_01101]

If software composing a function to terminate communication from Out-Car has architecture so that it can access to *non-volatile memory* (*1) in a ECU by a path of a file system, this requirement shall be allocated. If the software performs any operation shown below by a path to *non-volatile memory* in the entry point region where the operation is not permitted to be performed, or attempts to do so, a detection function shall notify a SEv creation function of the anomaly.

- Read access
- Write access
- Execute access
- Change *attribute* (*2)

*1: *non-volatile memory* means physical or logical devices that can keep data non-volatilely, regardless of implementation such as memory embedded in MCU/SoC or discrete memory. Note HSM is not non-volatile memory but IO (peripheral).

*2: *Attribute* means whether read/write/execute access is permitted or not.

<Note>

Detection method example: Monitoring file access

[Requirement: IDSHER_01102]

If software composing a function to terminate communication from Out-Car has architecture so that it can access to *non-volatile memory* (*1) in a ECU by an address, this requirement shall be allocated. If the software performs any operation shown below by a path to *non-volatile memory* in the entry point region where the operation is not permitted to be performed, or attempts to do so, a detection function shall notify a SEv creation function of the anomaly.

- Read access
- Write access
- Execute access
- Change *attribute* (*2)

*1: *non-volatile memory* means physical or logical devices that can keep data non-volatilely, regardless of implementation such as memory embedded in MCU/SoC or discrete memory. Note HSM is not non-volatile memory but IO (peripheral).

*2: *attribute* means whether read/write/execute access is permitted or not.

<Note>

Detection method example: Monitoring memory access

3.1.1.2.3. Detection of illegal access to volatile memory

[Requirement: IDSHER_01201]

If software composing a function to terminate communication from Out-Car has architecture so that it can access to *volatile memory* (*1) in a ECU by a path of a file system, this requirement shall be allocated. If the software performs any operation shown below by a path to *volatile memory* in the entry point region where the operation is not permitted to be performed, or attempts to do so, a detection function shall notify a SEv creation function of the anomaly.

- Read access
- Write access
- Execute access
- Change *attribute* (*2)

*1: *volatile memory* means physical or logical devices that can keep data volatilely, regardless of implementation.

*2: *attribute* means whether read/write/execute access is permitted or not.

<Note>

Detection method example: Monitoring file access

[Requirement: IDSHER_01202]

If software composing a function to terminate communication from Out-Car has architecture so that it can access to *volatile memory* (*1) in a ECU by an address, this requirement shall be allocated. If the software performs any operation shown below by a path to *volatile memory* in the entry point region where the operation is not permitted to be performed, or attempts to do so, a detection function shall notify a SEv creation function of the anomaly.

- Read access
- Write access
- Execute access
- Change *attribute* (*2)

*1: *volatile memory* means physical or logical devices that can keep data volatilely, regardless of implementation.

*2: *attribute* means whether read/write/execute access is permitted or not.

<Note>

Detection method example: Monitoring memory access

3.1.1.2.4. Detection of illegal access to IO (peripheral)

[Requirement: IDSHER_01501]

If software composing a function to terminate communication from Out-Car has architecture so that it can access to *IO (peripheral)* (*1) in a ECU by a path of a file system, this requirement shall be allocated. If the software performs any operation shown below by a path to *IO (peripheral)* memory in the entry point region where the operation is not permitted to be performed, or attempts to do so, a detection function shall notify a SEv creation function of the anomaly.

- Read access
- Write access
- Change *attribute* (*2)

*1: *IO (peripheral)* means physical or logical devices that can input/out data, regardless of implementation.

*2: *attribute* means whether read/write access is permitted or not.

<Note>

Detection method example: Monitoring file access

[Requirement: IDSHER_01502]

If software composing a function to terminate communication from Out-Car has architecture so that it can access to *IO (peripheral)* (*1) in a ECU by an address, this requirement shall be allocated. If the software performs any operation shown below by a path to *IO (peripheral)* in the entry point region where the operation is not permitted to be performed, or attempts to do so, a detection function shall notify a SEv creation function of the anomaly.

- Read access
- Write access
- Change *attribute* (*2)

*1: *IO (peripheral)* means physical or logical devices that can input/out data, regardless of implementation.

*2: *attribute* means whether read/write access is permitted or not.

<Note>

Detection method example: Monitoring memory access

3.1.1.2.5. Detection of illegal usage of function

[Requirement: IDSHER_01401]

If software composing a function to terminate communication from Out-Car uses a function unpermitted to use in the entry point region, or attempts to do so, a detection function shall notify a SEv creation function of the anomaly.

<Note>

Detection method example: Monitoring system call, Identity and Access Management

3.1.1.3. Detection of manipulation of CSP/PSP or software in entry point region

3.1.1.3.1. Detection of manipulation of CSP/PSP

[Requirement: IDSHER_02101]

If an entry point region has data fallen into CSP/PSP in *non-volatile memory* (*1), this requirement shall be allocated. If the data is manipulated *at the usage of it* (*2), a detection function shall notify a SEv creation function of the anomaly.

*1: *non-volatile memory* means physical or logical devices that can keep data non-volatilely, regardless of implementation such as memory embedded in MCU/SoC or discrete memory. Note HSM is not non-volatile memory but IO (peripheral).

*2: *at the usage of it* includes moment when the data stored in non-volatile, fallen into CSP/PSP, are allocated to volatile or HSM.

<Note>

Detection method example: Verification of integrity/authenticity of CSP/PSP before the usage

3.1.1.3.2. Detection of manipulation of software

[Requirement: IDSHER_02301]

If any of the following is manipulated at startup of software composing a function in an entry-point region, a detection function shall notify a SEv creation function of the anomaly. In addition, the detection of manipulation shall be performed from a region where integrity is guaranteed. However, if IDSHMR_01601 in [10] is allocated, both this system and Host-based IDS for Multi-layered

Separation Function does not have to detect manipulation of software.

- The code of the software
- The data controlling the behavior of the software

<Note>

Detection method example: Secure boot, detection of startup of software unpermitted to be started up

3.1.2. SEv creation function

3.1.2.1. SEv creation

[Requirement: IDSHER_07102]

When a SEv creation function is notified of an anomaly by a detection function, it shall create an SEv (Table 3-1), and notify a QSEv creation function of the SEv. Event Definition ID and Context Data shall be set in accordance Table 3-2. Context Data shall be set with big endian.

Table 3-1: Anomaly notification SEv

Field Name	Length	Description
Security Event ID	16 bit	This field shall be set to an identifier that identifies Event Definition ID and Sensor Instance ID that a QSEv creation function sets a QSEv to. - Event Definition ID shall be in accordance with an anomaly detected (Table 3-2). - Sensor Instance ID shall be fixed to 0. <Note> This field is implemented by an IdsMInternalEventId type parameter.
Context Data Size	8 or 32 bit	This field shall be set to a byte length of Context Data. One of them shall be chosen for each Event Definition ID in software design phase up to size of Context Data.
Context Data	Variable length	This field shall be set to a sequence of bytes about an anomaly detected, and shall be set depending on a requirement ID of a detection function that has notified an anomaly. Diagnostic timestamp of occurrence of anomaly shall be also set.

Table 3-2: Event Definition ID, Count, and Context Data for each requirement ID

Corresponding Requirement ID	Event Definition ID	Context Data		
		Field Name	Length [Byte]	Description
IDSHER_04101	0x8110	Format Version	1	Fixed vale: 0x01
		Diagnostic timestamp (*1)	7	Trip counter and time counter of diagnostic timestamp
		Diagnostic clock Information (*1)	6	Clock information of diagnostic timestamp
		Diagnostic vehicle odometer information (*1)	4	Odometer of diagnostic timestamp
		Software ID Size	1	This field shall be set to a byte length of Software ID (0~16).

		Software ID	Variable length	This field shall be set to the information (*3) to identify which software has been aborted unless it is difficult to obtain the information due to technical constraint (*2). (For example, the executable file name of the software, identifier related to the software, etc.)
IDSHER_01601	0x8120	Format Version	1	Fixed value: 0x01
		Diagnostic timestamp (*1)	7	Trip counter and time counter of diagnostic timestamp
		Diagnostic clock information (*1)	6	Clock information of diagnostic timestamp
		Diagnostic vehicle odometer information (*1)	4	Odometer of diagnostic timestamp
		Software ID Size	1	This field shall be set to a byte length of Software ID (0~16).
		Software ID	Variable length	This field shall be set to the information (*3) to identify which software an abnormal control flow occurred in unless it is difficult to obtain the information due to technical constraint (*2). (For example, the executable file name of the software, identifier related to the software, etc.)
		Subroutine ID Size	1	This field shall be set to a byte length of Subroutine ID (0~16).
		Subroutine ID	Variable length	This field shall be set to the information (*3) to identify which subroutine an abnormal transition occurred from unless it is difficult to obtain the information due to technical constraint (*2). (For example, the subroutine name, identifier related to the subroutine, etc.)
IDSHER_01101 IDSHER_01102 IDSHER_01201 IDSHER_01202 IDSHER_01501 IDSHER_01502	0x8130	Format Version	1	Fixed vale: 0x01
		Diagnostic timestamp (*1)	7	Trip counter and time counter of diagnostic timestamp
		Diagnostic clock information (*1)	6	Clock information of diagnostic timestamp
		Diagnostic vehicle odometer information (*1)	4	Odometer of diagnostic timestamp
		Software ID Size	1	This field shall be set to a byte length of Software ID (0~16).

		Software ID	Variable length	This field shall be set to the information (*3) to identify which software performed illegal access unless it is difficult to obtain the information due to technical constraint (*2). (For example, the executable file name of the software, identifier related to the software, etc.)
		Memory or IO ID Size	1	This field shall be set to a byte length of Memory or IO ID (0~16).
		Memory ID or IO ID	Variable length	This field shall be set to the information (*3) to identify which memory or IO (peripheral) was illegally accessed unless it is difficult to obtain the information due to technical constraint (*2). (For example, the memory address, the device name of the IO, identifier related to the IO, etc.)
IDSHER_01401	0x8140	Format Version	1	Fixed value: 0x01
		Diagnostic timestamp (*1)	7	Trip counter and time counter of diagnostic timestamp
		Diagnostic clock information (*1)	6	Clock information of diagnostic timestamp
		Diagnostic vehicle odometer information (*1)	4	Odometer of diagnostic timestamp
		Software ID Size	1	This field shall be set to a byte length of Software ID (0~16).
		Software ID	Variable length	This field shall be set to the information (*3) to identify which software used a function not permitted to do so unless it is difficult to obtain the information due to technical constraint (*2). (For example, the executable file name of the software, identifier related to the software, etc.)
		Function ID Size	1	This field shall be set to a byte length of Function ID (0~16).
		Function ID	Variable length	This field shall be set to the information (*3) to identify which function was used illegally unless it is difficult to obtain the information due to technical constraint (*2). (For example, the function name identifier related to the function, etc.)
IDSHER_02101 IDSHER_02301	0x8150	Format Version	1	Fixed value: 0x01
		Diagnostic timestamp (*1)	7	Trip counter and time counter of diagnostic tim1estamp
		Diagnostic clock information (*1)	6	Clock information of diagnostic timestamp

		Diagnostic vehicle odometer information (*1)	4	Odometer of diagnostic timestamp
		CSP/PSP or Software ID Size	1	This field shall be set to a byte length of CSP/PSP or Software ID (0~16).
		CSP/PSP ID or Software ID	Variable length	This field shall be set to the information (*3) to identify which CSP/PSP or software was manipulated unless it is difficult to obtain the information due to technical constraint (*2). (For example, the CSP/PSP name, the executable file name of the software, identifier related to the software, etc.)

*1: For details, see reference [8].

*2: For example, a case when OS or BSW is necessary to be modified to obtain the information.

*3: Developer (ECU software designer, supplier, etc.) defines data effective to identify the cause and the region where an event occurs.

3.1.3. QSEv creation function

3.1.3.1. SEv qualification

[Requirement: IDSHER_07103]

A QSEv creation function shall qualify notified SEvs to a QSEv for each Security Event ID, in accordance with [2], with parameters specified in [IDSHER_03402].

3.1.4. QSEv transmission function

3.1.4.1. QSEv transmission

[Requirement: IDSHER_07108]

If a detection master (reference [11]) exists on any ECU, this requirement shall be allocated. When a QSEv creation function creates a QSEv, a QSEv transmission function shall create a communication frame with data shown in Figure 3-2 set in a region shown below, and send it to the detection master.

- When an ECU sends a QSEv with CAN communication or CAN FD communication:
  A region where Data Label is defined by QSEV_DATA_[ECU node name (*1)]
- When an ECU sends a QSEv with Ethernet communication:
  A region where Property is defined by [ECU node name (*1)]QsevData

Protocol Version	Protocol Header	IdsM Instance	Sensor Instance	Event Definition	Count	Reserved	Context Data

		ID	ID	ID			(*2)
msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb	msb … lsb

Figure 3-2: Data Structure

*1: [ECU node name] shall be replaced by a node name, defined in communication specification, of an ECU that this document is allocated to. If Data Label or Property is not defined in communication specification, please contact us.
*2: Allocated to ECU/VMs on CAN-FD or Ethernet network but **NOT** allocated to ECU/VMs on CAN network.

[Requirement: IDSHER_07208]
If a QSEv transmission function transmits QSEvs to a detection master, this requirement shall be allocated. If QSEv transmission by the QSEv transmission function wakes up network or prevents network from sleeping, the QSEv transmission function shall not transmit QSEvs.
<Note>
This requirement has been defined to avoid running out of battery due to transmitting QSEv.

3.1.5. QSEv storing function

3.1.5.1. QSEv storing

[Requirement: IDSHER_07109]
If any detection master does not exist on any ECU, this requirement shall be allocated. A QSEv storing function shall store the latest QSEvs created by a QSEv creation function into non-volatile memory for each Event Definition ID where the number of QSEvs to be stored is [NumberOfQSEvs]. However, it may not store QSEvs at unexpected reset (e.g. power source instantaneous interruption, low voltage). In addition, QSEv storing function shall be designed considering the limit of number of writes to non-volatile memory.

[Note]
If a detection master exists on an ECU, it is optional to store QSEvs.
Buffering QSEvs in RAM during IG-ON, and then writing the QSEvs into non-volatile memory at IG-OFF can be an example of the implementation of storing QSEvs in non-volatile memory considering the maximum number of writes to non-volatile memory.

[Requirement: IDSHER_07111]
UserDefMemoryDTC and DID for QSEvs storing shall be in accordance with Table 3-3, Table 3-4, and Table 3-5.

UserDefMemoryDTC and DID are defined in accordance with the following policy.

・UserDefMemoryDTC: Defined for each Event Definition ID

・DID：Defined for whole QSEv, and common among all Event Definition IDs

Table 3-3: UserDefMemoryDTC Related Information

UserDefMemoryDTC	FTB	Event Definition ID corresponding to UserDefMemoryDTC	Memory Selection
U2B21	0x00	0x8110	0x14
U2B22	0x00	0x8120	0x14
U2B23	0x00	0x8130	0x14
U2B24	0x00	0x8140	0x14
U2B25	0x00	0x8150	0x14

Table 3-4: DID for QSEv storing

DID	Data	Length [Bit]
0xA910	Protocol Version	4
	Protocol Header	4
	IdsM Instance ID	10
	Sensor Instance ID	6
	Event Definition ID	16
	Count	16
	Reserved	8
	Context Data (*1)	Variable Length

*1: Allocated to ECU/VMs on CAN-FD or Ethernet network but **NOT** allocated to ECU/VMs on CAN network.

Table 3-5: Example of QSEv storage data(Store 5 QSEvs with Event Definition ID 0x8110)

UserDefMemoryDTC	FTB	UserDefDTC SnapshotRecordNumber	Description
U2B21	0x00	0x01	Oldest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)
		0x02	Second oldest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)
		0x03	Third oldest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)
		0x04	Fourth oldest QSEv of the last

			[NumberOfQSEv] QSEvs (DID: 0xA910)
		0x05	Newest QSEv of the last [NumberOfQSEv] QSEvs (DID: 0xA910)

3.1.5.2. QSEv read

[Requirement: IDSHER_07110]

If QSEvs are stored in non-volatile memory, this requirement shall be allocated. QSEvs stored in non-volatile memory shall be able to be read from off-board client and on-board client by diagnostic communication with SID 0x19 (Sub Function 0x17/0x18). However, if the QSEvs are loaded on volatile memory, these QSEvs shall be able to be read.

For the details of the diagnostics communication, see reference [9].

3.1.5.3. QSEv deletion

[Requirement: IDSHER_07204]

If QSEvs are stored in non-volatile memory, this requirement shall be allocated. QSEvs stored in non-volatile memory shall be able to be deleted from off-board client by diagnostic communication with SID 0x14 (QSEv output MemorySelection 0x14).

For the details of the diagnostics communication, see reference [9].

3.2. Quality requirements

We define quality requirements in this section.

[Requirement: IDSHER_12201]

Functions except detection ones of this system and QSEvs created by them shall be designed not to be manipulated from a function to terminate communication from Out-Car

<Note>

For example, this requirement can be satisfied by the four items below.

1) If functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than detection functions (3.1.1) uses a register, this requirement shall be allocated. A function to terminate communication from Out-Car shall not have write access to a register that functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than detection function (3.1.1) uses.

2) If functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than detection functions (3.1.1) uses a memory, this requirement shall be allocated. A function to terminate communication from Out-Car shall not have write access to a region of a memory that functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than

detection function (3.1.1) uses with the following exceptions.
Exception:
A region in virtual CAN communication interface or virtual Ethernet communication interface where only data transmitted between functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than a detection function (3.1.1) and a detection function are stored.
Example of the exception of the region of a memory:
A region in virtual CAN communication interface where data from a detection function (3.1.1) to functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) are stored.

3) If functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than detection functions (3.1.1) uses a HSM, this requirement shall be allocated. A function to terminate communication from Out-Car shall not have write access to output (cipher text, MAC value) from a HSM interface that functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than detection function (3.1.1) uses.

   Physical separation of HSM interface is not mandatory. For example, if satisfying 1) or/and 2) can prohibit write access to output from HSM interface, physical separation of HSM interface is not needed.

4) If functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than detection functions (3.1.1) uses a communication interface in In-CAR, this requirement shall be allocated. A function to terminate communication from Out-Car shall not have write access to a communication interface in In-CAR that functions (3.1.2, 3.1.3, 3.1.4, 3.1.5) other than detection function (3.1.1) uses.

   Physical separation of HSM interface is not mandatory. For example, if satisfying 1) or/and 2) can prohibit write access to a communication interface, physical separation of communication interface is not needed.

3.3. Constraints

None.

3.4. Parameters

We define parameters in this section.

[Requirement: IDSHER_03401]
All parameters defined in this section shall be able to be changed under conditions defined in each requirement.

[Requirement: IDSHER_03402]

QSEvs shall be created and stored with parameters in Table 3-6 and the meta-information of the parameters shall be in accordance with Table 3-7 and Table 3-8.

Table 3-6: Parameters for QSEv creation and storing

Name	Event Definition ID	Sensor Instance ID	Value (*1)
IdsMEventAggregationTimeInterval	0x8110	0x0	0.3
	0x8120	0x0	0.3
	0x8130	0x0	0.3
	0x8140	0x0	0.3
	0x8150	0x0	0.3
IdsMContextDataSourceSelector	0x8110	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8120	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8130	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8140	0x0	IDSM_FILTERS_CTX_USE_FIRST
	0x8150	0x0	IDSM_FILTERS_CTX_USE_FIRST
NumberOfQSEvs	0x8110	0x0	5
	0x8120	0x0	5
	0x8130	0x0	5
	0x8140	0x0	5
	0x8150	0x0	5

Table 3-7: Meta information of parameters for QSEv creation

Name	Unit	Type	Lower limit	Upper limit
IdsMEventAggregationTimeInterval (*2)	sec	EcucFloatParamDef	0.05	10.00
IdsMContextDataSourceSelector	-	EcucEnumerationParamDef	IDSM_FILTERS_CTX_USE_FIRST	IDSM_FILTERS_CTX_USE_LAST

*1: That value of IdsMEventAggregationTimeInterval is hyphen means no aggregation.

*2: If it is not available to set the value specified in the value column, the biggest value among available values smaller than the value specified shall be adopted.

Table 3-8: Meta information of parameters for QSEv storing

Name	Description	Unit	Lower limit	Upper limit
NumberOfQSEvs	The number of QSEvs	-	0	10

	to be stored			