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　評価仕様書 Test 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-TST-SPEC-a00-04-a

承認 Approved by	調査 Checked by	作成 Created by	
平林	松井	竹山	2022/11/25

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 Allocated to entry-point ECUs / VMs specified by another document.
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	英訳を追加	2021/05/14	46F 4G 稲垣
a00-01-a	要求仕様書の修正に応じた修正	2021/08/06	46F 4G 竹山
a00-02-a	評価内容を全体的に具体化	2022/03/24	46F 4G 竹山
a00-03-a	・IDSHER_07202 に関する記述を削除 ・IDSHET_07109 に UserDefMemoryDTC の確認を追加 ・4 章冒頭に QSEv 読み出しと QSEv 消去の説明を追加	2022/06/09	46F 4G 竹山
a00-04-a	・IDSHET_04101 具体化のための文言の修正 ・IDSHET_01601 具体化のための文言の修正 ・IDSHET_01101 適用条件の追加 ・IDSHET_01102 適用条件の追加 ・IDSHET_01201 適用条件の追加 ・IDSHET_01202 適用条件の追加 ・IDSHET_01501 適用条件の追加、誤記訂正（英語版のみ） ・IDSHET_01502 適用条件の追加、誤記訂正（英語版のみ） ・IDSHET_01401 適用条件の追加、具体化のための文言の修正 ・IDSHET_02301 具体化のための文言の修正 ・IDSHET_12201 試験内容の修正	2022/11/25	46F 4G 竹山

目次

1. はじめに

1.1. 本書の目的

本書では、侵入検知 エントリーポイント向け Host IDS 要求仕様書（上位文書[1]）によって定義された要求を評価するための評価仕様を定義する。

1.2. 適用先

本書は、侵入検知 エントリーポイント向け Host IDS 要求仕様書の適用対象となる ECU/VM に適用される。

1.3. 前提条件

QSEv 生成機能は、参照文書[1]に基づき評価されていること。

1.4. 要求事項の記載

【IDSHET_*】と記載されている部分が、本書で要求する評価要件である。なお、［補足］と記載されているものは補足事項のため評価要件ではない。

1.5. 関連文書

上位文書、参照文書を示す。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	侵入検知 エントリーポイント向け Host IDS 要求仕様書	-

1.5.2. 参照文書

表 1-2 参照文書

No.	文書名	Ver.
1	侵入検知 QSEv 生成評価仕様書	-
2	TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	-

2. 評価概要

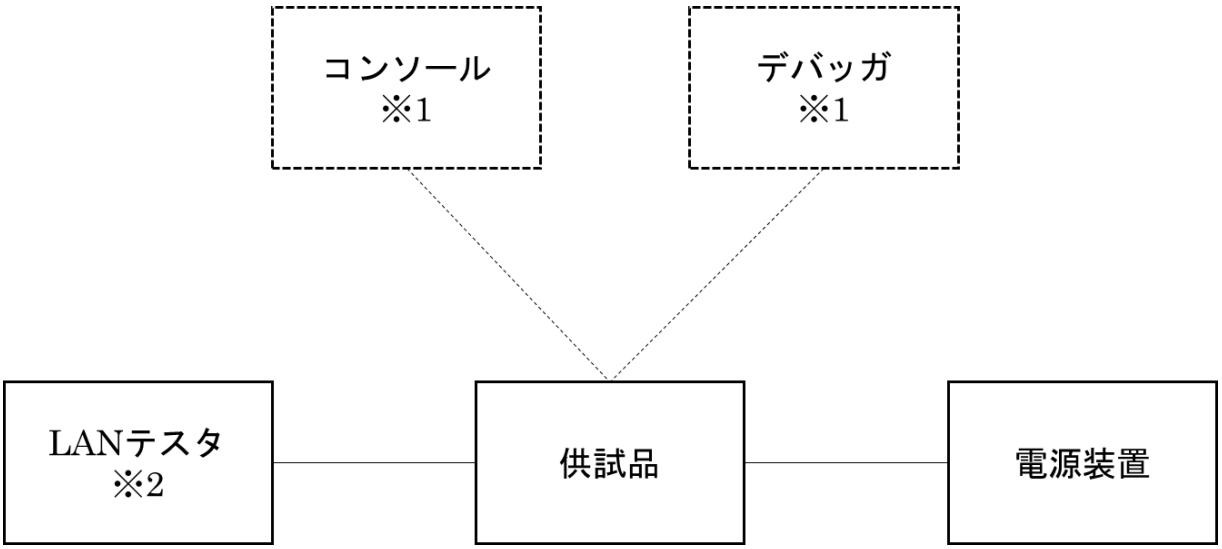
評価項目一覧を表 2-1 に示す。下記評価項目の合格基準を全て満たす場合、合格と判定すること。

表 2-1 評価項目一覧

上位文書[1]が定義する要求事項				対応する評価項目	生産時
分類			要求 ID	評価 ID	機能
機能要求	検知機能	遠隔車外との通信に対する 1 層目防御機能の停止の検知	IDSHER_04101	IDSHET_04101	-
		遠隔車外との通信を終端する機能の不正動作の検知	IDSHER_01601	IDSHET_01601	-
			IDSHER_01101	IDSHET_01101	-
			IDSHER_01102	IDSHET_01102	-
			IDSHER_01201	IDSHET_01201	-
			IDSHER_01202	IDSHET_01202	-
			IDSHER_01501	IDSHET_01501	-
			IDSHER_01502	IDSHET_01502	-
			IDSHER_01401	IDSHET_01401	-
		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	IDSHET_02101	-
			IDSHER_02301	IDSHET_02301	-
	SEv 生成機能	SEv の生成	IDSHER_07102	IDSHET_07108, IDSHET_07109 IDSHET_07118 IDSHET_07119	-
	QSEv 生成機能	SEv の集約	IDSHER_07103		
	QSEv 送信機能	QSEv の送信	IDSHER_07108	IDSHET_07108 IDSHET_07118	
			IDSHER_07208	IDSHET_07208	
	QSEv 保管機能	QSEv の保管	IDSHER_07109 IDSHER_07111	IDSHET_07109 IDSHET_07119	
		QSEv の読み出し	IDSHER_07110	IDSHET_07129	
		QSEv の消去	IDSHER_07204	IDSHET_07204	
品質要求			IDSHER_12201	IDSHET_12201	-
設計値			IDSHER_03401	IDSHET_03401	-
			IDSHER_03402	IDSHET_07108, IDSHET_07109 IDSHET_07118 IDSHET_07119 IDSHET_07129	-

3. 評価環境

本仕様書で想定する評価環境を図 3-1 に示す。



※1 必要に応じて評価に用いること。

※2 ダイアグ通信も可能なものを想定している。

図 3-1 評価環境

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）は、ソフトウェア内部の異常を捉える技術であるため、供試品の外部からの侵入またはその試みによって評価を行うことは困難である。したがって、本システムの評価に際しては、本システムが監視対象とするソフトウェアやその振舞い、データの改変を前提とした評価を行う方針とする。さらに、本システムの検知機能の実装によっては、意図したタイミングで異常を発生させることが困難であることと、検知機能以外の評価を行う際のシステム全体の改変を最小限に抑えることから、検知機能が SEv 生成機能に通知する各々の異常通知を模擬するソフトウェアの使用を前提とした検知機能以外の機能の評価を実施する方針とする。
上記内容に基づいた評価方針を図 3-2 に示す。なお、監視対象の改変や異常通知を模擬するソフトウェアの使用に際して、必要に応じて、供試品にコンソールやデバッガなどを接続してもよい。

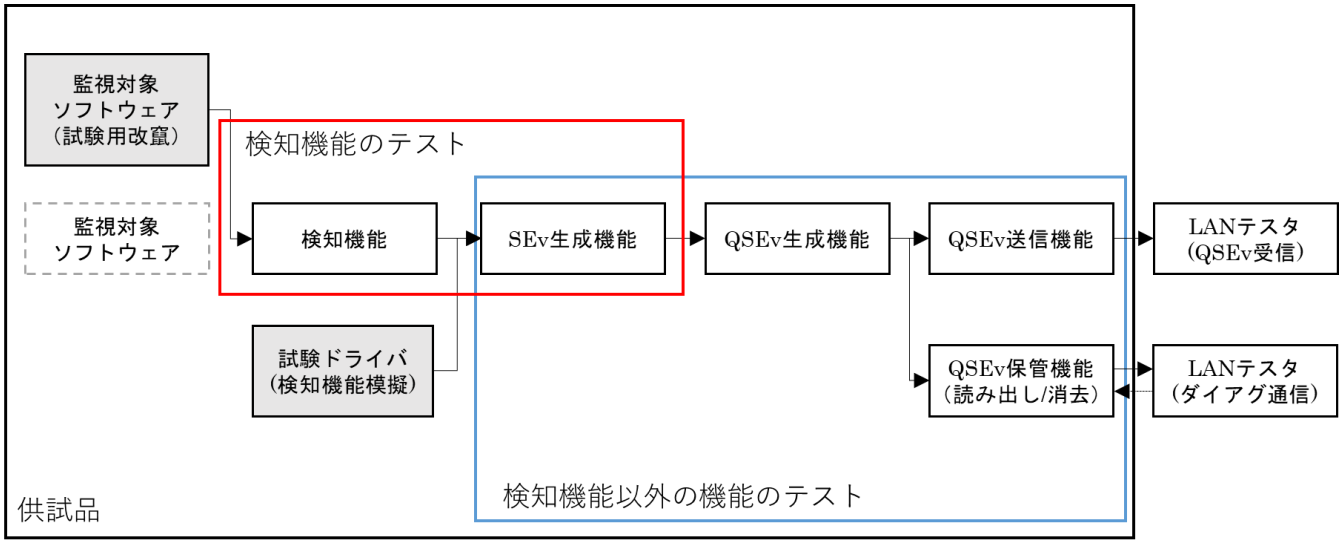


図 3-2　本システムの評価方針

検知機能以外の機能の評価を行うための試験パターンを表 3-1 に、試験イメージを図 3-3 に示す。各異常に対して、複数の異常の発生パターンで SEv 生成機能、QSEv 生成機能、QSEv 送信機能および QSEv 保管機能に対する評価を行う。

表 3-1　試験パターン

検知機能	異常通知の発生パターン	試験 ID	測定項目
各検知機能で発生させる異常の種別 ・IDSHER_04101 ・IDSHER_01601 ・IDSHER_01101 ・IDSHER_01102 ・IDSHER_01201 ・IDSHER_01202 ・IDSHER_01501 ・IDSHER_01502 ・IDSHER_01401 ・IDSHER_02101 ・IDSHER_02301	単発	IDSHET_07108	受信したメッセージ
		IDSHET_07109	読み出し結果
	複数 （集約間隔ごとに 3 回を、集約機能を確認するのに十分な回数繰り返す。ただし、QSEv の保管の上限数を超えない回数とする。具体的には、送信間隔を[IdsMEventAggregationTimeInterval]/3 秒、送信回数を 3*([NumberOfQSEvs]-1）回とすることを想定している）	IDSHET_07118	受信したメッセージ
		IDSHET_07119	読み出し結果

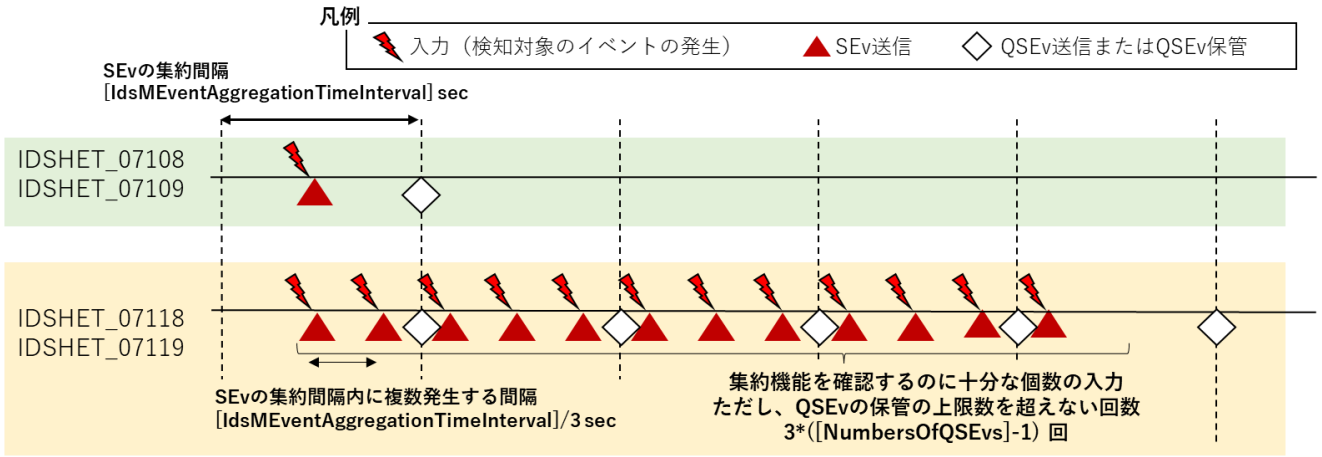


図 3-3：試験イメージ

4. 評価詳細

本システムの評価要求を定義する。なお、本章において、QSEv 読み出しは SID 0x19, DID 0xA910 を用いたダイアグ通信によって行う。また、QSEv 消去は SID 0x14 を用いたダイアグ通信によって行う。ただし、ダイアグ通信の詳細手順に関しては参照文書[2]を参照すること。

4.1. 機能要求評価

本節では機能要求に対する評価要求を定義する。

4.1.1. 検知機能

4.1.1.1. 遠隔車外との通信に対する 1 層目防御機能の停止の検知

【IDSHET_04101】	
試験内容	遠隔車外との通信に対する 1 層目防御機能が常駐ソフトウェア(常駐プロセス)として設計される場合に、本試験を実施する。当該ソフトウェアが設計上、動作すべき状況において動作していない場合、SEv 生成機能に異常が通知されることを確認する。
事前条件	● 本試験においては、遠隔車外との通信に対する 1 層目防御機能を監視対象ソフトウェアとする。 ● 監視対象ソフトウェアについて、試験的な改変が可能である。 ● 当該ソフトウェアが本来動作すべき状況を試験的に発生させることが可能である。
試験手順	(1) 監視対象ソフトウェアについて、動作しないよう改変(※1)を行った上で、当該ソフトウェアが本来動作すべき状況を試験的に発生させる。 (2) 検知機能から SEv 生成機能への異常通知を監視する。(※2) ※2 内部的な確認が困難な場合は LAN テスタ等を用いて最終的な出力の QSEv を確認してもよい。
測定項目	(A) 試験手順(2)において検知機能から SEv 生成機能に通知された異常通知
合格基準	● 測定項目が試験手順(1)により通知されるべき異常通知の内容である。
備考	※1 一例として、当該プロセスを起動させない、または、当該プロセスを停止させることが本試験における改変に該当する。

4.1.1.2. 遠隔車外との通信を終端する機能の不正動作の検知

4.1.1.2.1. 制御フローの異常検知

【IDSHET_01601】	
試験内容	遠隔車外との通信を終端する機能を構成する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関数遷移が行われたまたは試みられたとき、SEv 生成機能に異常が通知されることを確認する。 監視対象ソフトウェアが複数存在する場合には、試験者は監視対象ソフトウェアごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、遠隔車外との通信を終端する機能を構成するソフトウェアを監視対象ソフトウェアとする。 ● 監視対象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関数遷移を行うための試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアを動作させた上で、下記に示すデータを試験的に改変し、正規の制御フローとして起こりえない関数遷移を試みる。なお、下記のそれぞれについて、試験を実施する。 ➢ 関数ポインタを参照する関数呼出し（間接コール）が行われる箇所において、関数ポインタの値を正規の制御フローとして起こりえない値(※1)に改変する。 ➢ 関数からのリターンが行われる箇所において、コールスタックに格納されるリターンアドレスの値を正規の制御フローとして起こりえない値(※2)に改変する。 (2) 検知機能から SEv 生成機能への異常通知を監視する。(※3) ※3 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(2)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(1)により通知されるべき異常通知の内容である。
備考	※1 一例として、関数ポインタを改変する場合には、関数先頭以外の箇所が、正規の制御フローとして起こりえない値に該当する。 ※2 一例として、リターンアドレスを改変する場合には、関数呼出し以外の箇所が、正規の制御フローとして起こりえない値に該当する。

4.1.1.2.2. 不揮発性メモリへの不正アクセス検知

【IDSHET_01101】	
試験内容	遠隔車外と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エントリーポイント領域の不揮発性メモリにアクセスできる仕組みを持ち、かつ、当該ソフトウェアの動作に不必要なアクセスが許可されないよう設計される場合に、本試験を実施する。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、SEv 生成機能に異常が通知されることを確認する。 - 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 監視対象ソフトウェアが複数存在する場合には、監視対象ソフトウェアごとに試験を実施する。また、エントリーポイント領域の不揮発性メモリのパスが複数存在する場合には、パスごとに試験を実施する。そして、許可されていない操作が読み出しアクセス、書き込みアクセス、実行アクセス、属性の変更の複数に該当する場合には、操作ごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、遠隔車外との通信を終端する機能を構成するソフトウェアを監視対象ソフトウェアとする。 ● 監視対象ソフトウェアについて、試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアについて、エントリーポイント領域の不揮発性メモリのパスに対して許可されていない操作を行うように試験的に改変を行う。 (2) 改変した監視対象ソフトウェアより、許可されていない操作を試みる。 (3) 検知機能から SEv 生成機能への異常通知を監視する。(※1) ※1 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(3)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(2)により通知されるべき異常通知の内容である。
備考	無し。

【IDSHET_01102】	
試験内容	遠隔車外と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エントリーポイント領域の不揮発性メモリにアクセスできる仕組みを持ち、かつ、当該ソフトウェアの動作に不必要なアクセスが許可されないよう設計される場合に、本試験を実施する。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、SEv 生成機能に異常が通知されることを確認する。 - 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 監視対象ソフトウェアが複数存在する場合には、監視対象ソフトウェアごとに試験を実施する。また、エントリーポイント領域の不揮発性メモリのアドレスが複数存在する場合には、アドレスごとに試験を実施する。そして、許可されていない操作が読み出しアクセス、書き込みアクセス、実行アクセス、属性の変更の複数に該当する場合には、操作ごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、遠隔車外との通信を終端する機能を構成するソフトウェアを監視対象ソフトウェアとする。 ● 監視対象ソフトウェアについて、試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアについて、エントリーポイント領域の不揮発性メモリのアドレスに対して許可されていない操作を行うように試験的に改変を行う。 (2) 改変した監視対象ソフトウェアより、許可されていない操作を試みる。 (3) 検知機能から SEv 生成機能への異常通知を監視する。(※1) ※1 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(3)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(2)により通知されるべき異常通知の内容である。
備考	無し。

4.1.1.2.3. 揮発性メモリへの不正アクセス検知

【IDSHET_01201】	
試験内容	遠隔車外と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エントリーポイント領域の揮発性メモリにアクセスできる仕組みを持ち、かつ、当該ソフトウェアの動作に不必要なアクセスが許可されないよう設計される場合に、本試験を実施する。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、SEv 生成機能に異常が通知されることを確認する。 - 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 監視対象ソフトウェアが複数存在する場合には、監視対象ソフトウェアごとに試験を実施する。また、エントリーポイント領域の揮発性メモリのパスが複数存在する場合には、パスごとに試験を実施する。そして、許可されていない操作が読み出しアクセス、書き込みアクセス、実行アクセス、属性の変更の複数に該当する場合には、操作ごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、遠隔車外との通信を終端する機能を構成するソフトウェアを監視対象ソフトウェアとする。 ● 監視対象ソフトウェアについて、試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアについて、エントリーポイント領域の揮発性メモリのパスに対して許可されていない操作を行うように試験的に改変を行う。 (2) 改変した監視対象ソフトウェアより、許可されていない操作を試みる。 (3) 検知機能から SEv 生成機能への異常通知を監視する。(※1) ※1 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(3)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(2)により通知されるべき異常通知の内容である。
備考	無し。

【IDSHET_01202】	
試験内容	遠隔車外と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エントリーポイント領域の揮発性メモリにアクセスできる仕組みを持ち、かつ、当該ソフトウェアの動作に不必要なアクセスが許可されないよう設計される場合に、本試験を実施する。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、SEv 生成機能に異常が通知されることを確認する。 - 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 監視対象ソフトウェアが複数存在する場合には、監視対象ソフトウェアごとに試験を実施する。また、エントリーポイント領域の揮発性メモリのアドレスが複数存在する場合には、アドレスごとに試験を実施する。そして、許可されていない操作が読み出しアクセス、書き込みアクセス、実行アクセス、属性の変更の複数に該当する場合には、操作ごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、遠隔車外との通信を終端する機能を構成するソフトウェアを監視対象ソフトウェアとする。 ● 監視対象ソフトウェアについて、試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアについて、エントリーポイント領域の揮発性メモリのアドレスに対して許可されていない操作を行うように試験的に改変を行う。 (2) 改変した監視対象ソフトウェアより、許可されていない操作を試みる。 (3) 検知機能から SEv 生成機能への異常通知を監視する。(※1) ※1 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(3)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(2)により通知されるべき異常通知の内容である。
備考	無し。

4.1.1.2.4. IO(ペリフェラル)への不正アクセス検知

【IDSHET_01501】	
試験内容	遠隔車外と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エントリーポイント領域の IO(ペリフェラル)にアクセスできる仕組みを持ち、かつ、当該ソフトウェアの動作に不必要なアクセスが許可されないよう設計される場合に、本試験を実施する。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、SEv 生成機能に異常が通知されることを確認する。 - 読み出しアクセス - 書き込みアクセス - 属性の変更 監視対象ソフトウェアが複数存在する場合には、監視対象ソフトウェアごとに試験を実施する。また、エントリーポイント領域の IO(ペリフェラル)のパスが複数存在する場合には、パスごとに試験を実施する。そして、許可されていない操作が読み出しアクセス、書き込みアクセス、属性の変更の複数に該当する場合には、操作ごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、遠隔車外との通信を終端する機能を構成するソフトウェアを監視対象ソフトウェアとする。 ● 監視対象ソフトウェアについて、試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアについて、エントリーポイント領域の IO(ペリフェラル)のパスに対して許可されていない操作を行うように試験的に改変を行う。 (2) 改変した監視対象ソフトウェアより、許可されていない操作を試みる。 (3) 検知機能から SEv 生成機能への異常通知を監視する。(※1) ※1 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(3)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(2)により通知されるべき異常通知の内容である。
備考	無し。

【IDSHET_01502】	
試験内容	遠隔車外と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エントリーポイント領域の IO(ペリフェラル)にアクセスできる仕組みを持ち、かつ、当該ソフトウェアの動作に不必要なアクセスが許可されないよう設計される場合に、本試験を実施する。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、SEv 生成機能に異常が通知されることを確認する。 - 読み出しアクセス - 書き込みアクセス - 属性の変更 監視対象ソフトウェアが複数存在する場合には、監視対象ソフトウェアごとに試験を実施する。また、エントリーポイント領域の IO(ペリフェラル)のアドレスが複数存在する場合には、アドレスごとに試験を実施する。そして、許可されていない操作が読み出しアクセス、書き込みアクセス、属性の変更の複数に該当する場合には、操作ごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、遠隔車外との通信を終端する機能を構成するソフトウェアを監視対象ソフトウェアとする。 ● 監視対象ソフトウェアについて、試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアについて、エントリーポイント領域の IO(ペリフェラル)のアドレスに対して許可されていない操作を行うように試験的に改変を行う。 (2) 改変した監視対象ソフトウェアより、許可されていない操作を試みる。 (3) 検知機能から SEv 生成機能への異常通知を監視する。(※1) ※1 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(3)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(2)により通知されるべき異常通知の内容である。
備考	無し。

4.1.1.2.5. 機能の不正使用検知

【IDSHET_01401】	
試験内容	エントリーポイント領域が、使用に際して何らかの権限を必要とする機能を持ち、かつ、遠隔車外との通信を終端する機能を構成するソフトウェアにおいて、その動作に不必要な機能の使用が許可されないよう設計される場合に本試験を実施する。当該ソフトウェアが、使用に際して何らかの権限を必要とする機能のうち、使用を許可されていない機能を使用したまたは試みたとき、SEv 生成機能に異常が通知されることを確認する。 監視対象ソフトウェアが複数存在する場合には、監視対象ソフトウェアごとに試験を実施する。また、許可されていない機能が複数存在する場合には、機能ごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、遠隔車外との通信を終端する機能を構成するソフトウェアを監視対象ソフトウェアとする。 ● 監視対象ソフトウェアについて、試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアについて、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(※1)を使用するように試験的に改変を行う。 (2) 改変した監視対象ソフトウェアより、許可されていない機能の使用を試みる。 (3) 検知機能から SEv 生成機能への異常通知を監視する。(※2) ※2 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(3)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(2)により通知されるべき異常通知の内容である。
備考	※1 試験の対象となる機能の例を次に示す。 ✓ エントリーポイント領域に配置される OS により提供され、かつ、監視対象ソフトウェアによる使用が許可されていないシステムコール ✓ あるソフトウェアによってプロセス間通信を介して他のソフトウェアに提供され、かつ、監視対象ソフトウェアによる使用が許可されていない当該機能

4.1.1.3. 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

4.1.1.3.1. CSP/PSP の改ざん検知

【IDSHET_02101】	
試験内容	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、本試験を実施する。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、SEv 生成機能に異常が通知されることを確認する。 監視対象データが複数存在する場合には、監視対象データごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、エントリーポイント領域が不揮発性メモリに持つ CSP/PSP に該当するデータを監視対象データとする。 ● 監視対象データについて、試験的な改変が可能である。
試験手順	(1) 監視対象データを試験的に改変した上で、当該データの使用(※1)を試みる。 (2) 検知機能から SEv 生成機能への異常通知を監視する。(※2) ※2 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(2)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(1)により通知されるべき異常通知の内容である。
備考	※1 一例として、監視対象データの揮発性メモリまたは HSM への展開は、本試験における使用に該当する。

4.1.1.3.2. ソフトウェアの改ざん検知

【IDSHET_02301】	
試験内容	エントリーポイント領域に配置されるソフトウェアについて、それぞれの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、SEv 生成機能に異常が通知されることを確認する。 - 当該ソフトウェアのコード - リプログラミングでのみ更新可能な、当該ソフトウェアの振舞いを制御するデータ 監視対象ソフトウェアが複数存在する場合には、監視対象ソフトウェアごとに試験を実施する。ただし、監視の仕組みが同一であるものについては、代表して 1 つの試験としてもよい。
事前条件	● 本試験においては、エントリーポイント領域に配置されるソフトウェアを監視対象ソフトウェアとする。 ● 監視対象ソフトウェアのコード、または、リプログラミングでのみ更新可能な、その振舞いを制御するデータについて、試験的な改変が可能である。
試験手順	(1) 監視対象ソフトウェアのコード、または、リプログラミングでのみ更新可能な、その振舞いを制御するデータを試験的に改変した上で、当該ソフトウェアの起動(※1)を試みる。 (2) 検知機能から SEv 生成機能への異常通知を監視する。(※2) ※2 供試品内部における異常通知を直接的に測定することが困難な場合には、LAN テスタ等を用いて送信または保管される QSEv を測定してもよい。
測定項目	(A) 試験手順(2)において検知機能から SEv 生成機能に通知された異常通知。
合格基準	● 測定項目が試験手順(1)により通知されるべき異常通知の内容である。
備考	※1 一例として、監視対象ソフトウェアが一プロセスとして動作する場合、プロセスの生成時が本試験におけるソフトウェアの起動時に該当する。

4.1.2. QSEv 送信機能

4.1.2.1. QSEv の送信

【IDSHET_07108】	
試験内容	供試品が QSEv 送信機能を有する場合に、本試験を実施する。SEv 生成機能が、検知機能から 1 回の異常を通知されたとき、QSEv 送信機能が 1 つの通信フレームを生成し、検知マスタへ送信することを確認する。
事前条件	● QSEv 生成・保管に関する設計値が上位文書[1]に従い設定されている。 ● 検知機能の各々の異常通知を模擬するソフトウェアが試験的に配置されている。
試験手順	● 表 3-1 に従い、検知機能が通知する異常毎に下記の試験を実施すること。 (1) 異常通知を模擬するソフトウェアを用いて、SEv 生成機能に異常を通知する。 (2) LAN テスタを用いて、供試品から送信されるメッセージを受信する。
測定項目	● 検知機能が通知する異常毎に下記を測定すること。 (A) 試験手順(2)において受信したメッセージ
合格基準	● 検知機能が通知する異常毎に、測定項目が下記の内容である。 ➢ 測定項目(A)が試験手順(1)により生成されうる QSEv を含む。 ✧ 試験手順(1)によって発生しうる QSEv の個数が 1 個であること。 ✧ 各 QSEv の下記フィールドの値が期待値通り(※1)であること。 - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Count - Context Data ※1 上位文書[1] IDSHER_07103 及び参照文書[1] IDSQSR_03303 で定義されたものに従うこと
備考	無し。

【IDSHET_07118】	
試験内容	供試品が QSEv 送信機能を有する場合に、本試験を実施する。SEv 生成機能が、検知機能から複数回の異常を通知されたとき、SEv が適切に集約されたのち、QSEv 送信機能が通信フレームを生成し、検知マスタへ送信することを確認する。
事前条件	● QSEv 生成・保管に関する設計値が上位文書[1]に従い設定されている。 ● 検知機能の各々の異常通知を模擬するソフトウェアが試験的に配置されている。
試験手順	● 表 3-1 に従い、検知機能が通知する異常毎に下記の試験を実施すること。 (1) 異常通知を模擬するソフトウェアを用いて、SEv の集約間隔ごとに 3 回の間隔で複数回、SEv 生成機能に異常を通知する。 (2) LAN テスタを用いて、供試品から送信されるメッセージを受信する。
測定項目	● 検知機能が通知する異常毎に下記を測定すること。 (A) 試験手順(2)において受信したメッセージ
合格基準	● 検知機能が通知する異常毎に、測定項目が下記の内容である。 ➢ 測定項目(A)が試験手順(1)により生成されうる QSEv を含む。 ✧ 全受信メッセージの QSEv に含まれる Count の和が SEv 生成機能に異常を通知した回数と一致する。 ✧ 各 QSEv の下記フィールドの値が期待値通り(※1)であること。 - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Context Data ※1 上位文書[1] IDSHER_07103 及び参照文書[1] IDSQSR_03303 で定義されたものに従うこと
備考	無し。

【IDSHET_07208】	
試験内容	供試品が QSEv 送信機能を有する場合に、本試験を実施する。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に、QSEv 送信機能が QSEv を送信しないことを確認する。
事前条件	● QSEv 生成・保管に関する設計値が上位文書[1]に従い設定されている。 ● 検知機能の各々の異常通知を模擬するソフトウェアが試験的に配置されている。 ● QSEv 送信がネットワークの WakeUp 要因もしくは Sleep 阻害要因となるか否か、について制御が可能である。
試験手順	(1) QSEv 送信がネットワークの WakeUp 要因もしくは Sleep 阻害要因とならない状態で、異常通知を模擬するソフトウェアを用いて、SEv 生成機能に異常を通知する。 (2) LAN テスタを用いて、供試品から送信されるメッセージを受信する。 (3) QSEv 送信がネットワークの WakeUp 要因もしくは Sleep 阻害要因となる状態で、異常通知を模擬するソフトウェアを用いて、SEv 生成機能に異常を通知する。 (4) LAN テスタを用いて、供試品から送信されるメッセージを受信する。
測定項目	(A) 試験手順(2)において受信したメッセージ (B) 試験手順(4)において受信したメッセージ
合格基準	● 測定項目(A)が試験手順(1)により生成されうる QSEv を含む。 ● 測定項目(B)が試験手順(3)により生成されうる QSEv を含まない。
備考	● なし。

4.1.3. QSEv 保管機能

4.1.3.1. QSEv の保管・QSEv の読み出し

【IDSHET_07109】	
試験内容	供試品が QSEv 保管機能を有する場合に、本試験を実施する。下記を確認する。 ● SEv 生成機能が、検知機能から 1 回の異常を通知されたとき、QSEv 保管機能が QSEv を不揮発性メモリに保管すること。 ● 不揮発性メモリに保管される QSEv が、ダイアグ通信によって読み出しできること。
事前条件	● QSEv 生成・保管に関する設計値が上位文書[1]に従い設定されている。 ● 検知機能の各々の異常通知を模擬するソフトウェアが試験的に配置されている。
試験手順	● 表 3-1 に従い、検知機能が通知する異常毎に下記の試験を実施すること。 (1) LAN テスタから供試品に対して、QSEv の読み出しを実施する。 (2) 異常通知を模擬するソフトウェアを用いて、SEv 生成機能に異常を通知する。 (3) LAN テスタから供試品に対して、QSEv の読み出しを実施する。
測定項目	● 検知機能が通知する異常毎に下記を測定すること。 (A) 試験手順(1)における読み出しの結果 (B) 試験手順(3)における読み出しの結果
合格基準	● 検知機能が通知する異常毎に、測定項目が下記の内容である。 ➢ 測定項目(A)が試験手順(2)により生成されうる QSEv を含まない。 ➢ 測定項目(B)が上位文書[1] IDSHER_07111 で定義された、各イベントの Event Definition ID に対応する UserDefMemoryDTC を含む。 ➢ 測定項目(B)が試験手順(2)により生成されうる QSEv を含む。 ✧ 試験手順(2)によって発生しうる QSEv の個数が 1 個であること。 ✧ 各 QSEv の下記フィールドの値が期待値通り(※1)であること。 - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Count - Context Data ※1 上位文書[1] IDSHER_07103 及び参照文書[1] IDSQSR_03303 で定義されたものに従うこと
備考	無し。

【IDSHET_07119】	
試験内容	供試品が QSEv 保管機能を有する場合に、本試験を実施する。下記を確認する。 ● SEv 生成機能が、検知機能から複数回の異常を通知されたとき、SEv が適切に集約されたのち、QSEv 保管機能が QSEv を不揮発性メモリに保管すること。 ● 不揮発性メモリに保管される複数の QSEv が、ダイアグ通信によって読み出しできること。
事前条件	● QSEv 生成・保管に関する設計値が上位文書[1]に従い設定されている。 ● 検知機能の各々の異常通知を模擬するソフトウェアが試験的に配置されている。
試験手順	● 表 3-1 に従い、検知機能が通知する異常毎に下記の試験を実施すること。 (1) LAN テスタから供試品に対して、QSEv の読み出しを実施する。 (2) 異常通知を模擬するソフトウェアを用いて、SEv の集約間隔ごとに 3 回の間隔で複数回、SEv 生成機能に異常を通知する。 (3) LAN テスタから供試品に対して、QSEv の読み出しを実施する。
測定項目	● 検知機能が通知する異常毎に下記を測定すること。 (A) 試験手順(1)における読み出しの結果 (B) 試験手順(3)における読み出しの結果
合格基準	● 検知機能が通知する異常毎に、測定項目が下記の内容である。 ➢ 測定項目(A)が試験手順(2)により生成されうる QSEv を含まない。 ➢ 測定項目(B)が試験手順(2)により生成されうる QSEv を含む。 ✧ 全ての保管されたメッセージの QSEv に含まれる Count の和が SEv 生成機能に異常を通知した回数と一致する。 ✧ 各 QSEv の下記フィールドの値が期待値通り(※1)であること。 - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Count - Context Data ※1 上位文書[1] IDSHER_07103 及び参照文書[1] IDSQSR_03303 で定義されたものに従うこと
備考	無し。

【IDSHET_07129】	
試験内容	供試品が QSEv 保管機能を有する場合に、本試験を実施する。QSEv を保管する個数の上限値以上の数の QSEv が生成されたとき、最も古い QSEv が上書きされ、新しく生成された QSEv が保管されることを確認する
事前条件	● QSEv 生成・保管に関する設計値が上位文書[1]に従い設定されている。 ● QSEv を保管する個数の上限値の数の QSEv が保管されている。 ● 検知機能の各々の異常通知を模擬するソフトウェアが試験的に配置されている。
試験手順	● 検知機能が通知する異常毎に下記の試験を実施すること。 (1) LAN テスタから供試品に対して、QSEv の読み出しを実施する。 (2) 異常通知を模擬するソフトウェアを用いて、SEv 生成機能に異常を通知する。 (3) LAN テスタから供試品に対して、QSEv の読み出しを実施する。
測定項目	● 検知機能が通知する異常毎に下記を測定すること。 (A) 試験手順(1)における読み出しの結果 (B) 試験手順(3)における読み出しの結果
合格基準	● 検知機能が通知する異常毎に、測定項目が下記の内容である。 ➢ 測定項目(A), (B)が試験手順(2)により生成されうる QSEv を含む。 ✧ 試験手順(2)によって発生しうる QSEv の個数が QSEv を保管する個数の上限値であること。 ✧ 各 QSEv の下記フィールドの値が期待値通り(※1)であること。 - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Count - Context Data (※2) ※1 上位文書[1] IDSHER_07103 及び参照文書[1] IDSQSR_03303 で定義されたものに従うこと ※2 最も古い QSEv が上書きされたことがわかる Context Data となるように評価を行うこと
備考	無し。

4.1.3.2. QSEv の消去

【IDSHET_07204】	
試験内容	供試品が QSEv 保管機能を有する場合に、本試験を実施する。不揮発性メモリに保管される QSEv がダイアグ通信によって消去できることを確認する。
事前条件	● 不揮発性メモリに QSEv が保管されている。
試験手順	(1) LAN テスタから供試品に対して、QSEv の読み出しを実施する。 (2) LAN テスタから供試品に対して、QSEv の消去を実施する。 (3) LAN テスタから供試品に対して、QSEv の読み出しを実施する。
測定項目	(A) 試験手順(1)における読み出しの結果 (B) 試験手順(3)における読み出しの結果
合格基準	● 測定項目(A)が QSEv を含む。 ● 測定項目(B)が QSEv を含まない。
備考	無し。

4.2. **品質評価**

【IDSHET_12201】	
試験内容	本システムおよび生成される QSEv は、遠隔車外との通信を終端する機能から改ざんされないよう、当該機能から書き込みアクセス禁止とされていることを確認する。
事前条件	● なし。
試験手順	(1) 供試品の設計仕様を確認する。
測定項目	(A) 試験手順(1)の設計仕様
合格基準	● 測定項目(A)が要求事項通りに設計されている。
備考	無し。

4.3. **設計値評価**

【IDSHET_03401】	
試験内容	QSEv 生成・保管に関する設計値が上位文書[1]に従い設定可能であることを確認する。
事前条件	● なし。
試験手順	(1) 供試品のソースコードを確認する。(※1) ※1 ソースコードを確認できない場合は設計仕様を確認してもよい。
測定項目	(A) 試験手順(1)のソースコード
合格基準	● 設計値を変更した際、ロジックを変更することなくソフトウェアの動作を変更できることを確認する。
備考	無し。

Revision record

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	Modified corresponding to modification of requirements specification	2021/08/06	46F 4G Takeyama
a00-02-a	Tests fleshed	2022/03/24	46F 4G Takeyama
a00-03-a	・Description related to IDSHER_07202 deleted ・Check of UserDefMemoryDTC added because of addition of IDSHET_07109 ・Description of QSEv read and QSEv storing added at the beginning of 4.Tests	2022/06/09	46F 4G Takeyama
a00-04-a	- IDSHET_04101 requirement modified for clarification - IDSHET_01601 requirement modified for clarification - IDSHET_01101 allocation condition added - IDSHET_01102 allocation condition added - IDSHET_01201 allocation condition added - IDSHET_01202 allocation condition added - IDSHET_01501 allocation condition added, error corrected (only for English version) IDSHET_01502 allocation condition added, error corrected (only for English version) - IDSHET_01401 allocation condition added and requirement modified for clarification - IDSHET_02301 requirement modified for clarification - IDSHET_12201 Test modified	2022/11/25	46F 4G Takeyama

Table of Contents

1. Introduction

1.1. Purpose of this document

This document defines the test specification for testing the requirements defined by the *Requirements specification of Host-based IDS for Entry Point* (Input document [1]).

1.2. Target of this document

This document shall be allocated to entry-point ECUs/VMs to which "*Requirements specification of Host-based IDS for Entry Point*" is applied.

1.3. Prerequisites

QSEv creation function has been tested based on Reference [1].

1.4. Description of tests

We describe tests as [IDSHET_*] in this document where [Note] means just a supplementary note.

1.5. Related 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	Requirements Specification of Host-based IDS for Entry Point	-

1.5.2. References

Table 1-2: References

No.	Document name	Ver.
1	Test Specification of QSEvs Creation	-
2	TOYOTA Phase6 Diagnostics Communication and Reprogramming standard specifications	-

2. Test Overview

We show the table of all tests defined in this document (Table 2-1). Only if all tests applied are judged "pass", the test sample shall be judged as "passed".

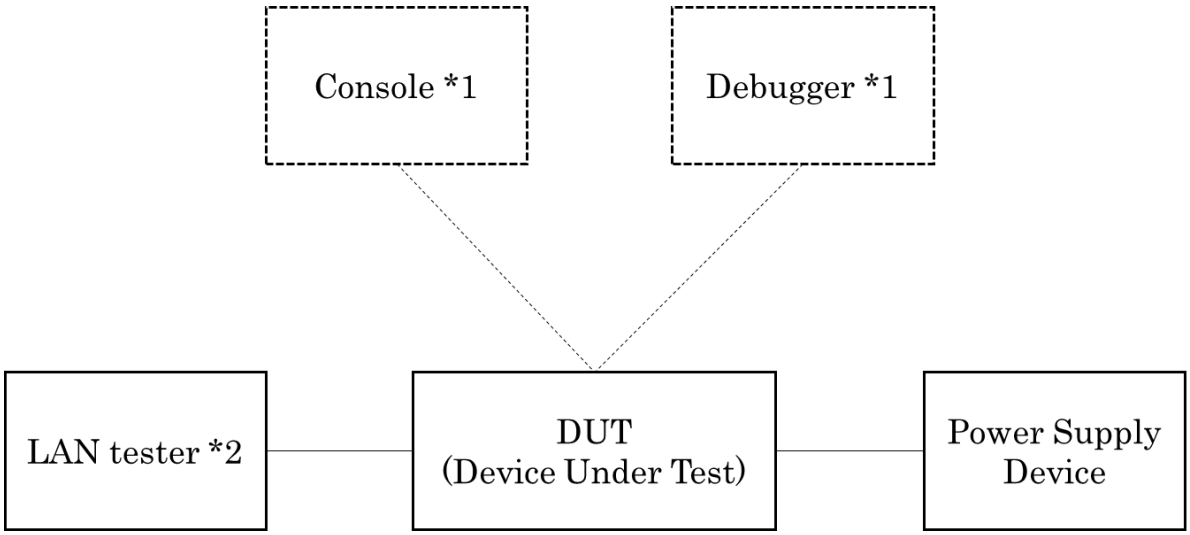
Table 2-1: Table of all tests

Requirements defined in the input document [1]				Tests	Production-time function
Category			Requirement ID	Test ID	
Functional requirements	Detection function	Detection of abort of a first layer protection function for communication from remote Out-Car	IDSHER_04101	IDSHET_04101	-
		Detection of illegal operation of a function to terminate communication from remote Out-Car	IDSHER_01601	IDSHET_01601	-
			IDSHER_01101	IDSHET_01101	-
			IDSHER_01102	IDSHET_01102	-
			IDSHER_01201	IDSHET_01201	-
			IDSHER_01202	IDSHET_01202	-
			IDSHER_01501	IDSHET_01501	-
			IDSHER_01502	IDSHET_01502	-
			IDSHER_01401	IDSHET_01401	-
		Detection of manipulation of CSP/PSP or software in an entry point region	IDSHER_02101	IDSHET_02101	-
			IDSHER_02301	IDSHET_02301	-
		SEv creation	IDSHER_07102	IDSHET_07108	-
	QSEv creation function	SEv qualification	IDSHER_07103	IDSHET_07109 IDSHET_07118 IDSHET_07119	
	QSEv transmission function	QSEv transmission	IDSHER_07108	IDSHET_07108 IDSHET_07118	
			IDSHER_07208	IDSHET_07208	
	QSEv storing function	QSEv storing	IDSHER_07109 IDSHER_07111	IDSHET_07109 IDSHET_07119	
		QSEv read	IDSHER_07110	IDSHET_07129	
		QSEv deletion	IDSHER_07204	IDSHET_07204	
Quality tests			IDSHER_12201	IDSHET_12201	-
Parameters tests			IDSHER_03401	IDSHET_03401	-
			IDSHER_03402	IDSHET_07108 IDSHET_07109 IDSHET_07118 IDSHET_07119 IDSHET_07129	-

3. Test Environment

In this specification, we assume the test environment shown in Figure 3-1.

.



*1 Use one if necessary.

*2 It can be able to perform diagnostic communication.

Figure 3-1: Test environment

It is difficult to conduct tests to Host-based IDS for entry point (hereinafter referred to as *this system*) by intrusion to DUT from outside because this system detects anomaly inside software. Therefore, we alter the software to be monitored, its behavior, and data to test this system. In addition to that, you may use a dummy detection function that simulates original notification of anomaly to conduct tests except detection function because it is difficult to control the timing of anomaly occurrence depending the implementation of the software and it makes possible to minimize alteration of the system. We show the test policy based on reasons above in Figure 3-2. However, you may use console and debugger to DUT when you alter the software and use dummy detection function that simulates original notification of anomaly.

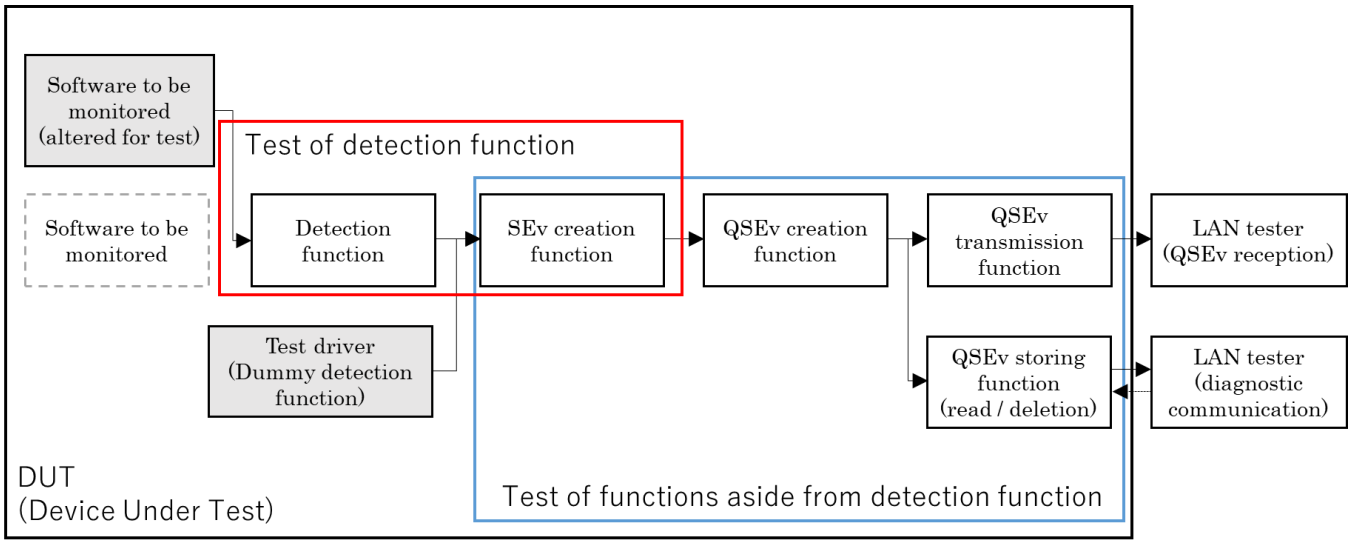


Figure 3-2: Test policy of this system

We show the patterns of the tests and the image for the tests except those of detection function in Table 3-1 and Figure 3-3. We conduct tests for SEv creation function, QSEv creation function, QSEv transmission function, and QSEv storing function with multiple test patterns of anomaly occurrence for each anomaly.

Table 3-1: Test pattern

Detection function	Pattern of notifications of anomaly	Test ID	Measurement item
Anomaly type for each detection function ・IDSHER_04101 ・IDSHER_01601 ・IDSHER_01101 ・IDSHER_01102 ・IDSHER_01201 ・IDSHER_01202 ・IDSHER_01501 ・IDSHER_01502 ・IDSHER_01401 ・IDSHER_02101 ・IDSHER_02301	Single	IDSHET_07108	Received messages
		IDSHET_07109	Read results
	Multiple (3 notifications are transmitted several times enough to test qualification function in each aggregation interval. However, the number of times equals to the number of the upper limit of QSEv storing or less. Specifically, we assume that the aggregation interval is [IdsMEventAggregationTimeInterval]/3 sec, and the number of times of transmission is 3*([NumberOfQSEvs]-1) times)	IDSHET_07118	Received messages
		IDSHET_07119	Read results

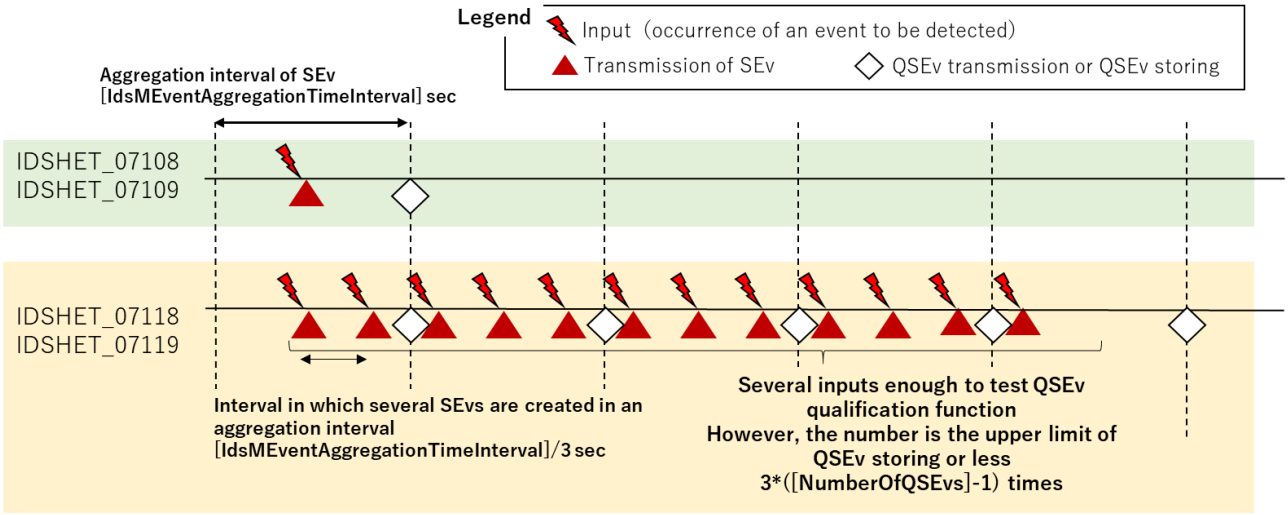


Figure 3-3: Test pattern image

4. Tests

We define tests for this system. In this chapter, QSEv read is conducted by diagnostic communication using SID 0x19 and DID 0xA910, and QSEv deletion is conducted by diagnostic communication using SID 0x14. For details of the procedure of diagnostic communication, see the references document [2].

4.1. Functional requirement tests

We define functional requirement tests for the implementation of the functional requirements in this section.

4.1.1. Detection function

4.1.1.1. Detection of abort of a first layer protection function for communication from remote Out-Car

【IDSHET_04101】	
Test	If a first layer protection function for communication from remote Out-Car is designed as resident software (resident process), this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function if such software does not work in a situation when the software should work
Pre-condition	● We define a first layer protection function for communication from remote Out-Car as software to be monitored. ● Software to be monitored can be altered for the test. ● An event that leads to operate the software can be triggered for the test.
Test procedure	(1) Trigger an event that leads to operate the software to be monitored after the software was altered (*1) so that the software does not operate. (2) Monitor notification from detection function to SEv creation function. (*2) *2 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (2).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (1).
Note	*1 One of the examples of alteration is that the process does not start or the process halts.

4.1.1.2. Detection of illegal operation of a function to terminate communication from remote Out-Car

4.1.1.2.1. Detection of abnormal control flow

【IDSHET_01601】	
Test	Test whether an anomaly is notified to SEv creation function when a transition between functions that shall not occur in an authenticate flow occurs or is attempted when software composing a function to terminate communication from remote Out-Car is running If there are some software to be monitored, conduct tests of each software to be monitored. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software composing a function to terminate communication from remote Out-Car as software to be monitored. ● Data can be altered for the test so that an illegal transition occurs while the software to be monitored is running.
Test procedure	(1) Trigger a transition between functions that shall not occur in an authenticate flow by altering data below while the software to be monitored is running. However, each item below shall be performed for the test. ➢ Alter the value of a function pointer into data that trigger a transition that shall not occur in an authenticate flow (*1) at the point of a function call that uses a function pointer (indirect call). ➢ Alter the value of a return address stored in a call stack into data that trigger a transition that shall not occur in an authenticate flow (*2) at the point of a return from a function. (2) Monitor notification from detection function to SEv creation function (*3). *3 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (2).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (1).

Note	*1 For example, addresses except tops of a function are applicable to data that trigger a transition that shall not occur in an authenticate flow when a function pointer is altered. *2 For example, addresses except points of a function call are applicable to data that trigger a transition that shall not occur in an authenticate flow when a return address is altered.

4.1.1.2.2. Detection of illegal access to non-volatile memory

【IDSHET_01101】	
Test	If software composing a function to terminate communication from remote Out-Car has architecture so that it can access to non-volatile memory in an entry point region by a path of a file system and the software is designed so that unnecessary access is not permitted, this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function when 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. - Read access - Write access - Execute access - Change attribute If there are some software to be monitored, conduct tests of each software to be monitored. If there are several paths on non-volatile memory in the entry point region, conduct tests to each path. Moreover, if there are several unpermitted operations from read access, write access, execute access, or change attribute, conduct tests to each operation. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software composing a function to terminate communication from remote Out-Car as software to be monitored. ● Software to be monitored can be altered for the test.
Test procedure	(1) Alter the software to be monitored to perform any operation that is not permitted to a path on non-volatile memory in the entry point region. (2) Perform any operation that is not permitted by the software to be monitored. (3) Monitor notification from detection function to SEv creation function. (*1) *1 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (3).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (2).
Note	None.

【IDSHET_01102】	
Test	If software composing a function to terminate communication from remote Out-Car has architecture so that it can access to non-volatile memory in an entry point region by an address of a file system and the software is designed so that unnecessary access is not permitted, this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function when the software performs any operation shown below by an address to non-volatile memory in the entry point region where the operation is not permitted to be performed, or attempts to do so. - Read access - Write access - Execute access - Change attribute If there are some software to be monitored, conduct tests of each software to be monitored. If there are several addresses on non-volatile memory in the entry point region, conduct tests to each address. Moreover, if there are several unpermitted operations from read access, write access, execute access, or change attribute, conduct tests to each operation. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software composing a function to terminate communication from remote Out-Car as software to be monitored. ● Software to be monitored can be altered for the test.
Test procedure	(1) Alter the software to be monitored to perform any operation that is not permitted to an address on non-volatile memory in the entry point region. (2) Perform any operation that is not permitted by the software to be monitored. (3) Monitor notification from detection function to SEv creation function. (*1) *1 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (3).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (2).
Note	None.

4.1.1.2.3. Detection of illegal access to volatile memory

【IDSHET_01201】	
Test	If software composing a function to terminate communication from remote Out-Car has architecture so that it can access to volatile memory in an entry point region by a path of a file system and the software is designed so that unnecessary access is not permitted, this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function when 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. - Read access - Write access - Execute access - Change attribute If there are some software to be monitored, conduct tests of each software to be monitored. If there are several paths on volatile memory in the entry point region, conduct tests to each path. Moreover, if there are several unpermitted operations from read access, write access, execute access, or change attribute, conduct tests to each operation. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software composing a function to terminate communication from remote Out-Car as software to be monitored. ● Software to be monitored can be altered for the test.
Test procedure	(1) Alter the software to be monitored to perform any operation that is not permitted to a path on volatile memory in the entry point region. (2) Perform any operation that is not permitted by the software to be monitored (3) Monitor notification from detection function to SEv creation function. (*1) *1 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (3).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (2).

Note	None.

【IDSHET_01202】	
Test	If software composing a function to terminate communication from remote Out-Car has architecture so that it can access to volatile memory in an entry point region by an address of a file system and the software is designed so that unnecessary access is not permitted, this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function when the software performs any operation shown below by an address to volatile memory in the entry point region where the operation is not permitted to be performed, or attempts to do so. - Read access - Write access - Execute access - Change attribute If there are some software to be monitored, conduct tests of each software to be monitored. If there are several addresses on volatile memory in the entry point region, conduct tests to each address. Moreover, if there are several unpermitted operations from read access, write access, execute access, or change attribute, conduct tests to each operation. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software composing a function to terminate communication from remote Out-Car as software to be monitored. ● Software to be monitored can be altered for the test.
Test procedure	(1) Alter the software to be monitored to perform any operation that is not permitted to an address on volatile memory in the entry point region. (2) Perform any operation that is not permitted by the software to be monitored. (3) Monitor notification from detection function to SEv creation function. (*1) *1 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (3).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (2).
Note	None.

4.1.1.2.4. Detection of illegal access to IO (peripheral)

【IDSHET_01501】	
Test	If software composing a function to terminate communication from remote Out-Car has architecture so that it can access to IO (peripheral) in an entry point region by a path of a file system and the software is designed so that unnecessary access is not permitted, this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function when 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. - Read access - Write access - Change attribute If there are some software to be monitored, conduct tests of each software to be monitored. If there are several paths to IO (peripheral) in the entry point region, conduct tests to each path. Moreover, if there are several unpermitted operations from read access, write access, or change attribute, conduct tests to each operation. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software composing a function to terminate communication from remote Out-Car as software to be monitored. ● Software to be monitored can be altered for the test.
Test procedure	(1) Alter the software to be monitored to perform any operation that is not permitted to a path to IO (peripheral) in the entry point region. (2) Perform any operation that is not permitted by the software to be monitored (3) Monitor notification from detection function to SEv creation function. (*1) *1 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (3).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (2).
Note	None.

【IDSHET_01502】	
Test	If software composing a function to terminate communication from remote Out-Car has architecture so that it can access to IO (peripheral) in an entry point region by an address of a file system and the software is designed so that unnecessary access is not permitted, this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function when the software performs any operation shown below by an address to IO (peripheral) in the entry point region where the operation is not permitted to be performed, or attempts to do so. - Read access - Write access - Change attribute If there are some software to be monitored, conduct tests of each software to be monitored. If there are several addresses to IO (peripheral) in the entry point region, conduct tests to each address. Moreover, if there are several unpermitted operations from read access, write access, or change attribute, conduct tests to each operation. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software composing a function to terminate communication from remote Out-Car as software to be monitored. ● Software to be monitored can be altered for the test.
Test procedure	(1) Alter the software to be monitored to perform any operation that is not permitted to an address to IO (peripheral) in the entry point region. (2) Perform any operation that is not permitted by the software to be monitored. (3) Monitor notification from detection function to SEv creation function. (*1) *1 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (3).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (2).
Note	None.

4.1.1.2.5. Detection of illegal usage of function

【IDSHET_01401】	
Test	If an entry point region has a function that require an authority to use and the software composing functions to terminate communication from remote Out-Car is designed so that unnecessary access is not permitted, this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function when the software uses a function unpermitted to use, or attempts to do so. If there are some software to be monitored, conduct tests of each software to be monitored. If there are several functions unpermitted to use in the entry point region, conduct tests to each function. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software composing a function to terminate communication from remote Out-Car as software to be monitored. ● Software to be monitored can be altered for the test.
Test procedure	(1) Alter the software to be monitored as the software uses a function (*1) unpermitted to use in the entry point region. (2) Perform any operation that is not permitted by the software to be monitored. (3) Monitor notification from detection function to SEv creation function. (*2) *2 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (3).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (2).
Note	*1 We show examples of functions for the test. - A system call provided by OS in the entry point region that the software to be monitored is not permitted to use. - A function provided by software to other software through communications between processes that the software to be monitored is not permitted to use.

4.1.1.3. Detection of manipulation of CSP/PSP or software in entry-point area

4.1.1.3.1. Detection of manipulation of CSP/PSP

【IDSHET_02101】	
Test	If an entry point region has data fallen into CSP/PSP in non-volatile memory, this requirement shall be allocated. Test whether an anomaly is notified to SEv creation function when the data is manipulated at the usage of it. If there are several data to be monitored, conduct tests to each data to be monitored. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define CSP/PSP in non-volatile memory in an entry point region as data to be monitored. ● Data to be monitored can be altered for the test.
Test procedure	(1) Attempt to use the data after altering the data to be monitored for the test. (2) Monitor notification from detection function to SEv creation function. (*2) *2 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (2).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (1).
Note	*1 For example, data allocation to be monitored to non-volatile memory and HSM is applicable to usage in this test.

4.1.1.3.2. Detection of manipulation software

【IDSHET_02301】	
Test	Test whether an anomaly is notified to SEv creation function when any of the following is manipulated at startup of each software allocated to an entry-point region. - The code of the software - The data controlling the behavior of the software which can be updeted only by reprogramming If there are some software to be monitored, conduct tests of each software to be monitored. However, you can conduct one test instead of conducting all tests that have the same mechanism of monitor.
Pre-condition	● We define software allocated to an entry-point region as software to be monitored. ● The code and the data controlling the behavior of the software which can be updeted only by reprogramming to be monitored can be altered for the test.
Test procedure	(1) Attempt startup of the software after altering the code and data controlling the behavior of the software which can be updeted only by reprogramming to be monitored for the test. (*1) (2) Monitor notification from detection function to SEv creation function. (*2) *2 If it is impossible to monitor notification directly inside the DUT, you can confirm the QSEv which is transmitted or stored by a LAN tester etc.
Measurement item	(A) Notification from detection function to SEv creation function in the test procedure (2).
Pass Criteria	● Measurement item shall be the notification that shall be notified in the test procedure (1).
Note	*1 For example, process creation is applicable to startup of software when the software to be monitored operates as a process.

4.1.2. QSEv transmission function

4.1.2.1. QSEv transmission

【IDSHET_07108】	
Test	If the DUT has QSEv transmission function, this requirement shall be allocated. Test whether QSEv creation function creates a communication frame and transmits it to IDM when SEv creation function is notified of an anomaly from detection function.
Pre-condition	● Parameters about QSEv creation and QSEv storing have been set in accordance with input document [1]. ● The software that simulates each anomaly notification of detection function has been installed.
Test procedure	● Conduct tests below for each anomaly that detection function reports in accordance with Table 3-1. (1) Notify SEv creation function of anomaly by the software that simulates anomaly notification. (2) Receive messages transmitted from DUT by a LAN tester.
Measurement item	● Measure an item below for each anomaly that detection function reports. (A) Messages received in the test procedure (2).
Pass Criteria	● Measurement item shall follow items below for each anomaly that detection function reports. ➢ Measurement item (A) contains QSEvs that can be generated in the test procedure (1). ✧ The number of QSEvs that can be generated in the test procedure (1) is one. ✧ Values in fields below of QSEv are expected (*1). - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Count - Context Data *1 Follow the definition of IDSHER_07103 in input document [1], and IDSQSR_03303 in reference document [1].
Note	None.

【IDSHET_07118】	
Test	If the DUT has QSEv transmission function, this requirement shall be allocated. Test whether QSEv creation function create a communication frame and transmit it to IDM after SEvs are qualified properly when SEv creation function is notified of an anomaly from detection function several times.
Pre-condition	● Parameters about QSEv creation and QSEv storing have been set in accordance with input document [1]. ● The software that simulates each anomaly notification of detection function has been installed.
Test procedure	● Conduct tests below for each anomaly that detection function reports in accordance with Table 3-1. (1) Notify SEv creation function of anomaly three times in an aggregation interval by the software that simulates anomaly notification several times. (2) Receive messages transmitted from DUT by a LAN tester.
Measurement item	● Measure an item below for each anomaly that detection function reports. (A) Messages received in the test procedure (2).
Pass Criteria	● Measurement item shall follow items below for each anomaly that detection function reports. ➢ Measurement item (A) contains QSEvs that can be generated in the test procedure (1). ✧ Sum of Count contained in all QSEvs received equals to the number of times SEv creation function is notified of anomaly. ✧ Values in fields below of QSEv are expected (*1). - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Context Data *1 Follow the definition of IDSHER_07103 in input document [1], and IDSQSR_03303 in reference document [1].
Note	None.

【IDSHET_07208】	
Test	If the DUT has QSEv transmission function, this requirement shall be allocated. Test whether the QSEv transmission function shall not transmit QSEvs if QSEv transmission by the QSEv transmission function wakes up network or prevents network from sleeping.
Pre-condition	● Parameters about QSEv creation and QSEv storing have been set in accordance with input document [1]. ● The software that simulates each anomaly notification of detection function has been installed. ● The state of network can be controlled as QSEv transmission by the QSEv transmission function wakes up network or prevents network from sleeping.
Test procedure	(1) Notify SEv creation function of anomaly by the software that simulates anomaly notification providing that QSEv transmission by the QSEv transmission function does not wake up network or does not prevent network from sleeping. (2) Receive messages transmitted from DUT by a LAN tester. (3) Notify SEv creation function of anomaly by the software that simulates anomaly notification providing that QSEv transmission by the QSEv transmission function wakes up network or prevents network from sleeping. (4) Receive messages transmitted from DUT by a LAN tester.
Measurement item	(A) Messages received in the test procedure (2). (B) Messages received in the test procedure (4).
Pass Criteria	● Measurement item (A) contains QSEvs that can be generated in the test procedure (1). ● Measurement item (B) does not contain QSEvs that can be generated in the test procedure (3).
Note	None.

4.1.3. QSEv storing function

4.1.3.1. QSEv storing / QSEv read

【IDSHET_07109】	
Test	If the DUT has QSEv transmission function, this requirement shall be allocated. Test items below. ● When SEv creation function is notified of an anomaly from detection function, QSEv storing function stores QSEvs on non-volatile memory. ● QSEvs stored on non-volatile memory can be read by diagnostic communication.
Pre-condition	● Parameters about QSEv creation and QSEv storing have been set in accordance with input document [1]. ● The software that simulates each anomaly notification of detection function has been installed.
Test procedure	● Conduct tests below for each anomaly that detection function reports in accordance with Table 3-1. (1) Read messages on DUT by a LAN tester. (2) Notify SEv creation function of anomaly by the software that simulates anomaly notification. (3) Read messages on DUT by a LAN tester.
Measurement item	● Measure items below for each anomaly that detection function reports. (A) Read results in the test procedure (1). (B) Read results in the test procedure (3).

Pass Criteria	● Measurement item shall follow items below for each anomaly that detection function reports. ➢ Measurement item (A) does not contain QSEvs that can be generated in the test procedure (2). ➢ Measurement item (B) contains UserDefMemoryDTC defined by IDSHER_07111 in the input document [1] corresponding to the event ➢ Measurement item (B) contains QSEvs that can be generated in the test procedure (2). ✧ The number of QSEvs that can be generated in the test procedure (2) is one. ✧ Values in fields below of QSEv are expected (*1). - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Count - Context Data *1 Follow the definition of IDSHER_07103 in input document [1], and IDSQSR_03303 in reference document [1].
Note	None.

【IDSHET_07119】	
Test	If the DUT has QSEv transmission function, this requirement shall be allocated. Test items below. ● When SEv creation function is notified of an anomaly from detection function several times, QSEv storing function stores QSEvs on non-volatile memory after SEvs are qualified properly. ● Several QSEvs stored on non-volatile memory can be read by diagnostic communication.
Pre-condition	● Parameters about QSEv creation and QSEv storing have been set in accordance with input document [1]. ● The software that simulates each anomaly notification of detection function has been installed.
Test procedure	● Conduct tests below for each anomaly that detection function reports in accordance with Table 3-1. (1) Read messages on DUT by a LAN tester. (2) Notify SEv creation function of anomaly three times in an aggregation interval by the software that simulates anomaly notification several times. (3) Read messages on DUT by a LAN tester.
Measurement item	● Measure items below for each anomaly that detection function reports. (A) Read results in the test procedure (1). (B) Read results in the test procedure (3).

Pass Criteria	● Measurement item shall follow items below for each anomaly that detection function reports. ➢ Measurement item (A) does not contain QSEvs that can be generated in the test procedure (2). ➢ Measurement item (B) contains QSEvs that can be generated in the test procedure (2). ✧ Sum of Count contained in all QSEvs stored equals to the number of times SEv creation function is notified of anomaly. ✧ Values in fields below of QSEv are expected (*1). - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Count - Context Data *1 Follow the definition of IDSHER_07103 in input document [1], and IDSQSR_03303 in reference document [1].
Note	None.

【IDSHET_07129】	
Test	If the DUT has QSEv transmission function, this requirement shall be allocated. Test whether the new QSEv is stored and the oldest QSEv is overwritten when more QSEvs are generated than the number of the upper limit for QSEv storing.
Pre-condition	● Parameters about QSEv creation and QSEv storing have been set in accordance with input document [1]. ● The number of stored QSEvs equals to the number of the upper limit for QSEv storing. ● The software that simulates each anomaly notification of detection function has been installed.
Test procedure	● Conduct tests below for each anomaly that detection function reports. (1) Read messages on DUT by a LAN tester. (2) Notify SEv creation function of anomaly by the software that simulates anomaly notification. (3) Read messages on DUT by a LAN tester.
Measurement item	● Measure items below for each anomaly that detection function reports. (A) Read results in the test procedure (1). (B) Read results in the test procedure (3).
Pass Criteria	● Measurement item shall follow items below for each anomaly that detection function reports. ➢ Measurement item (A), (B) contains QSEvs that can be generated in the test procedure (2). ✧ The number of QSEvs that can be generated in the test procedure (2) equals to the number of the upper limit for QSEv storing. ✧ Values in fields below of QSEv are expected (*1). - Protocol Header - IdsM Instance ID - Sensor Instance ID - Event Definition ID - Count - Context Data (*2) *1 Follow the definition of IDSHER_07103 in input document [1], and IDSQSR_03303 in reference document [1]. *2 Use proper Context Data so that the oldest QSEv is overwritten.
Note	None.

4.1.3.2. QSEv deletion

【IDSHET_07204】	
Test	If the DUT has QSEv transmission function, this requirement shall be allocated. Test whether QSEvs stored on non-volatile memory can be deleted by diagnostic communication.
Pre-condition	● QSEvs are stored on non-volatile memory.
Test procedure	(1) Read QSEvs on DUT by a LAN tester. (2) Delete QSEvs on DUT by diagnostic communication. (3) Read QSEvs on DUT by a LAN tester.
Measurement item	(A) Read results in the test procedure (1). (B) Read results in the test procedure (3).
Pass Criteria	● Measurement item (A) contains QSEvs. ● Measurement item (B) does not contain QSEvs.
Note	None.

4.2. Quality requirements

【IDSHET_12201】	
Test	Confirm that a function to terminate communication from remote Out-Car is prohibited from having write access to this system and generated QSEv so that they are not manipulated by the function.
Pre-condition	None.
Test procedure	(1) Check the design of the DUT.
Measurement item	(A) The design in the test procedure (1).
Pass Criteria	● Measurement item (A) follows requirement specification.
Note	None.

4.3. Parameters

【IDSHET_03401】	
Test	Confirm that parameters about QSEv creation and QSEv storing are configurable according to input document [1].
Pre-condition	None.
Test procedure	(1) Check the source code of the DUT. (*1) *1 If you cannot check the source code, you can check the design of the software.

Measurement item	(A) The source code in the test procedure (1).
Pass Criteria	● Confirm that when parameters are changed, the behavior of the software can be changed without altering logic.
Note	None.